Version 8.0

Part No. NN46110-507 02.01
311645-L Rev 01
20 October 2008
Document Status: Standard

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Router Using the Command Line Interface



Copyright © 2008 Nortel Networks. All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Check Point and FireWall-1 are trademarks of Check Point Software Technologies Ltd.

Cisco and Cisco Systems are trademarks of Cisco Systems, Inc.

Entrust and Entrust Authority are trademarks of Entrust Technologies, Incorporated.

Java and Solaris are trademarks of Sun Microsystems.

Linux and Linux FreeS/WAN are trademarks of Linus Torvalds.

Microsoft, Windows, Windows NT, and MS-DOS are trademarks of Microsoft Corporation.

Netscape, Netscape Communicator, Netscape Navigator, and Netscape Directory Server are trademarks of Netscape Communications Corporation.

SPARC is a trademark of Sparc International, Inc.

All other trademarks are the property of their respective owners.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN

ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Preface 45

Before you begin 45
Text conventions 45
Related publications 48
Printed technical manuals 49
How to get help 49

New in this release. 53

Features 53

Introduction 55

Accessing the CLI 56
Command modes 57
Configuration modes 59
Editing command line entries 64
Using command abbreviations 65
Using CLI online Help 66

User EXEC mode commands 67

cd 68
clear ip route 69
dir 71
enable 73
exit 74
help 75
ls 76
ping 78
pwd 81
show file systems 82
show flash: contents 83

show reload 85
show services 86
show sessions 88
show version 90
terminal paging 91
trace ip 92
who 94
Privileged EXEC mode commands 97

boot system 98
clear arp-cache 100
clear logging events 101
configure terminal 102
copy 103
delete 105
disable 106
exit 107
forced-logoff 108
help 110
kill 111
mkdir 113
more 114
reload 117
reload at 120
reload cancel 123
reload in 125
reload no-sessions 128
rename 131
retrieve software 132
rmdir 134
show arp 135
show data-collection-interval 136
show event-log size 137
show health 139
show log-file-lifetime 140
show logging config 142

show logging events 145
show logging history 150
show logging security 151
show logging syslog 154
show safe-mode 157
show serial-port 158
show software version 159
show system forwarding 160
Global Configuration mode commands. 163

arp 165
async-over-tcp enable 166
async-over-tcp local-ip-address 168
async-over-tcp peer-ip-address 170
async-over-tcp port number 172
async-over-tcp private 174
async-over-tcp public 176
async-over-tcp originator 177
async-over-tcp num-of-ticks 179
audible alarm 180
authentication-banner 181
auto-save-logging enable 182
auto-save-logging max-files 184
console mode 186
crypto exp 188
data-collection-interval 189
enable-ping 190
event-log size 191
exit 193
ftp access-list 194
ftp-server access-list 195
ftp-server passive 196
ftp-server port 198
help 199
hostname 200
http access-list 202

http port . . . 203
https access-list . . . 204
https private port . . . 206
ip http server . . . 208
ldap . . . 209
load . . . 211
log-file-lifetime . . . 212
logging history . . . 213
logging save-log . . . 215
logout . . . 217
ping-address . . . 217
ping-interval . . . 219
prompt . . . 220
restrict . . . 221
safe-mode duration . . . 223
safe-mode enable . . . 225
service ssh . . . 226
ssh-server access-list . . . 227
service ssh sftp . . . 229
show crypto . . . 231
show ssh-server . . . 232
snmp-server access-list . . . 233
snmp-server port . . . 235
ssh-server . . . 236
system forwarding gratuitous-arp enable . . . 237
system forwarding nexthop-forward enable . . . 239
system forwarding proxy-arp branch-office-tunnels enable . . . 240
system forwarding proxy-arp physical-interfaces enable . . . 241
system forwarding tunnel-to-tunnel-traffic BO-to-BO enable . . . 243
system forwarding tunnel-to-tunnel-traffic EU-to-BO enable . . . 245
system forwarding tunnel-to-tunnel-traffic EU-to-EU enable . . . 246
system-log-to-file enable . . . 248
telnet access-list . . . 249
telnet port . . . 251
validate . . . 252

Creating and using scripts to provision a VPN Router 255

Creating a script with the show running-config command 256
Editing the output file 257
Guidelines for creating and executing scripts 259
Estimating provisioning time 260
Preparing to run a script file 261
Executing a script 263
show running-config command 263

Group, filters, users, branch office group configuration commands . . . 271

access-hours 275
action 278
action nexthop 279
add-rule 280
address 282
administration group-manage 283
administration switch-manage 285
administration uid 287
administration users-manage 288
antireplay enable 290
authentication (Branch Office Group RIP or Branch Office Group OSPF) 292
authentication (Group IPsec Tunnel) 293
authentication (L2TP, PPTP, L2F) 295
banner 297
bo-group 298
client 300
client-address 302
client auto-connect 303
client auto-connect networks 304
client dynamic-dns enable 306
client failover-tuning 307
client failover-tuning interval 309
client failover-tuning retransmissions 310
client nat interval 311
client policy 312

client screen-saver activation-time 314
client screen-saver password 315
committed rate 316
compress 318
connection 319
contact 320
dead-interval 322
default 323
df-bit 325
direction 327
display-banner 328
dynamic-authenticate 329
encryption 331
encryption ike 333
excess action 336
excess rate 337
exit 339
export bo-static-metric 340
export default-metric 341
export ospf-metric 342
export static-metric 343
filters (Group Connectivity Configuration) 344
filter add 346
filter rule add 348
forced-logoff 350
group (Global Configuration Command) 351
group 353
hello-interval 355
idle-timeout 356
import default-route 357
initial-contact enable 358
ip address 360
ip address-pool 361
ip address-src 362
ip domain-name 364

ipsec issuer-ca 365
ipsec server-ca (User Configuration) 366
ipsec subject-alt-name 368
ipsec subject-dn 369
ipsec uid (User Configuration) 370
ipsec uid pwchange enable 372
ipsec-transport 373
ipx 374
isakmp-retransmission interval 375
isakmp-retransmission max-attempts 377
keepalive interval 378
keepalive ondemand-conn 379
l2f uid (User Configuration) 380
l2tp uid (User Configuration) 382
login max-attempts 383
logins 384
logoff-notification-interval 385
move-rule 387
nailed-up 388
nat-traversal 389
no bo-group 391
no group 392
nortel-client action 394
nortel-client filter 396
nortel-client message 397
nortel-client version 399
no uid lockout 400
password 401
password-storage 403
pfs 404
poison-reverse 405
port 406
ppp-links max-number 407
pptp uid (User Configuration) 409
priority 410

priority call-admission 411
priority forwarding 413
receive version 414
rekey data-count 415
rekey timeout 417
remove-rule 418
retransmit-interval 419
rsvp 421
rsvp token-bucket 422
send version 423
server 425
show bo-group 427
show filters 428
show groups 430
show users 432
split inverse-tunnel-network 433
split tunneling 435
split tunnel-networks 436
static-ipaddress (Group Connectivity Configuration) 438
static-ipaddress (User Configuration) 439
static-subnet-mask 440
transmit-delay 442
use address 443
use dest-port 444
use nexthop-addr 446
use protocol 447
use src-port 449
user add 450
vendor-id 452
wins address 453

Event log commands 455

logging capture-filter entity add 456
logging capture-filter entity remove 458
logging capture-filter severity add 461
logging capture-filter severity remove 463

logging display-filter entity add 465
logging display-filter entity remove 467
logging display-filter severity add 470
logging display-filter severity remove 472
show logging capture-filter 474
show logging capture-filter entity all 475
show logging capture-filter entity 478
show logging capture-filter severity all 480
show logging capture-filter severity 481
Branch office connection configuration commands 485

bo-conn 486
compress 488
conn-type 489
filter 490
group 491
ipsec authentication 493
ipsec issuer-ca 494
ipsec relative-dn 496
ipsec server-ca 498
ipsec subject-alt-name 499
ipsec subject-dn 500
l2tp authentication 502
l2tp concentrator 503
l2tp ipsec-data-protection 504
l2tp stateless-mode 506
local-endpoint 507
local-gateway 508
local-network 510
mtu 511
mtu enable 513
nat 514
pptp authentication 515
remote-endpoint 517
remote-endpoint host 518
remote-network 520

routing 521
show bo-conn 523
state 524
tunnel-type 525
Access-hours, client policy, domains, and networks commands 527

access-hours 527
client-policy 529
domain add 530
network add 532
show access-hours 534
show client-policy 535
show domains 536
show networks 538
IP address pool commands 541

ip address-pool 542
show ip dhcp proxy-server 545
show ip local pool 547
Administrator, system identity, time, Syslog, and NTP commands 551

adminname 553
clock dst-observance 555
clock set 557
clock timezone 558
compress-files enable 560
create diskette 562
create recovery 564
create safe-mode-config 565
default language 567
dns-proxy enable 568
erase config-file 569
exception backup 571
ftp-coredump 575
ftp-coredump enable 577
hostname 578

idle-timeout 579
ip address 581
ip domain-name 582
ip name-server 583
license 584
logging 586
ntp 588
ntp authentication-key 589
ntp broadcast server 590
ntp multicast server 591
ntp server 592
reformat diskette 594
retrieve backup 596
save current-config-file 598
scheduler manageability 599
show admin settings 601
show clock 602
show compress-files 603
show config-files 605
show current-config-file 606
show exception backup 607
show ftp-coredump 609
show hosts 610
show ip name-server 611
show license 613
show ntp 614
show scheduler 616
show status statistics admin 617
show status statistics hardware 620
show status statistics interfaces 624
show status statistics network 627
show status statistics resources 634
show status statistics routing 640
show status statistics security 642
show status statistics system 645

show syslog-host 652
show system accelerator 653
show system accelerator statistics 656
split-dns enable 659
system accelerator auto-recovery enable 660
system accelerator enable 662
verify system 663
Service and tunnel configuration commands 665

aaa authentication administrator 666
aaa authentication fwua 668
aaa authentication ipsec 669
aaa authentication l2f 671
aaa authentication l2tp 672
aaa authentication pptp 673
cmp 675
crl retrieval 676
demand 677
fips 679
firewall user-authentication 680
ftp-server enable 682
http enable 683
https 684
identification enable 686
ipsec authentication 688
ipsec encryption 689
ipsec encryption ike 691
ipsec fail-over 693
ipsec load-balance 694
ipsec nat-traversal 696
ipsec nat-traversal-bo 697
ipsec nat-traversal port 698
l2f authentication 699
l2f nas-uid 701
l2tp authentication 702
l2tp lac-uid 704

pptp authentication 706
radius service 707
radius-accounting private enable 709
radius-accounting public enable 710
radius-client 711
radius-client host 713
radius-client port 714
show firewall user-authentication 715
show (ipsec | l2f | l2tp | pptp) 717
telnet enable 718
tunnel protocol 719
SSL configuration commands 721

reset ssl-vpn 721
restart ssl-vpn 723
show ssl cipher 724
show ssl server-cert 726
show ssl option des-cbc-padding 727
show ssl-vpn 728
ssl cipher 729
ssl https-port 731
ssl option des-cbc-padding enable 733
ssl server-cert 735
ssl-vpn enable 736
ssl-vpn init 737
ssl-vpn csfw-implied-rule enable 739
ssl-vpn paste-config 740
ssl-vpn-cli 742
RADIUS server configuration commands 745

aaa accounting network radius 746
aaa accounting session update 747
aaa accounting timeout 748
aaa accounting timeout enable 750
aaa accounting update 751
aaa authorization network radius 752

accounting radius-server 753
accounting radius-server host 754
clear accounting 756
radius-server 757
radius-server authentication 758
radius-server default-group 760
radius-server domain-delimiter 761
radius-server group 762
radius-server group enable 764
radius-server group domain-delimiter 766
radius-server group group-level enable 767
radius-server group maximum-transmit-attempts 769
radius-server group response-timeout-interval 770
radius-server group suffix-remove enable 772
radius-server host 773
radius-server interface 775
radius-server key 776
radius-server retransmit 778
radius-server suffix-remove 779
radius-server suppress-service-type enable 780
radius-server timeout 782
show accounting radius-server 783
show authentication radius-server 784
show radius-server group 786

LDAP server configuration commands 789

aaa authentication ldap-server 790
authentication ldap-server base-dn 791
authentication ldap-server contivity-group 793
authentication ldap-server default-group 794
authentication ldap-server digital-certificate 795
authentication ldap-server domain-delimiter 797
authentication ldap-server filter 798
authentication ldap-server host 799
authentication ldap-server ip-address 802
authentication ldap-server ldap-filter 803

authentication ldap-server net-mask 805
authentication ldap-server password 806
authentication ldap-server remove-suffix 808
authentication ldap-server subject-dn 809
authentication ldap-server timeout 811
authentication ldap-server uid 812
authentication ldap-server username-password 814
ldap-server encryptionkey-hex 815
ldap-server encryptionkey-text 817
ldap-server external 818
ldap-server external host 820
ldap-server internal 823
ldap-server source 826
ldap-server triple-des enable 827
proxy ldap-server server-type 829
proxy ldap-server pwd-timestamp-attr 830
proxy ldap-server pwd-lifetime 831
show authentication ldap-server 832
show ldap-server 834
ssl encryption 836

DHCP server configuration commands 839

bootfile 840
debug dhcp 841
description 843
excluded-address 844
hardware-address 847
host 848
included-address 850
ip dhcp server pool 851
lease 853
next-server 856
option 857
option client-identifier 860
option default-router 861
option dns-server 863

option domain-name 864
option netbios-name-server 865
option netbios-node-type 867
server-name 868
service dhcp enable 870
service dhcp restart 871
show ip dhcp server 872
DHCP server configuration example 875
SNMP commands 877

show snmp get-host 878
show snmp host 879
show snmp identity 880
show snmp mib 881
show snmp-traps trap-groups 883
show snmp-traps trap-hosts 886
snmp-ifspeed 888
snmp-server contact 889
snmp-server enable traps attack 890
snmp-server enable traps hardware 891
snmp-server enable traps ietf 896
snmp-server enable traps server 898
snmp-server enable traps service 900
snmp-server get-host 901
snmp-server host 903
snmp-server location 904
snmp-server management 905
snmp-server mib 906
snmp-server name 908
Certificate commands 909

ca-allow-all enable 911
ca-import enable 912
ca-trusted enable 914
country 915
create 916

crl . . . 918
crl http . . . 919
crl optimize . . . 921
crl optional . . . 922
crl search-base host port attribute . . . 923
crl search-base host port bind-dn . . . 925
crl search-base host port enable . . . 928
crl search-base host port object-class . . . 930
crl search-base host port password . . . 932
crl search-base host port ssl-enable . . . 934
crl update . . . 936
crypto ca allow . . . 937
crypto ca configure . . . 939
crypto ca identity . . . 940
crypto import . . . 941
crypto password . . . 942
crypto server configure . . . 943
crypto server request . . . 945
crypto trusted . . . 946
default-group . . . 947
enrollment url . . . 948
key . . . 950
locality . . . 951
name . . . 952
no crypto ca enroll . . . 953
no crypto server certificate renew . . . 954
openSSL enable . . . 955
org-unit . . . 957
organization . . . 958
ocsp . . . 960
recover reference-number . . . 961
renew . . . 962
revoke now . . . 963
set authorization-code . . . 964
set ca-default-group . . . 965

set issuer 966
set issuer-dn 967
set key-size 968
set port 969
set reference-number 971
set subject-dn 972
show crypto ca certificates 973
show crypto certificates 976
show crypto enrollment 977
show crypto password 978
show crypto server certificates renew 980
state 981
subject-dn 982

Nortel VPN Router Stateful Firewall and NAT commands 985

clear flow-cache 987
firewall 988
firewall alg snmp enable 990
firewall alg virtual 991
firewall anti-spoof 993
firewall cone-nat 994
firewall connection number 995
firewall hairpin enable 997
firewall logging 998
firewall scan-detection 1001
firewall tunnel-filter 1003
firewall tunnel-management-filter 1004
nat-traversal 1006
netobj 1007
netobj-group 1010
policy nat 1012
policy nat enable 1014
policy nat interface 1015
policy object 1017
policy security 1019
rule (Firewall Policy Configuration) 1021

rule (NAT Policy Configuration) 1025
rule description (NAT Policy Configuration) 1029
rule service (NAT Policy Configuration) 1030
rule status (NAT Policy Configuration) 1032
service (Firewall Policy Configuration) 1034
service (NAT Policy Configuration) 1037
service-group 1038
show firewall 1040
show interfaces 1044
show netobjs 1046
show policy nat 1047
show policy security 1049
show rules (Firewall Policy Configuration) 1051
show rules (NAT Policy Configuration) 1053
show services 1055
Example: Using the NOT operand to configure NAT 1058
TunnelGuard configuration commands 1059

show tunnel-guard filters 1060
show tunnel-guard policy 1061
show tunnel-guard server-port 1062
tunnel-guard agent-min-version 1063
tunnel-guard agent-query-timeout 1065
tunnel-guard banner 1067
tunnel-guard banner-fragment 1068
tunnel-guard enable 1069
tunnel-guard fail-action 1071
tunnel-guard noagent-action 1072
tunnel-guard recheck-interval 1074
tunnel-guard display-error-detail 1075
tunnel-guard heartbeat-interval 1077
tunnel-guard heartbeat-retry 1078
tunnel-guard jre-location 1080
tunnel-guard log-level 1082
tunnel-guard server-port 1083
use tunnel-guard filter 1085

use tunnel-guard policy 1087
Ethernet configuration commands 1089

arp timeout 1090
description 1091
duplex 1092
filter 1094
interface fastethernet 1095
interface gigabitethernet 1097
mac-pause 1099
mac-pause threshold 1100
mac-pause ticks 1101
mtu 1102
public 1104
service dhcp enable 1106
show interface fastethernet 1107
show interface gigabitethernet 1110
shutdown 1111
speed 1113
tcp-mss 1114
tcp-mss enable 1116
802.1Q VLAN configuration commands 1119

description 1121
dot1q enable 1122
dot1q interface untag egress 1124
dot1q interface untag ingress 1125
dot1q interface vlan-id 1127
encapsulation dot1q 1129
filter 1130
ip address 1132
ip address dhcp 1134
ip address type 1136
ip ospf 1138
ip rip 1140
ip vrrp 1141

ip vrrp backup 1142
ip vrrp backup enable 1144
ip vrrp backup disable 1145
ip vrrp master 1146
rule (Firewall Policy Configuration) 1147
show dot1q 1151
show dot1q statistics 1153
subinterface 1154
subinterface enable 1156
Configuration example 1158
IP interface configuration commands 1159

ip address 1160
ip multicast-relay boundary 1161
ip ospf 1163
ip ospf authentication-key 1165
ip ospf cost 1166
ip ospf dead-interval 1168
ip ospf hello-interval 1169
ip ospf message-digest-key 1171
ip ospf network 1172
ip ospf poll-interval 1174
ip ospf priority 1175
ip ospf retransmit-interval 1177
ip ospf transmit-delay 1178
ip rip 1180
ip rip authentication mode 1181
ip rip cost 1183
ip rip export-bgp-metric 1185
ip rip export-bo-static-metric 1186
ip rip export-default-metric 1187
ip rip export-ospf-metric 1189
ip rip export-static-metric 1190
ip rip import-default 1192
ip rip poison-reverse 1194
ip rip receive version 1195

ip rip send version 1197
ip vrrp 1198
ip vrrp backup 1200
ip vrrp backup disable 1201
ip vrrp backup enable 1203
ip vrrp master 1204
show ip int 1205
Circuitless IP interface configuration commands 1207

clip enable 1208
clip ip 1209
clip ip interface-type 1211
clip ip services 1213
clip ip state 1215
show clip 1216
show clip services 1218
PPP over Ethernet configuration commands 1221

debug interface fastethernet pppoe 1222
interface 1223
pppoe admin-state enable 1224
pppoe cost 1226
pppoe enable 1228
pppoe idle-timeout 1229
pppoe ip local 1231
pppoe ip tcp adjust-mss enable 1233
pppoe on-demand enable 1234
pppoe ppp authentication 1236
pppoe ppp ipcp vj-connect-id-compression-negotiation 1238
pppoe ppp ipcp vj-max-slots 1239
pppoe ppp ipcp vj-negotiation 1241
pppoe ppp lcp echo-fault-threshold 1242
pppoe ppp lcp echo-interval 1243
pppoe ppp lcp protocol-field-compression 1245
pppoe ppp username 1246
pppoe service-name 1248

show interface pppoe 1249
PPPoE configuration example 1252
Dial serial port commands 1253

auto-answer 1254
baud-rate 1255
connect 1256
dial-prefix-string 1258
interface dial 1260
interface dial enable 1261
menu-access-level 1263
microcode 1264
microcode reload 1266
mode 1267
modem-command-string 1269
modem-initialization-string 1271
modem-termination-string 1272
phone 1274
reset 1276
serial-port baud-rate 1277
serial-port mode 1279
show interface dial 1281
show interface dial statistics 1283
show microcode 1285
shutdown 1286
ISDN BRI configuration commands 1289

connect 1290
interface bri 1292
interface bri enable 1293
interface bri isdn calls-per-tei 1295
isdn auto-answer 1296
isdn auto-spid-detection enable 1298
isdn auto-switch-detect 1299
isdn bandwidth-monitor enable 1301
isdn country-code 1303

isdn manual-tei 1305
isdn microcode 1306
isdn not-end-to-end 1308
isdn phone 1309
isdn public 1311
isdn spid1 1312
isdn spid2 1314
isdn switch-type 1316
line-power-detection enable 1318
microcode reload bri 1320
reset 1322
show interface bri 1323
show interface bri statistics 1326
show microcode bri 1328
shutdown 1330

ADSL and ATM configuration commands 1333

circuit-id 1334
controller atm 1335
debug atm 1337
description (interface) 1339
description (subinterface) 1340
dsl operating-mode 1342
encapsulation 1344
filter 1346
interface atm 1348
ip local 1349
ip local address-type 1352
ip remote 1353
ip remote address-type 1355
mac-crc-included 1357
public 1359
show dsl interface atm 1360
show interface atm 1362
show interface atm statistics 1364
shutdown (interface) 1367

shutdown (subinterface) 1368
subinterface 1370
virtual-circuit 1371
PPP configuration commands 1375

circuit-id 1377
description 1378
encapsulation 1380
filter 1381
interface 1383
ppp authentication chap 1384
ppp authentication pap 1386
ppp ip default-route 1388
ppp ip local (ATM subinterfaces) 1390
ppp ip local (dial interfaces) 1392
ppp ip local (serial interfaces) 1394
ppp ip ospf 1396
ppp ip primary-dns-obtain enable 1398
ppp ip remote (ATM subinterfaces) 1399
ppp ip remote (dial interfaces) 1401
ppp ip remote (serial interfaces) 1403
ppp ip rip 1405
ppp ip secondary-dns-obtain enable 1407
ppp ipcp vj-connect-id-compression-negotiation 1408
ppp ipcp vj-max-slots 1410
ppp ipcp vj-negotiation 1412
ppp lcp address-control-field-compression 1413
ppp lcp echo-fault-threshold 1415
ppp lcp echo-interval 1417
ppp lcp protocol-field-compression 1418
ppp lcp-ncp interface-debug 1420
ppp local authentication chap 1422
ppp local authentication pap 1424
ppp local password 1426
ppp local username 1428
ppp multilink high-threshold-duration 1430

ppp multilink high-threshold-percent 1431
ppp multilink incoming enable 1433
ppp multilink low-minimum-duration 1435
ppp multilink low-threshold-duration 1437
ppp multilink low-threshold-percent 1439
ppp multilink minimum-links 1440
ppp multilink outgoing enable 1442
ppp password 1444
ppp public 1446
ppp remote authentication pap 1447
ppp remote password 1449
ppp remote username 1451
ppp username 1453
show interface serial 1455
show interface serial ppp 1456
show interface serial statistics 1458

T1 and E1 CSU/DSU commands 1463

clock source 1464
controller 1466
framing 1468
invert data 1469
line-buildout 1471
linecode 1472
performance-report-message 1474
show controller 1476
timeslot 1478
tx-ringsize 1480

Frame relay commands 1483

class 1484
cost 1485
description 1487
dlci 1489
encapsulation (interface) 1490
encapsulation (subinterface) 1492

fragment 1494
frame-relay bc 1495
frame-relay be 1496
frame-relay cir 1498
frame-relay connection-type 1499
frame-relay debug 1501
frame-relay lmi-n391dte 1503
frame-relay lmi-t391dte 1504
frame-relay lmi-type 1506
frame-relay subinterface 1507
interleave 1510
interface 1511
inverse-arp 1513
ip local 1514
ip ospf 1516
ip remote 1518
ip rip 1519
map-class frame-relay 1521
payload-compress frf9 1522
priority 1524
public 1526
show frame-relay lmi 1527
show frame-relay pvc 1529
traffic-shape rate 1532

Demand Services configuration commands 1535

dial 1536
demand 1538
demand add 1539
demand delay 1540
demand enable 1541
exit 1542
hours name 1543
interface 1546
interface-group 1548
ping 1549

priority 1551
redial 1553
remote-network 1555
route-unreachable 1557
show demand 1558
timeout 1560
trigger 1561
wait 1564
Router RIP configuration commands 1567

distribute-list 1567
network 1570
redistribute 1571
router rip 1573
show ip rip 1574
show ip rip database 1575
show ip rip interface 1576
show ip rip redistribution 1578
timers basic 1579
RIP configuration example 1580
Router VRRP configuration commands 1581

activate 1581
critical-interface-group 1584
interface group 1586
network 1588
respond-icmp 1589
router vrrp 1590
show critical-interface 1591
show interface groups 1592
show ip vrrp 1594
show run routing vrrp 1596
Router OSPF configuration commands. 1599

area 1600
asbr 1602

auto-vlink 1604
compat-3-6 1605
distribute-list 1607
external-metric 1609
network 1610
redistribute 1612
router-id 1613
router ospf 1615
show ip ospf 1616
show ip ospf border-routers 1618
show ip ospf database 1619
show ip ospf interface 1620
show ip ospf neighbor 1621
show ip ospf virtual-links 1623

IPX configuration commands 1625

disable 1625
enable 1626
ipx public-network-address 1628
ipx interface 1630
network 1632

Routing table configuration commands 1635

copy ip ospf-lsdb-table 1635
copy ip route-table 1636
show ip route 1638

CAR configuration commands 1643

aggregation 1644
router car 1646
show router car 1647
threshold 1649

Equal-cost multipath configuration commands 1651

ip load-sharing 1651
maximum-paths 1653
ospf maximum-paths 1654

rip maximum-paths 1655
show ecmp 1657
DHCP relay configuration commands 1659

ip dhcp-relay 1659
ip forward-protocol dhcp-relay 1661
ip helper-address 1662
show dhcp-relay config 1663
show dhcp-relay config interface 1664
show dhcp-relay config statistics 1665
Multicast relay configuration commands 1667

multicast-boundary interface 1668
multicast-relay congestion-threshold 1670
multicast-relay enable 1672
show multicast-relay 1673
show multicast-relay status interfaces 1675
show multicast-relay status statistics 1676
IGMP configuration commands 1679

access-filter 1680
clear ip igmp statistics 1683
ip igmp proxy-type 1685
ip igmp enable 1687
last-member-query-int 1690
query-interval 1693
query-max-resp 1696
query-timeout 1699
robustval 1702
show ip igmp groups 1705
show ip igmp groups interface 1707
show ip igmp interface 1709
show ip igmp statistics 1711
show ip igmp statistics interface 1713
show running-config for igmp routing 1715
snmp-server mib igmp 1717

snmp-server enable traps service igmp 1718
static members 1720
unsolicited-report-interval 1722
Static routing configuration commands 1725

ip default-network 1726
ip default-route-preference 1727
ip route 1729
router static 1731
show ip default-route-preference 1732
show ip static 1734
Access list/route policy configuration commands 1737

access-list permit/deny 1737
route-policy enable/disable 1739
Packet capture (PCAP) commands 1741

buffersize 1742
capture 1743
capture add 1745
capture-all 1747
capture enable 1748
capture save 1751
capture start 1752
capture stop 1754
clear capture 1756
direction 1757
filepath 1759
filesize 1761
filter 1762
length 1765
maxfiles 1766
persistent 1768
promiscuous 1770
remoteip 1771
show capture 1773

trigger 1777
type 1779
userid 1782
wrapping 1784

Quality of service (QoS) commands 1787

add-rule 1789
destination-address 1790
diffserv-marking 1792
dscp-values 1794
move-rule 1795
protocol 1797
qos admission-control 1799
qos bandwidth-management 1801
qos bandwidth-rates 1802
qos egress-dscp-map enable 1804
qos egress-queuing-mode 1806
qos egress-traffic-conditioning 1808
qos ingress-dscp-map enable 1810
qos ingress-traffic-conditioning 1812
qos mf-class (Interface Configuration) 1815
qos mf-class (Global Configuration) 1817
qos mf-class add 1818
qos mf-class enable 1820
qos mf-class rule 1821
qos mf-class rule add 1823
qos non-tunnel-traffic-ratio 1824
qos over-subscription-ratio 1827
qos shaping 1829
qos shaping-state enable 1831
qos statistics reset 1832
qos traffic-conditioning enable 1834
remove-rule 1836
show qos admission-control 1837
show qos bandwidth-management 1838
show qos bandwidth-rates 1840

show qos interfaces 1841
show qos mf-class 1843
show qos statistics 1845
show rules 1849
source-address 1850
tcp-udp-destination-port 1852
tcp-udp-source-port 1855
use destination_address 1857
use diffserv_marking 1858
use dscp 1860
use protocol 1862
use source_address 1864
use tcp_udp_destination_port 1866
use tcp_udp_source_port 1868

DLSw configuration commands 1871

Global configuration mode commands 1874
dlsw clear circuit 1875
dlsw clear mac-cache 1876
dlsw local-peer 1878
dlsw local-peer backlevel-flowcontrol 1879
dlsw local-peer enable 1881
dlsw local-peer mac-cache 1882
dlsw local-peer mac-translation 1883
dlsw local-peer unconfigured-peer enable 1884
dlsw mac-translation 1885
dlsw remote-peer 1886
dlsw remote-peer backup 1887
dlsw remote-peer backup-peer holdtime backuptime 1888
dlsw remote-peer circuit-inactivity 1890
dlsw remote-peer cost 1891
dlsw remote-peer enable 1892
dlsw remote-peer receive-initial-pacing 1893
dlsw remote-peer rfc1795 1895
dlsw timer circuit-ack-timeout 1896
dlsw timer explorer-delay 1897

dlsw timer explorer-timeout 1898
dlsw timer explorer-wait-timeout 1899
dlsw timer idle-timeout 1900
dlsw timer tcp-connect-retry 1901
dlsw timer test-timeout 1902
LAN interface configuration commands 1904
llc2 ack-delay-time 1904
llc2 busy-time 1906
llc2 enable 1907
llc2 idle-time 1909
llc2 lantype 1910
llc2 max-received-window 1911
llc2 max-retry 1912
llc2 lpf-time 1913
llc2 rej-time 1914
llc2 t2timeout 1916
SDLC and Link Station configuration commands 1917
clock-type 1918
counter disconnect 1920
counter fast-contact 1921
counter fast-poll 1922
counter no-response 1923
counter remote-busy 1924
counter slow-contact 1925
counter slow-poll 1926
enable 1927
encapsulation sdlc 1928
grouppoll 1930
line-encoding 1931
line-speed 1932
lmac lsap 1933
pollframe 1934
proxy-xid 1935
recvwindow 1936
rmac rsap 1937

sdlc activation-sequence 1938
sdlc counter idle-time 1940
sdlc counter non-productive 1941
sdlc counter write-port 1942
sdlc debug 1944
sdlc interframe-fill enable 1945
sdlc link-station polladdress 1946
sdlc max-received-window 1947
sdlc polladdress 1948
sdlc primary-full-duplex 1949
sdlc role 1950
sdlc secondary-full-duplex 1952
sdlc send-rej 1953
sdlc timer idle-time 1954
sdlc timer non-productive 1955
sdlc timer write-port 1956
sendwindow 1958
start 1959
stop 1961
timer disconnect 1962
timer fast-contact 1963
timer fast-poll 1964
timer no-response 1965
timer rnr-limit 1966
timer slow-contact 1968
timer slow-poll 1969
timer turn-around 1970
Privileged exec mode commands 1971
show dlsw capabilities 1971
show dlsw circuits 1973
show dlsw directory 1975
show dlsw mac-table 1977
show dlsw peers 1978
show dlsw port 1981
show dlsw sdlc 1984

Debug mode commands 1986
dlsw debug_level 1986
dlsw ips-trace enable 1988
tx-ringsize 1989
Digital Data Service (DDS) configuration commands 1991

clock rate 1992
clock source 1994
controller 56k 1996
show controller 56k 1998
transmit-data-monitor 2000
BGP configuration commands 2003

auto-summary 2005
bgp always-compare-med 2007
bgp client-to-client reflection 2008
bgp cluster-id 2010
bgp default local-preference 2011
bgp multiple-paths 2013
bgp public 2014
bgp redistribute-internal 2015
bgp router-id 2017
default-information originate 2018
default-metric 2020
ip as-path access-list 2021
ip community-list 2024
match as-path 2026
match community 2028
match ip address 2030
multiple-paths 2032
neighbor 2033
neighbor advertisement-interval 2034
neighbor allow-as-in 2036
neighbor default-originate 2037
neighbor distribute-list 2039
neighbor ebgp-multihop 2041

neighbor enable 2042
neighbor filter-list 2043
neighbor next-hop-self 2045
neighbor loop-detection 2047
neighbor password 2048
neighbor remote-as 2050
neighbor retry-interval 2051
neighbor route-map 2053
neighbor route-reflector-client 2055
neighbor send-community 2056
neighbor shutdown 2058
neighbor update-source 2059
neighbor timers 2061
neighbor weight 2062
network 2065
redistribute 2066
route-map 2068
route-reflector enable 2070
router bgp 2071
set as-path 2073
set community 2075
set ip next-hop 2078
set local-preference 2079
set metric 2080
set origin 2081
set weight 2083
show ip as-path access-list 2084
show ip bgp 2085
show ip bgp community 2088
show ip bgp neighbors 2089
show ip bgp networks 2094
show ip bgp redistribution 2095
show ip bgp redistribute-routes 2096
show ip bgp regexp 2098
show ip bgp summary 2099

show ip community-list 2102
show ip route-map 2103
synchronization 2104
timers bgp 2105

Sample scripts and output files generated by the show running-config command 2109

Example 1: Add networks, domains, access hours, and groups 2110
Example 2: Add users to a group 2112
Example 3: Add branch office connections 2115
Example 4: Configure group properties 2117

Using the bulk load commands 2139

bulk load command 2139
file_format command 2141
User commands 2142
Branch office commands 2146
Nortel VPN Router configuration commands 2152
Network definition commands 2152
NAT commands 2153
Address pool commands 2154
Filter commands 2155
Automatic backup commands 2157
SYSLOG forwarding commands 2158
SNMP commands 2158
DHCP commands 2160
Licensing commands 2161
Usage notes 2161

Index 2163

Tables

Table 1 Configuration modes described 65
Table 2 Configuration modes, prompts, and access commands 67
Table 3 Nortel Networks CLI (NNCLI) key combinations 69
Table 4 copy command results 109
Table 5 Restricted mode commands 190
Table 6 Configuration file dependencies 256
Table 7 Provisioning time estimates 259
Table 8 Default MTU by interface 1105
Table 9 ISDN country codes and switch types 1305
Table 10 TCP/UDP port names and addresses 1809
Table 11 DSCP values for rules 1816
Table 12 show ip bgp field descriptions 2045
Table 13 *show ip bgp neighbors* field descriptions 2049
Table 14 show **ip bgp neighbors** advertised-routes and routes field descriptions 2051
Table 15 *show ip bgp summary* field descriptions 2059

Preface

This guide describes the commands that you can execute using the Nortel VPN Router command line interface (CLI). Throughout this guide, the Nortel VPN Router is referred to as the gateway.

Before you begin

This guide is for network managers who are responsible for the configuration, management, and maintenance of the Nortel VPN Router. This guide is based on the assumption that you have experience with command line interfaces and are familiar with network management.

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicates that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. Example: If the command syntax is **ping** <*ip_address*>, you enter **ping 192.32.10.12**
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the **show health** command. Example: Enter **terminal paging** {**off** | **on**}.

braces ({})	Indicates required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when you enter the command. Example: If the command syntax is **`ldap-server source {external | internal}`**, you must enter either **`ldap-server source external`** or **`ldap-server source internal`**, but not both.
brackets ([ ])	Indicates optional elements in syntax descriptions. Do not type the brackets when you enter the command. Example: If the command syntax is **`show ntp [associations]`**, you can enter either **`show ntp`** or **`show ntp associations`**. Example: If the command syntax is **`default rsvp`** [**`token-bucket`** {**`depth | rate`**}], you can enter **`default rsvp`**, **`default rsvp token-bucket depth`**, or **`default rsvp token-bucket rate`**.
ellipsis points (. . .)	Indicates that you repeat the last element of the command as needed. Example: If the command syntax is **`more disk`***`n`*`:<`*`directory`*`>/...<`*`file_name`*`>`, you enter **`more`** and the fully qualified name of the file.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, an underscore connects the words are connected by an underscore. Example: If the command syntax is **`ping`** <*`ip_address`*>, *`ip_address`* is one variable and you substitute one value for it.
`plain Courier text`	Indicates system output, for example, prompts and system messages. Example: `File not found.`
separator (>)	Shows menu paths. Example: Choose Status > Health Check.

vertical line (|)	Separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. Example: If the command syntax is **`terminal paging {off | on}`**, you enter either **`terminal paging off`** or **`terminal paging on`**, but not both.

Related publications

For more information about the Nortel VPN Router, see the following publications:

- Release notes provide the most recent information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Nortel VPN Router Configuration — Client* (NN46110-306) provides information to install and configure client software for the Nortel VPN Router.
- *Nortel VPN Router Configuration — TunnelGuard* (NN46110-307) provides information to configure and use the TunnelGuard feature.
- *Nortel VPN Router Upgrades — Server Software Release 8.0* (NN46110-407) provides information to upgrade the server software to the most recent release.
- *Nortel VPN Router Installation and Upgrade — Client Software Release 8.01* (NN46110-409) provides information to upgrade the Nortel VPN Client to the most recent release.
- *Nortel VPN Router Configuration — Basic Features* (NN46110-500) introduces the product and provides information about initial setup and configuration.
- *Nortel VPN Router Configuration — SSL VPN Services* (NN46110-501) provides instructions to configure services on the SSL VPN Module 1000, including authentication, networks, user groups, and portal links.
- *Nortel VPN Router Configuration — Advanced Features* (NN46110-502) provides configuration information for advanced features such as the Point-to-Point Protocol (PPP), Frame Relay, and interoperability with other vendors.
- *Nortel VPN Router Configuration — Tunneling Protocols* (NN46110-503) provides configuration information for the tunneling protocols IPsec, Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Forwarding (L2F).
- *Nortel VPN Router Configuration — Routing* (NN46110-504) provides instructions to configure the Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP), Equal Cost Multipath (ECMP), routing policy services, and client address redistribution (CAR).

- *Nortel VPN Router Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508) provides instructions to configure the Stateful Firewall and Nortel VPN Router interface and tunnel filters.
- *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600) provides instructions to configure authentication services and digital certificates.
- *Nortel VPN Router Troubleshooting — Server* (NN46110-602) provides information about system administrator tasks such as recovery and instructions to monitor VPN Router status and performance. This document provides troubleshooting information and event log messages.
- *Nortel VPN Router Administration* (NN46110-603) provides information about system administrator tasks such as backups, file management, serial connections, initial passwords, and general network management functions.
- *Nortel VPN Router Troubleshooting — Client* (NN46110-700) provides information to troubleshoot installation and connectivity problems with the Nortel VPN Client.

Printed technical manuals

To print selected technical manuals and release notes for free, directly from the Internet, go to www.nortel.com/documentation, find the product for which you need documentation, and then locate the specific category and model or version for the hardware or software product. Use Adobe Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems Web site at www.adobe.com to download a free copy of the Adobe Reader.

How to get help

This section explains how to get help for Nortel products and services.

Finding the most recent updates on the Nortel Web site

The content of this documentation was current at the time the product was released. To check for updates to the most recent documentation and software for Nortel VPN Router, click one of the following links.

Link	Web site
Most recent software	Nortel page for **VPN Router** software located at support.nortel.com/go/main.jsp?cscat=SOFTWARE&poid=12325
Most recent documentation	Nortel page for **VPN Router** documentation located at support.nortel.com/go/main.jsp?cscat=DOCUMENTATION&poid=12325

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can perform the following activities:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to the following Web site:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

New in this release

The following sections detail what's new in *Nortel VPN Router Using the Command Line Interface* (NN46110-507) for Release 8.0:

- "Features" on page 53

Features

The following table identifies new commands or command changes.

Table 1 New feature commands

Command	Purpose or change	Details
`authentication`	Specify dual authentication methods for IPsec groups.	"authentication (Group IPsec Tunnel)" on page 293
`authentication external, no authentication external`	Added the **`passgo-defender`** parameter	"authentication (Group IPsec Tunnel)" on page 293
`authentication-banner`	Configures the authentication banner message.	"authentication-banner" on page 181
`crl http`	Configures the HTTP CRL server	"crl http" on page 919
`ftp access-list`	Configures FTP access list settings	"ftp access-list" on page 194
`https access-list`	Configures HTTPS access list settings	"https access-list" on page 204
`ip address-pool` and **`ip address-src`**	Modifies how you assign IP addresses through local address pools or DHCP	"ip address-pool" on page 542 and "ip address-src" on page 362
`ip igmp and related commands`	Configures IGMP	"IGMP configuration commands" on page 1679

Table 1 New feature commands

Command	Purpose or change	Details
ipsec authentication	Configure dual authentication for IPsec tunnels.	"ipsec authentication" on page 493
ipsec nat-traversal-bo	Enable or disable IPsec NAT Traversal for branch office tunnels.	"ipsec nat-traversal-bo" on page 697
key and **set key-size**	Increases the allowable size of a certificate from 2048 bits to 4096 bits.	"key" on page 950 and "set key-size" on page 968
nat-traversal	Configure IPsec NAT Traversal on branch office tunnels.	"nat-traversal" on page 1006
ocsp	Configures the OCSP status check feature	"ocsp" on page 960
radius-server authentication	Added the **passgo-defender** parameter	"radius-server authentication" on page 758
ssh-server access-list	Configure SSH server access-list settings	"ssh-server access-list" on page 227

Chapter 1
Introduction

This chapter introduces the Nortel VPN Router command line interface (CLI).

Topic	Page
Accessing the CLI	56
Command modes	57
Configuration modes	59
Editing command line entries	64
Using command abbreviations	65
Using CLI online Help	66

Accessing the CLI

You can access the CLI over a Telnet session or through the serial port menu.

Access from a Telnet session

To access the CLI via a Telnet connection, Telnet must be enabled on the VPN Router. If you need to enable the Telnet management protocol, go to the Services > Available screen. To access the Nortel VPN Router CLI:

1. Start a Telnet session to the VPN Router management IP address, for example:

   `telnet 10.0.16.247`

2. Log in to the VPN Router using an account with administrator privileges, for example:

   ```
   Login: admin
   Password:<password>
   CES>
   ```

When you log in, the CLI prompt (`CES>`) appears, indicating that you are in CLI User EXEC mode. You can execute any User EXEC mode command or change the command mode to execute other commands.



Note: You can change the text "`CES`" in the default CLI prompt (see the description of the **`prompt`** command on page 220).

Access from the serial port menu

If you have a serial port connection to the VPN Router, you can access the CLI through the serial port menu. Select **L** from the serial port menu (shown below) to access the CLI.

```
Main Menu: System is currently in NORMAL mode.

   1) Interfaces
   2) Administrator
   3) Default Private Route Menu
   4) Default Public Route Menu
   5) Create A User Control Tunnel(IPsec) Profile
   6) Restricted Management Mode FALSE
   7) Allow HTTP Management TRUE
   8) Firewall Options
   9) Shutdown
   B) System Boot Options
   P) Configure Serial Port
   C) Controlled Crash
   L) Command Line Interface
   R) Reset System to Factory Defaults
   E) Exit, Save and Invoke Changes

   Please select a menu choice (1 - 9,B,P,C,L,R,E):_
```



Note: To provision a Nortel VPN Router Secure IP Services Gateway that has been reset to factory defaults with a file produced by the CLI command **`show running-config`**, the Nortel VPN Router must have an assigned IP management address and must have the FTP management protocol enabled on the Services > Available screen.

Command modes

The Nortel VPN Router CLI has three main command modes:

- User EXEC mode
- Privileged EXEC mode
- Global Configuration mode

User EXEC mode

When you first establish a CLI session to the VPN Router, you enter User EXEC mode. User EXEC mode is a limited display mode. You cannot modify configuration parameters or view the configuration file in this mode; however, you can clear a route.

The User EXEC mode prompt is:

```
CES>
```



Note: You can change the text "CES" in the default CLI prompt (see the description of the **prompt** command on page 220).

Privileged EXEC mode

To access Privileged EXEC mode from User EXEC mode, enter the **enable** command and the administrator password. To exit Privileged EXEC mode and return to User EXEC mode, use the **disable** or **exit** command. To leave User EXEC mode and exit the Telnet session or return to the serial port menu, you must enter **exit**.

Privileged EXEC mode is a full display and configuration mode; it supports additional commands not supported in User EXEC mode. Privileged EXEC mode commands are typically one-time commands, for example, **show** commands. You can execute User EXEC mode commands in Privileged EXEC mode.

The Privileged EXEC mode prompt is:

```
CES#
```



Note: You can change the text "CES" in the default CLI prompt (see the description of the **prompt** command on page 220).

Global Configuration mode

Global Configuration mode allows you to make changes to the VPN Router running configuration. These changes are saved across reboots. You enter Global Configuration mode from Privileged EXEC mode using the **`configure terminal`** command. The Global Configuration mode prompt is:

```
CES(config)#
```



Note: You can change the text "`CES`" in the default CLI prompt (see the description of the **`prompt`** command on page 220).



Important!! The normal terminators, the EXIT or END commands, accept and execute all deferred commands. The abort termination (Ctrl-Z or <end-of-file>), however, discards and *does not* execute deferred commands.

To leave Global Configuration mode and return to Privileged EXEC mode, enter **`exit`**, **`end`**, or Ctrl-z.

Configuration modes

From Global Configuration mode, you can access other configuration modes, such as LDAP, Firewall Policy, and NAT Policy Configuration modes. The following table lists the configuration modes:

Table 2 Configuration modes described

Mode	Description
Branch Office Connection Configuration	Branch office tunnel configuration commands
Branch Office Connection Control Tunnel Configuration	Branch office control tunnel configuration commands
Branch Office Group IGMP Configuration	Branch office group connectivity configuration commands
Branch Office Group IPsec Configuration	Branch office group IPsec configuration commands

Table 2 Configuration modes described

Mode	Description
Branch Office Group OSPF Configuration	Branch office group OSPF configuration commands
Branch Office Group RIP Configuration	Branch office group RIP configuration commands
Branch Office Static Routing Configuration	Branch office tunnel routing configuration commands
CA Configuration	CA certificate configuration commands
Capture Configuration	Packet capture configuration commands
Certificate Request Configuration	Certificate request configuration commands
Controller Configuration	ATM or T1/E1 controller configuration commands
Crypto CA Identity Configuration	CMP configuration commands
Crypto Server Certificate Configuration	Server certificate configuration commands
Demand Services Configuration	Demand services configuration commands
Filter Interface Configuration	Filter interface configuration mode commands
Filter Rule Configuration	Filter rule configuration commands
Filter Tunnel Configuration	Filter tunnel configuration mode commands
Group Connectivity Configuration	User group configuration commands
Group IGMP Configuration	Group IGMP configuration commands
Group IPsec Configuration	User group IPsec configuration commands
Group L2F Configuration	User group L2F configuration commands
Group L2TP Configuration	User group L2TP configuration commands
Group PPTP Configuration	User group PPTP configuration commands
Interface Configuration	Interface configuration commands
IPX Interface Configuration	IPX LAN interface configuration commands
QoS MF Classifier Configuration	QoS classifier configuration commands
QoS Rule Configuration	QoS classifier rule configuration commands
Router CAR Configuration	Routing client address redistribution configuration commands
Router OSPF Configuration	Routing OSPF configuration commands

Table 2 Configuration modes described

Mode	Description
Router RIP Configuration	Routing RIP configuration commands
Router VRRP Configuration	Routing VRRP configuration commands
Subinterface Configuration	802.1Q, ATM, and frame relay subinterface configuration commands
User Configuration	User configuration commands

The following table lists configuration modes, commands that navigate to that configuration mode, and their default prompts. If the initial command mode is not provided, you execute the command at the Global Configuration mode prompt.

Table 3 Configuration modes, prompts, and access commands

Configuration mode	Access command	Prompt
Global Configuration	Enter the command **configure terminal** at the Privileged EXEC mode prompt.	CES(config)#
Group IGMP Configuration	Enter the command **group igmp <group-name>.**	CES(config-group/igmp)#
Firewall Policy Configuration	Enter the command **policy security**.	CES(config-fwpolicy)#
NAT Policy Configuration	Enter the command **policy nat**.	CES(config-natpolicy)#
Policy Object Configuration	Enter the command **policy object**	CES(config-policyobj)#
Group IPsec Configuration	Enter the command **group ipsec**.	CES(config-group/ipsec)#
Group L2F Configuration	Enter the command **group l2f**.	CES(config-group/l2f)#
Group L2TP Configuration	Enter the command **group l2tp**.	CES(config-group/l2tp)#
Group PPTP Configuration	Enter the command **group pptp**.	CES(config-group/pptp)#
Group Connectivity Configuration	Enter the command **group connectivity**.	CES(config-group/con)#
Branch Office Group IPsec Configuration	Enter the command **bo-group ipsec**.	CES(config-bo_group/ ipsec)#
Branch Office Group Connectivity Configuration	Enter the command **bo-group connectivity**.	CES(config-bo_group/ con)#
Branch Office Connection Configuration	Enter the command **bo-conn**.	CES(config/bo_conn)#

Table 3 Configuration modes, prompts, and access commands (Continued)

Configuration mode	Access command	Prompt
Branch Office Group IGMP Configuration	Enter the command **bo-group igmp <group-name>.**	CES(config/bo-group/ igmp#
Branch Office Group OSPF Configuration	Enter the command **bo-group ospf**.	CES(config-bo_group/ ospf)#
Branch Office Group RIP Configuration	Enter the command **bo-group rip**.	CES(config-bo_group/ rip)#
Branch Office Connection Control Tunnel Configuration	Enter the command **bo-conn**.	CES(config/bo_conn)#
Branch Office Static Routing Configuration	Enter the command **routing static** in Branch Office Connection Configuration mode.	CES(config/bo_conn/ routing_static)#
Demand Services Configuration	Enter the command **demand** in Demand Services Configuration mode.	CES(config/demand)#
User Configuration	Enter the command **user**.	CES(config-user)#
Filter Tunnel Configuration	Enter the command **filter tunnel**.	CES(config-filter)#
Filter Rule Configuration	Enter the command **filter** {**tunnel** | **interface**} rule.	CES(config/rule)#
Filter Interface Configuration	Enter the command **filter interface**.	CES(config-filter)#
Interface Configuration	Enter the command **interface**.	CES(config-if)#
Subinterface Configuration	Enter the command **subinterface**.	CES(config-subif)#
DHCP Pool Configuration	Enter the command **ip dhcp server pool**.	CES(config-dhcp)#
IPX Interface Configuration	Enter the command **ipx interface**.	CES(config-ipx)#
Router CAR Configuration	Enter the command **router car**.	CES(config-car)#
Router OSPF Configuration	Enter the command **router ospf**.	CES(config-ospf)#
Router RIP Configuration	Enter the command **router rip**.	CES(config-rip)#
Router VRRP Configuration	Enter the command **router vrrp**.	CES(config-vrrp)#
Crypto CA Configuration	Enter the command **crypto ca configure** <*subject dn*>.	CES(config-ca)#
Crypto CA Identity Configuration	Enter the command **crypto ca identity**.	CES(ca-identity)#

Table 3 Configuration modes, prompts, and access commands (Continued)

Configuration mode	Access command	Prompt
Crypto Server Certificate Configuration	Enter the command **crypto server configure**.	CES(config-servercert)#
Certificate Request Configuration	Enter the command **crypto server request**.	CES(config-request)#
QoS MF Classifier Configuration	Enter the command **qos mf-class**.	CES(config-mfclass)#
QoS Rule Configuration	Enter the command **qos mf-class rule**.	CES(config-mfrule)#
Capture Configuration	Enter the command **capture** *object*.	CES(capture-*type*)#
Controller Configuration	Enter the command **controller**.	CES(config-controller)#

The prompt reflects the current mode and whether the user is privileged or not. If the user is privileged, the last character of the prompt is #. If not, the character is >. Use the **enable** and **disable** commands to switch between privileged and non-privileged modes.

Note: You can change the text "CES" in the default CLI prompt (see the description of the **prompt** command on page 220). However, you cannot change the final character: > or #.

The cursor shows where typed characters will be inserted. You can use the keys described in Table 4 to change the location of the cursor. You can type a line that is longer than the width of the screen. If you do, the line scrolls to the left (sliding window) to allow you to type in more characters. If you move the cursor to the far left, the line scrolls to the right.

The terminal settings control the behavior of the Nortel Networks CLI (NNCLI) parser. You can change the width of the terminal as well as the page length.

Editing command line entries

You can use the Nortel Networks Command Line Interface (NNCLI) editing commands to edit command line text entries. Table 4 describes key combinations that you can use for the CLI.

Table 4 NNCLI key combinations

Key combination	Function
control-A	Move cursor to start of line.
control-B	Move cursor back one character.
control-C	Abort command.
control-D	Delete one character.
control-E	Move cursor to end of line.
control-F	Move cursor forward one character.
control-H &	Delete character left of cursor.
control-I &	Complete command/parameter.
control-K	Delete all characters after cursor.
control-L & control-R	Display line again.
control-N or down arrow	Move to next history command (in the same mode).
control-P or up arrow	Move to previous history command (in the same mode).
control-Q	Escape sequence for unprintable characters.
control-T	Transpose characters.
control-U	Delete entire line.
control-W	Delete word left of cursor.
control-X	Delete all characters before cursor, including character at cursor.
control-z	Exit configuration mode. **Note:** Ctrl-Z discards and *does not* execute deferred commands.
?	Display context-sensitive Help.
esc-c & esc-u	Capitalize character at cursor.
esc-l	Convert character at cursor to lowercase.

Table 4 NNCLI key combinations (Continued)

Key combination	Function
esc-b	Move backward one word.
esc-d	Delete one word to the right.
esc-f	Move forward one word.

Using command abbreviations

When you type CLI commands, you usually do not need to type the entire command or parameter. For example, instead of typing **`show interface`** at the Privileged EXEC prompt, you can type **`sh int`**. You must enter a sufficient number of characters to uniquely identify the command or option.

Using CLI online Help

To obtain Help for a CLI command or option, use the question mark (**?**) command to display the next parameters that you can configure. The following example illustrates how to display syntax and options for the **clip** command that you use to configure circuitless IP services.

```
CES(config)# clip ?
  enable  Enables Circuitless IP globally
  ip      Configures the CLIP address
CES(config)# clip ip ?
  A.B.C.D  CLIP address
CES(config)# clip ip 2.2.2.2 ?
  interface-type  Configures the interface type of the CLIP address
  services        Configures the allowed services for the CLIP address
  state           Configures the state of the CLIP address
  <cr>
CES(config)# clip ip 2.2.2.2 services ?
  fwua      Enables Firewall User Authentication services
  ipsec     Enables IPSEC services
  l2tp&l2f  Enables L2TP and L2F services
  pptp      Enables PPTP services
CES(config)# clip ip 2.2.2.2 services ipsec ?
  both     Enables both public and private
  none     Disables both public and private
  private  Enables only private
  public   Enables only public
CES(config)# clip ip 2.2.2.2 services ipsec both ?
  <cr>
CES(config)#
```

In one situation, you do not see command options when you use the question mark (**?**) command to display Help. When a command is obsoleted, it is usually left in the CLI for customers who use the older command in scripts. The older command still works, but it is not displayed by the parser.

Chapter 2
User EXEC mode commands

This chapter describes the User EXEC CLI commands.

Command	Page
cd	68
clear ip route	69
dir	71
enable	73
exit	74
help	75
ls	76
ping	78
pwd	81
show file systems	82
show flash: contents	83
show reload	85
show services	86
show sessions	88
show version	90
terminal paging	91
trace ip	92
who	94

cd

Use this command to change the default directory or file system.

Syntax

cd <*file_system*>[:]

Parameters

file_system[**:**]	Name of a directory followed by an optional colon. The name can be an absolute path or a relative path. A slash (**/**) can be appended to the end of the path. The root directory (/) is not supported. Valid values include: • **.** • **..** • **/ide0** • **/ide0/** • **system:** • **/ide0/system/:**

Default

None

Command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

% Directory does not exist: <*file_system*>

Related commands

copy
delete
dir
pwd
show file systems

Example

```
CES> pwd
/ide0/
CES> cd /ide0/system:
CES> pwd
/ide0/system/
CES> cd ..
CES> pwd
/ide0/
CES> cd system
CES> pwd
/ide0/system/
CES> cd /
% Directory does not exist: /
```

clear ip route

Use this command to remove a route from the route table. Note that static routes are not removed from the VPN Router browser interface by this command. This command is a troubleshooting tool for use when routing problems are caused by the presence of a wrong route.

Syntax

clear ip route *<address> <mask>*

Parameters

address	The address of the network to remove from the route table.
mask	The mask associated with the address to remove.

Default

The mask defaults to 255.255.255.255.

Command mode

User EXEC

Next command mode

User EXEC

Warning messages

```
% Address not found in route table.
```

Related commands

show ip route

Example

```
CES> clear ip route 10.11.0.12
```

dir

Use this command to display a list of files on a file system.

Syntax

dir [<*file_system*>[:]] [<*file_url*>]

Parameters

file_system[**:**]	Name of a directory followed by an optional colon. The name can be an absolute path or a relative path. A slash (**/**) can be appended to the end of the path. The root directory (/) is not supported. Valid values include: • **.** • **..** • **/ide0** • **/ide0/** • **system:** • **/ide0/system/:**
file_url	Name of the file or files to display. The files can be of any type. You can use wildcards in the file name. The wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Default

The default file system is specified by the **cd** command. If you enter the **dir** command with no arguments, the command displays the contents of the current default directory.

If you enter the **dir** command with two arguments, the command displays files in the specified directory that match the file URL.

If you enter the **dir** command with only one argument, the command determines whether the argument represents a file system or a file URL as follows:

1. If there is a colon at the end of the argument, the argument is a file system. The **dir** command displays the contents of the directory.
2. If the argument is a valid directory, the argument is a file system. The **dir** command displays the contents of the directory.
3. If no colon appears at the end of the argument, and the argument is not a valid directory, then the argument represents a file URL. The **dir** command displays only the files that match the file URL.

Command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Directory does not exist: <directory>
```

Related commands

cd
ls

Example

```
CES> dir
CES> dir sys
CES> dir sys*
CES> dir system
CES> dir system:
CES> dir /ide0/: sys*
CES> dir /ide0 v*
```

enable

Use this command to place the CLI parser into Privileged EXEC mode, allowing you to use additional CLI commands.

You are prompted for a case-sensitive password before you enter Privileged EXEC mode. This password is created when the administrator user account is set up using the VPN Router management pages.

You are allowed three tries to enter the password. After the third incorrect attempt, an error message is displayed (`Bad secrets`) and the User EXEC prompt is redisplayed.

Syntax

`enable`

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

Privileged EXEC

Warning messages

```
% Bad secrets.
```

Related commands

configure
disable

Example

```
CES> enable
Password: *****
CES#
```

exit

Use this command to exit any configuration mode or to close an active Telnet session when you are in User EXEC mode.

Syntax

exit

Parameters

None

Default

None

Command mode

Available in all command modes

Next command mode

Either the lower level command mode, or none because the Telnet session is terminated

Related commands

end

Example

This example shows a user in Global configuration mode using the **exit** command twice to end in User EXEC mode.

```
CES(config)# exit
CES# exit
CES>
```

help

Use this command to display a message about how to use the Help system.

Syntax

help

Parameters

None

Command mode

Available in all command modes

Example

```
CES> help
Help may be requested at any point in a command by entering
a question mark (?). If nothing matches, the Help list will
be empty and you must back up until entering a '?' shows the
available options.
Two styles of Help are provided:
1. Full Help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
   possible argument.
2. Partial help is provided when an abbreviated argument is
   entered and you want to know what arguments match the
   input (e.g. 'show se?').
CES>
```

ls

Use this command to display a list of files on a file system in a compact format.

Syntax

ls [<*file-system*>[:]] [<*file-url*>]

Parameters

file-system[**:**]	Name of a directory followed by an optional colon. The name can be an absolute path or a relative path. A slash (**/**) can be appended to the end of the path. The root directory (/) is not supported. Valid values include: • **.** • **..** • **/ide0** • **/ide0/** • **system:** • **/ide0/system/:**
file-url	Name of the file or files to display. The files can be of any type. You can use wildcards in the file name. The wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Default

The default file system is specified by the **cd** command. If you enter the **ls** command with no arguments, the command displays the contents of the current default directory.

If you enter the **ls** command with two arguments, the command displays files in the specified directory that match the file URL.

If you enter the **ls** command with only one argument, the command determines whether the argument represents a file system or a file URL as follows:

1. If there is a colon at the end of the argument, the argument is a file system. The **ls** command displays the contents of the directory.
2. If the argument is a valid directory, the argument is a file system. The **ls** command displays the contents of the directory.
3. If no colon appears at the end of the argument, and the argument is not a valid directory, then the argument represents a file URL. The **ls** command displays only the files that match the file URL.

Command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Directory does not exist: <directory>
```

Related commands

cd
dir

Example

```
CES> ls
CES> ls sys
CES> ls sys*
CES> ls system
CES> ls system:
CES> ls /ide0/: sys*
CES> ls /ide0 v*
```

ping

Use this command to provide a basic ping facility. By default, it sends three 100-byte ping packets.

Syntax

ping {<*dest_hostname*> | <*dest_address*>} [<*source-address*>] [<*num_packets*>]

Parameters

dest_hostname	Host name of the system to ping.
dest_address	IP address (in dotted-decimal notation) of the system to ping.
source_address	IP address (in dotted-decimal notation) of the interface to ping from.
num_packets	Number of ping packets to send to the destination host.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Warning messages

This message appears if the system cannot map an address to a host name.

```
% Unknown Host
```

Related commands

`trace ip`

Example

This example shows a successful **ping** command.

```
CES> ping 122.104.11.112
PING 122.104.11.112: 36 data bytes
  64 bytes from 122.104.11.112: icmp_seq=0. time= 16 ms
  64 bytes from 122.104.11.112: icmp_seq=1. time=<16 ms
  64 bytes from 122.104.11.112: icmp_seq=2. time=<16 ms
  ----122.104.11.112 PING Statistics----
  3 packets transmitted, 3 packets received, 0% packet loss
  round-trip (ms)  min/avg/max = <16/<16/16
```

This example shows an attempt to ping an unknown host address.

```
CES> ping badaddress.com
  ping: unknown host baddaddress.com
```

This example shows an attempt to ping an unreachable IP address.

```
CES> ping 10.0.4.44
  PING 10.0.4.44: 36 data bytes
  ping: timeout
  no answer from 10.0.4.44
```

This example shows a successful attempt to ping an IP address where the source address is specified and where the number of ping packets to send is 5.

```
CES> ping 47.17.248.158 47.17.248.156 5
PING 47.17.248.158: 36 data bytes
64 bytes from 47.17.248.158: icmp_seq=0. time=<16 ms
64 bytes from 47.17.248.158: icmp_seq=1. time=<16 ms
64 bytes from 47.17.248.158: icmp_seq=2. time=<16 ms
64 bytes from 47.17.248.158: icmp_seq=3. time=<16 ms
64 bytes from 47.17.248.158: icmp_seq=4. time=<16 ms
----47.17.248.158 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = <16/<16/<16
```

pwd

Use this command to show the current setting of the **cd** command.

Syntax

pwd

Parameters

None

Default

None

Command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

cd
dir

Example

```
CES> pwd
/ide0/
```

show file systems

Use this command to display information about the available file systems on the VPN Router, including information about device size and available free space.

Syntax

show file systems

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Example

This example shows the output for a VPN Router that has one hard disk drive:

```
CES> show file systems
 File System(s):
      Size(b)       Free(b)     Type    Flags  Prefixes
      2135040000    695697408   disk       rw    ide0:
```

show flash: contents

Use this command to display the current settings that are in flash on the VPN Router.

Syntax

show flash: contents

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Related commands

show version

Next command mode

User EXEC

Example

This example shows the flash settings for a Nortel VPN Router device. The output will differ, depending on the type of Nortel VPN Router device being used.

```
CES> show flash: contents

Flash Header - copyright: Nortel Networks, Copyright 1999,
2000
               tag:       NOC
               version:   1
               length:    711
               count:     15
Flash Data -
model number: CES1510D
MAC address: 00-E0-7B-00-0D-30
serial number: 12192
feature keys:
     Maximum Ethernet ports: 2
     Maximum T-1 ports: 1
     Maximum T-3 ports: 0
     Allow PPTP tunnels: True
     Allow L2F tunnels: True
     Allow L2TP tunnels: True
     Allow IPsec tunnels: True
     Allow QoS internal: True
     Allow QoS admission: True
     Allow RSVP: True
     Allow RADIUS authentication: True
     Allow LDAP authentication: True
     Allow NT Domain authentication: True
     Allow RSA encryption: True
     Allow SSL: True
     Allow X.509 certificates: True
     Allow RADIUS accounting: True
     CPU clock rate 400 MHz
     CPU cache size 0 KB
     Number of CPUs supported: 1
     Allow IPX: True
     Allow NAT: True
     Allow FW-1: True
     Require FW-1: False
     Firewall: Disabled
```

```
     Maximum Hifn 7751 Accelerators: 0
     FIPS Mode: False
     Allow Safe Mode Boot: False
feature mask
Flash Revision: 1
key length: 128
Boot Device: /ide0/
maximum concurrent sessions: 100
system IP address: 10.211.4.42
system IP netmask: 255.255.0.0
system default VPN Router: 10.0.0.10
checksum: 56091
```

show reload

Use this command to display information about any pending shutdowns that are scheduled on the VPN Router. The same information is available on the Admin->Shutdown and the Status -> System Web management pages.

Syntax

show reload

Parameters

None

Command mode

User EXEC

Next command mode

User EXEC

Related commands

reload
reload at
reload cancel
reload in
reload no-sessions

Example

This example shows information about the pending reload operation.

```
CES> show reload
  Reload scheduled in 1 hour 45 minutes
  Explanation: Load latest software patches
  After shutdown: Restart
  Current logins: Enabled
  Reboot logins: Disabled
  Boot drive:/ide0
  Config file: latest
```

show services

Use this command to display information about the available services on the VPN Router.

Syntax

show services [**tunnel**] [**all**] [**management**] [**authentication**]

Parameters

tunnel	Show information for tunnels.
all	Show information for all services.
management	Show information for management protocols.
authentication	Show information for authentication protocols.

Default

If no options are selected, this command will show summary and detailed information for all services.

Command mode

User EXEC

Next command mode

User EXEC

Related commands

show sessions
ip http server

Example

```
CES> show services tunnel

Type     Public Private
----------------------------
IPsec    True  False
L2F & L2TPTrue False
PPTP     True  False
```

show sessions

Use this command to display information about the current sessions connected to the VPN Router.

Syntax

```
show [branch-office] [ipsec] [pptp] [l2tp] [l2f] [admin]
[all] sessions [detail]
```

Parameters

admin	Show information about administrator connections.
all	Show information about all connection types.
branch-office	Show information about branch office connections.
ipsec	Show information about IPsec connections.
l2f	Show information about L2F connections.
l2tp	Show information about L2TP connections.
pptp	Show information about PPTP connections.
detail	Show detailed information about the specified session type.

Default

If you enter the **show sessions** command with no options, the command shows summary and detailed information about all session types.

Command mode

User EXEC

Next command mode

User EXEC

Related commands

kill
who

Example

This example shows the detailed information about administrator connections that are currently made to the VPN Router. If you omit the **detail** parameter, you see the first (Summary) portion of the output only.

```
CES> show admin sessions detail

Summary:
 Current Sessions:
  Admin: 2
 Peak Sessions for Today:
  Admin: 2
 Total Sessions Since Boot:
  Admin: 13

Current End User Sessions:
 User: admin
 Account Type: Admin
 UID: admin
  Session Type: Telnet
  Session ID: 13
  IP Address Assigned: 192.32.229.107
  Start Date: 03/16/2002
  Start Time: 19:18:53

User: admin
 Account Type: Admin
 UID: admin
  Session Type: HTTP
  Session ID: 12
  IP Address Assigned: 192.32.229.107
  Start Date: 03/16/2002
  Start Time: 19:18:05
```

show version

Use this command to display the configuration of the system hardware, the software version, the name and location of the configuration file, and the system up time.

Syntax

show version

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Related commands

show flash: contents

Example

```
CES> show version
System Up Time
Up Time:                 004 21:05:06

System Configuration
Software Version:        V07_00.024
Software Build Date:     Jul  6 2006, 08:23:16
System Serial Number:    510649
MAC Address:             00-09-97-91-70-C0
BIOS Version:            PO8

Hardware Configuration
Processor 1:   Pentium 4 Xeon 2.25 Ghz, L2 Cache:512K
Processor 2:   Pentium 4 Xeon 2.25 Ghz, L2 Cache:512K
Memory:        348 MB Free, 513 MB Total
Hard Disk 0:   305 MB Free, 2146 MB Total
Hard Disk 1:   1858 MB Free, 2146 MB Total
Diskette:      3.5 Inch
```

terminal paging

Use this command to enable or disable paging on the terminal screen.

Syntax

terminal paging {**off** | **on**}

Parameters

off	Turns off paging.
on	Turns on paging.

Default

Paging is on.

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - View
User Management - None

trace ip

Use this command to determine the route that packets use when traveling to their destination. The **trace ip** command is commonly used as a diagnostic command (called **traceroute** on most systems).

Syntax

```
trace ip {<dest_host> | <dest_address>} [source
{<source_host> | <source_address>}] [hops <hops>]
[wait <seconds>]
```

Parameters

dest_host	Specifies the host name of the destination system for the trace packets.
dest_address	Specifies the IP address of the destination system for the trace packets.
source	Specify the IP address or host name of the source system for the trace packets.
source_host	Specifies the host name of the source system for the trace packets.

source_address	Specifies the IP address of the source system for the trace packets.
hops	Specify the maximum number of hops to the destination address (the default is 30).
hops	Specifies the maximum number of hops (0 through 250).
wait	Specify the wait timeout.
seconds	Specifies the wait timeout in seconds (0 through 60).

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Warning messages

If the system cannot map an address to a host name, the following message is displayed:

```
% Unknown Host
```

Related commands

ping

Example

This example shows a successful trace. The command limits the number of hops to 3 and sets a wait timeout value of 2 seconds.

```
CES> trace ip 192.32.137.59 hops 3 wait 2
traceroute to 192.32.137.59, 3 hops max, 60 byte packets
 1  47.17.248.1  0 ms 0 ms 0 ms
 2  47.17.22.202 0 ms 0 ms 0 ms
 3 192.32.137.59 0 ms 0 ms 0 ms
```

This example shows an attempt to trace the path to an unknown host address:

```
CES> trace ip badaddress.com
traceroute: unknown host baddaddress.com
```

who

Use this command to show the active Telnet administration sessions on the VPN Router with the IP address from which they are connected. The sessions are listed by session ID. Session ID values are fixed for the duration of a session.

Syntax

who [<*ip_address*>]

Parameters

ip_address	IP address in dotted-decimal notation. This argument limits the output to Telnet sessions that are connected from the specified IP address. If this argument is not specified, then all Telnet sessions are displayed.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Warning messages

```
% No Telnet sessions from specified IP address.
% Illegal IP address.
```

Related commands

kill
show sessions

Example

This example shows the output for all current Telnet sessions:

```
CES> who
121: From 116.102.4.45
213: From 116.102.12.23
217: From 116.102.12.23
```

This example shows the output for sessions connected from a specific IP address:

```
CES> who 116.102.12.23
213: From 116.102.12.23
217: From 116.102.12.23
```

Chapter 3
Privileged EXEC mode commands

This chapter describes the Privileged EXEC CLI commands.

Command	Page
boot system	98
clear arp-cache	100
clear logging events	101
configure terminal	102
copy	103
delete	105
disable	106
exit	107
forced-logoff	108
help	110
kill	111
mkdir	113
more	114
reload	117
reload at	120
reload cancel	123
reload in	125
reload no-sessions	128
rename	131
retrieve software	132
rmdir	134

Command	Page
show arp	135
show data-collection-interval	136
show event-log size	137
show health	139
show log-file-lifetime	140
show logging config	142
show logging events	145
show logging history	150
show logging security	151
show logging syslog	154
show safe-mode	157
show serial-port	158
show software version	159
show system forwarding	160

boot system

This command specifies the software image that the VPN Router loads at startup. This command restarts the system with the image that you now want to run on the VPN Router.

Syntax

boot system <*version*> [**recurse**]

Parameters

version	Version of the software image.
recurse	All user connections and branch office connections are also to be deleted. If this parameter is not entered and there are connections to the VPN Router, the system boot will fail.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Warning messages

```
% The following numbers of users are currently connected to
the switch
   Admin:   End user:   Branch Office:
```

Related commands

show software version
retrieve

Example

```
CES# boot system V40_01.03
% The following numbers of users are currently connected to
the switch
   Admin: 2 End user: 0 Branch Office: 1

CES# boot system V40_01.03 recurse
    Do you want to proceed? (Y/N)
```

clear arp-cache

This command deletes all dynamic entries from the ARP cache, the fast-switching cache, and the IP route cache.

Syntax

```
clear arp-cache
```

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

```
arp
arp timeout
show arp
```

Example

```
CES# clear arp-cache
```

clear logging events

This command is used to clear the contents of the system event log.

Syntax

clear logging events

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

show logging events

Example

This command clears the event log. This command does not provide any feedback.

```
CES# clear logging events
CES#
```

configure terminal

This command puts the CLI into Global configuration mode. This allows the administrator to access Global configuration mode commands. To exit this mode, you can enter Ctrl-z, the **exit** command, or the **end** command. You enter all Global configuration commands from the terminal.

Syntax

configure terminal

Parameters

terminal

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

disable
enable
end

Example

```
CES# configure terminal
CES(config)# end
```

copy

This command is used to copy files or a single directory.

Caution: Use caution when you execute this command. Files and directories can be overwritten without warning.

Syntax

copy *<source_url> <destination_url>*

Parameters

source_url	Name of the source files or the source directory to be copied. The name can be an absolute path or a relative path. You can use wildcards in the file or directory name. The wildcard character (*) matches all patterns. Strings after a wildcard are ignored.
destination_url	Destination URL for a single copied file or directory, or the directory URL where the source files or directory will be copied. The name can be an absolute path or a relative path.

The **copy** command operates on files, groups of files, and directories as described in Table 5.

Table 5 copy command results

***source-url* (file, group of files, or directory)**	***destination-url* (file, directory, or neither)**	**Result of copy command**
File	Not a directory	Copy the source file to the destination URL.
File	Directory	Copy the source file to the destination directory.
Group of files that match a string with the wildcard character	Directory	Copy the group of files to the destination directory.

Table 5 copy command results (Continued)

***source-url* (file, group of files, or directory)**	***destination-url* (file, directory, or neither)**	**Result of copy command**
Directory	Directory	Copy the source directory into the destination directory.
Directory	Not a file or a directory	Copy the source directory to the destination URL.

Default

None

Command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% No such file or directory: <source_url>
% <destination_url> is an existing file
% Source and destination conflict: <directory1>,
<directory2>
```

Related commands

cd
delete
dir
show file systems

Example

```
CES# copy foo.py foobar.py
CES# copy foo.py ./foodir/
CES# copy ./foodir/ ..
CES# copy foo* ./foodir/
CES# copy foodir/ foobar/
```

delete

This command deletes files from the file system.



Caution: Use caution when you execute this command. Files and directories are deleted without warning.

Syntax

delete *<target_url>*

Parameters

target_url	Name of the file or files to be deleted. The files can be of any type. The name can be an absolute path or a relative path. You can use wildcards in the file name. The wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Default

None

Command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% File does not exist: <target_url>
% Directory does not exist: <directory portion of
target_url>
```

Related commands

copy
rmdir

Example

```
CES# delete system/python/lib/site/foo.py
CES# delete system/python/lib/site/foo/f*
CES# delete system/python/lib/site/foo/*
CES# delete foobar*
```

disable

This command makes the CLI parser exit from Privileged EXEC mode and return to User EXEC mode.

Syntax

disable

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

User EXEC

Related commands

configure
enable
end

Example

```
CES# disable
CES>
```

exit

This command allows you to exit any configuration mode or to close an active Telnet session if you use the command when in User EXEC mode.

Syntax

exit

Parameters

None

Default

None

Command mode

Available in all command modes

Next command mode

Either the lower level command mode, or none because the Telnet session is terminated.

Related commands

end

Example

This example shows a user starting in Global configuration mode and using the exit command twice to end in User EXEC mode.

```
CES(config)# exit
CES# exit
CES>
```

forced-logoff

Use this command to log off a branch office tunnel or user tunnel immediately.

Syntax

forced-logoff boconn {**all** | <*bo_name*> <*bo_group_name*>}

forced-logoff user {**all-non-admin** | <*user_name*> <*group_name*>}

Parameters

all	Specifies that all branch office connections be immediately logged off.
bo_name	Specifies the name of the branch office tunnel connection that you want to log off. If the name includes spaces, enclose it in quotation marks.
bo_group_name	Specifies the name of the branch office group that the branch office connection belongs to. If the name includes spaces, enclose it in quotation marks.
all-non-admin	Specifies that all users who are not logged on as administrators be immediately logged off.
user_name	Specifies the name of the user that you want to log off. If the name includes spaces, enclose it in quotation marks.
group_name	Specifies the name of the user group that the user belongs to. If the name includes spaces, enclose it in quotation marks.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management – Manage
User Management – Manage

Warning messages

```
% Connection does not exist for BO <bo_name> in group
<group_name>
% Connection does not exist for user <user_name> in group
<group_name>
```

Related commands

kill
show sessions
who

Example

The following example immediately logs off the branch office tunnel Boston.

```
CES# forced-logoff boconn Boston "/Base/Branch1"
CES#
```

The following example immediately logs off user tunnel george123.

```
CES# forced-logoff user george123 "/Base/PQHQ"
CES#
```

help

This command displays a message about how to use the Help system.

Syntax

help

Parameters

None

Command mode

Available in all command modes

Related commands

None

Example

```
CES# help
Help may be requested at any point in a command by entering
a question mark (?). If nothing matches, the Help list will
be empty and you must back up until entering a '?' shows the
available options.
Two styles of Help are provided:
1. Full Help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
   possible argument.
2. Partial help is provided when an abbreviated argument is
   entered and you want to know what arguments match the
   input (e.g. 'show se?').
CES#
```

kill

This command terminates an identified Telnet session. You can obtain the Telnet session ID using the **who** command.

Any in-progress session commands are completed and the session is then terminated without any warning or message to the Telnet user.

If the session ID you supply is not valid, the **kill** command displays an error message and does nothing.

Syntax

kill <*telnet_id*>

Parameters

telnet_id	Session ID of the Telnet session to be terminated.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Warning messages

```
% Invalid session ID.
% Session is not a Telnet session.
```

Related commands

who
show sessions

Example

In this example, the **who** command is used to display the Telnet sessions active on the VPN Router. One session is terminated using the **kill** command and the results are shown in the subsequent **who** command.

```
CES# who
121: From 116.102.4.45
213: From 116.102.12.23
217: From 116.102.12.23
CES# kill 213
CES# who
121: From 116.102.4.45
217: From 116.102.12.23
```

mkdir

This command creates a new directory in the file system.

Syntax

mkdir <*directory*>

Parameters

directory	Name of the directory to create. The name can be an absolute path or a relative path. A slash (*/*) can be appended to the end of the path.

Default

None

Command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

% Directory already exists: <*directory*>

Related commands

cd
dir
rmdir

Example

```
CES# mkdir foo
CES# mkdir /ide0/foobar
```

more

This command displays a readable file on the VPN Router. The file is displayed one Telnet screen at a time. You can use the pagination keys to see the next screen.

On the Nortel VPN Router, you cannot use this command to display a file on a remote file system. It also does not support the /ebcdic option that causes the file to be printed in EBCDIC mode.

On the VPN Router, this command is limited to files that are 10 KB or smaller. If you try to use the **more** command on a file that is larger than 10 KB, an error message is displayed.

Syntax

more [**/ascii** | **/binary**] <*file-name*>

Parameters

/ascii	Display the file in ASCII.
/binary	Display the file in binary.
file-name	Fully qualified name of the VPN Router file to display. The name has this format: **disk***n*:[<*directory*>**/**]...<*file.ext*> **disk***n* is either disk0 or disk1.

Default

The default depends on the type of file. If the file contains non-printable characters, the output defaults to binary; otherwise the output defaults to ASCII. You cannot print a binary file in ASCII output format. If you attempt to print a binary file in ASCII output format, the command is ignored.

Printable characters are characters whose character codes are in the range decimal 32 (space) to decimal 126 (~) inclusive, plus the characters \t (decimal 9), \n (decimal 10), and \r (decimal 13). Non-printable characters are represented by a period (.) in the ASCII part of the binary output format.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Warning messages

```
% File not found.
% Cannot display a file that is larger that 10KB.
```

Example

The first example uses the **more** command to display the contents of a configuration file in ASCII mode. The second example shows the file contents in the binary output format.

```
CES# more disk0:system/config/CFG01022.DAT

+AccessLst[abc]
AccessLst[abc].Name=abc
+AccessLst[abc].Rule[11.4.1.6:1.1.1.1:DENY]
AccessLst[abc].Rule[11.4.1.6:1.1.1.1:DENY].Key=11.4.1.6:1.1.1.1:DENY
AccessLst[abc].Rule[11.4.1.6:1.1.1.1:DENY].Protocol=IP
AccessLst[abc].Rule[11.4.1.6:1.1.1.1:DENY].SourceAddr=11.4.1.6
AccessLst[abc].Rule[11.4.1.6:1.1.1.1:DENY].SourceWildcard=1.1.1.1
+AccessLst[abc].Rule[abdguiwfeh:255.255.0.0:Permit]
AccessLst[abc].Rule[abdguiwfeh:255.255.0.0:Permit].Action=PERMIT
AccessLst[abc].Rule[abdguiwfeh:255.255.0.0:Permit].Key=abdguiwfeh:255.25
5.0.0:Permit
AccessLst[abc].Rule[abdguiwfeh:255.255.0.0:Permit].SourceWildcard=255.25
5.0.0
+AccessLst[abc].Rule[2.0.0.0:255.0.0.:Permit]
AccessLst[abc].Rule[2.0.0.0:255.0.0.:Permit].Action=PERMIT
AccessLst[abc].Rule[2.0.0.0:255.0.0.:Permit].Key=2.0.0.0:255.0.0.:Permit
AccessLst[abc].Rule[2.0.0.0:255.0.0.:Permit].SourceAddr=2.0.0.0
+AccessLst[bar]
AccessLst[bar].Name=bar
+AccessLst[bar].Rule[1.2.0.0:255.255.0.0:0]
AccessLst[bar].Rule[1.2.0.0:255.255.0.0:0].Key=1.2.0.0:255.255.0.0:0

CES#

CES# more /binary disk0:system/config/CFG01022.DAT

00000000:  0A210A21 204C6173 7420636F 6E666967    .!.!  Las t co nfig
00000010:  75726174 696F6E20 6368616E 67652061    urat ion  chan ge a
00000020:  74203134 3A30333A 32322070 73742046    t 14 :03: 22 p st F
00000030:  72692041 75672032 37203139 39390A21    ri A ug 2 7 20 01.!
00000040:  204E5652 414D2063 6F6E6669 67206C61     NVR AM c onfi g la
00000050:  73742075 70646174 65642061 74203134    st u pdat ed a t 14
00000060:  3A30393A 30392070 73742046 72692041    :09: 09 p st F ri A
00000070:  75672032 37203139 39390A21 0A766572    ug 2 7 20 01.! .ver
00000080:  73696F6E 2031322E 300A7365 72766963    sion  12. 0.se rvic
```

reload

This command forces the VPN Router to reboot immediately. Options can be specified to determine whether the VPN Router turns itself off or reboots, which configuration to use after a reboot, and other settings.

You are prompted to continue with the reload. If the answer is yes and if the **reload** command is valid, the system reload starts in approximately 10 seconds.

A system booted in safe mode can only accept secured management tunnel establishment. When the secured management tunnel is established, Telnet, HTTP, and FTP traffic are allowed to come into the VPN Router; no other VPN traffic is allowed through the secured management tunnel or the VPN Router.



Note: The Nortel VPN Router 1010, 1050, and 1100 do not have safe mode. Safe mode options are not available on the Nortel VPN Router 1010/1050/1100.

In normal mode, the system operates with the normal software and configuration and transports both VPN traffic and management traffic. For most Telnet client software, the reboot will cause the Telnet client to close the connection to the VPN Router. If there are any outstanding reboot commands, they will be canceled. There can only be one reboot scheduled at any time.

Syntax

```
reload [power-off | restart] [boot-safe | boot-normal]
[boot-drive {ide0 | ide1}] [config-file {latest | factory |
<config_name>}] [disable-logins] [disable-after-restart]
[<text>]
```

Parameters

power-off	Turn off the VPN Router after it has completed shutdown.
restart	Restart the VPN Router after it has completed shutdown.
boot-safe	Restart the VPN Router in safe boot mode.
boot-normal	Restart the VPN Router in normal boot mode.
boot-drive	Disk drive from which the VPN Router will reboot.
ide0 | **ide1**	Disk drive from which the bootable image will be loaded.
config-file	Use the specified configuration file after a reboot.
config_name	Name of a previously saved configuration to use on reboot.
latest	Reboot the VPN Router with the latest configuration file.
factory	Reboot the VPN Router with the reset configuration file. This file sets the VPN Router to basic defaults. The contents of the LDAP database and other settings are maintained.
disable-logins	No more logins should be permitted before the reboot occurs.
disable-after-restart	Logins should not be permitted after the reboot. This is intended to support system maintenance tasks after a reboot.
text	Display the reason for a **reload** command. This text will be displayed on the Admin -> Shutdown and Status -> System management pages. If the text parameter contains spaces, enclose it in double quotation marks so that it has a single parameter value.

Default

The default settings for this command are determined by any previous **reload** command. For the first **reload** command, the following defaults apply:

```
restart
boot-drive ide0
config-file latest
```

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Prerequisites

A named configuration file can only be used after it has been created.

Warning messages

Any warnings cause the command to fail. You must re-enter the command after correcting the parameters in error.

```
% Configuration file does not exist.
```

Related commands

reload at
reload cancel
reload in
reload no-sessions
show reload
shutdown

Example

The following command reboots the VPN Router from ide0 using the factory-installed defaults and disables logins after the reboot to allow for system maintenance. You use these commands when upgrading the software. Press Return or any subset of the string “yes” to confirm that the reload should proceed.

```
CES# reload restart boot-drive ide0 config-file factory
disable-after-restart “Upgrade software”
 Reload Scheduled Shutdown
 Reload Explanation: Upgrade software
 After Shutdown: Restart
 Disable New Logins: No
 Disable Logins after Restart: Yes
 Boot Mode: Normal
 Config File: Reset Config File
 Boot Drive: /ide0/
 Proceed with reload? [confirm] y
```

reload at

This command sets a time at which the VPN Router will reboot. Options can be specified to determine whether the VPN Router turns itself off or reboots, which configuration to use after a reboot, and other settings. You are prompted to confirm whether you want to continue with the reload. If you select yes and if the **reload** command is valid, the system reload starts at the specified time.

After a successful **reload at** command, the VPN Router will reboot at the time specified based on internal clock settings. For most Telnet client software, the reboot will cause the Telnet client to close the connection to the VPN Router. If there are any outstanding **reboot** commands, they will be canceled. There can be only one reboot scheduled at any time.



Note: The Nortel VPN Router 1010, 1050, and 1100 do not have safe mode. Safe mode options are not available on the Nortel VPN Router 1010/1050/1100.

Syntax

```
reload at <hh:mm> [power-off | restart] [boot-safe |
boot-normal] [boot-drive {ide0 | ide1}] [config-file
{latest | factory | <config-name>}] [disable-logins]
[disable-after-restart] [<text>]
```

Parameters

hh:mm	Time at which the shutdown will begin. Values are based on a 24-hour clock. If this time has already passed today, then the reload will occur at this time tomorrow.
power-off	Turn off the VPN Router after it has completed shutdown.
restart	Restart the VPN Router after it has completed shutdown.
boot-safe	Restart the VPN Router in safe boot mode.
boot-normal	Restart the VPN Router in normal boot mode.
boot-drive	Disk drive from which the VPN Router will reboot.
ide0 | **ide1**	Disk drive from which the bootable image will be loaded.
config-file	Use the specified configuration file after a reboot.
config_name	Name of a previously saved configuration to use on reboot.
latest	Reboot the VPN Router with the latest configuration file.
factory	Reboot the VPN Router with the reset configuration file. This file sets the VPN Router to basic defaults. The contents of the LDAP database and other settings are maintained.
disable-logins	No more logins should be permitted before the reboot occurs.
disable-after-restart	Logins should not be permitted after the reboot. Use this option to support system maintenance tasks after a reboot.
text	Display the reason for a **reload** command. This text will be displayed on the Admin -> Shutdown and Status -> System management pages. If the text parameter contains spaces, enclose it in double quotation marks.

Default

The default settings for this command are determined by any previous **reload** command. For the first **reload** command, the following defaults apply:

```
restart
boot-drive ide0
config-file latest
```

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Prerequisites

A named configuration file can only be used after it has been created.

Warning messages

Any warnings cause the command to fail. You must re-enter the command after correcting the parameters in error.

```
% Configuration file does not exist.
```

Related commands

```
reload
reload cancel
reload in
reload no-sessions
show reload
shutdown
```

Example

The following command reboots the VPN Router from ide0 using the latest configuration and disables logins after the reboot to allow for system maintenance. You use these commands to back up the LDAP database.

```
CES# reload at 22:00 restart boot-drive ide0
disable-after-restart “Back up LDAP database”

 Reload Scheduled Shutdown at 22:00:00
 Reload Explanation: Back up LDAP database
 After Shutdown: Restart
 Disable New Logins: No
 Disable Logins after Restart: Yes
 Boot Mode: Normal
 Config File: latest
 Boot Drive: /ide0/
Proceed with reload? [confirm] y
```

reload cancel

This command cancels any pending **reload** command. There can only be one pending reload at any given time. When a reload is canceled, the information about the pending reload is displayed.

Syntax

reload cancel

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Prerequisites

A reload operation must already have been scheduled.

Warning messages

```
% No currently scheduled reload operation.
```

Related commands

reload
reload at
reload in
reload no-sessions
show reload
shutdown

Example

This command cancels a pending **reload** command and then displays information about the original **reload** command.

```
CES# reload cancel
Reload Scheduled Shutdown at 22:00:00 has been canceled
Reload Explanation: Back up LDAP database
After Shutdown: Restart
Disable New Logins: No
Disable Logins after Restart: Yes
Boot Mode: Normal
Config File: latest
Boot Drive: /ide0/
```

reload in

This command sets a timer that causes the VPN Router to reboot after a specified amount of time has elapsed. Options can be specified to determine whether the VPN Router turns itself off or reboots, which configuration to use after a reboot, and other settings. You are prompted to confirm whether you want to continue with the reload. If you select yes and if the **reload** command is valid, the system reload begins at the specified time.

After a successful **reload in** command, the VPN Router will reboot after the time specified has elapsed. For most Telnet client software, the reboot will cause the Telnet client to close the connection to the VPN Router. If there are any outstanding **reboot** commands, they will be canceled. Only one reboot can be scheduled at any time.



Note: The Nortel VPN Router 1010, 1050, and 1100 do not have safe mode. Safe mode options are not available on the Nortel VPN Router 1010/1050/1100.

Syntax

```
reload in {<hh:mm> | <minutes>} [power-off | restart]
[boot-safe | boot-normal] [boot-drive {ide0 | ide1}]
[config-file {latest | factory | <config-name>}]
[disable-logins] [disable-after-restart] [<text>]
```

Parameters

hh:*mm*	Shut down the VPN Router after the specified number of hours and minutes. Enter a value from 00:01 through 23:59.
minutes	Shut down the VPN Router after the specified number of minutes. Enter a value from 1 through 59.
power-off	Turn off the VPN Router after it has completed shutdown.
restart	Restart the VPN Router after it has completed shutdown.
boot-safe	Restart the VPN Router in safe boot mode.
boot-normal	Restart the VPN Router in normal boot mode.

boot-drive	Disk drive from which the VPN Router will reboot.
ide0 | **ide1**	Disk drive from which the bootable image will be loaded.
config-file	Use the specified configuration file after a reboot.
config_name	Name of a previously saved configuration to use on reboot.
latest	Reboot the VPN Router with the latest configuration file.
factory	Reboot the VPN Router with the reset configuration file. This file sets the VPN Router to basic defaults. The contents of the LDAP database and other settings are maintained.
disable-logins	No more logins should be permitted before the reboot occurs.
disable-after-restart	Logins should not be permitted after the reboot. Use this option to support system maintenance tasks after a reboot.
text	Display the reason for a **reload** command. This text will be displayed on the Admin -> Shutdown and Status -> System management pages. If the text parameter contains spaces, enclose it in double quotation marks.

Default

The default settings for this command are determined by any previous **reload** command. For the first **reload** command, the following defaults apply:

```
restart
boot-drive ide0
config-file latest
```

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Prerequisites

A named configuration file can only be used after it has been created.

Warning messages

Any warnings cause the command to fail. You must re-enter the command after correcting the parameters in error.

```
% Configuration file does not exist.
```

Related commands

reload
reload cancel
reload at
reload no-sessions
show reload
shutdown

Example

This command causes the VPN Router to turn itself off in 8 hours. The VPN Router will reboot from ide1. Further logins are disabled until the VPN Router has rebooted.

```
CES# reload in 8:00 restart boot-drive ide1 power-off
disable-logins

 Reload Scheduled Shutdown in 480 minutes
 Reload Explanation: Scheduled Shutdown in 480 minutes
 After Shutdown: Powerdown
 Disable New Logins: Yes
 Disable Logins after Restart: No
 Boot Mode: Normal
 Config File: latest
 Boot Drive: /ide1/
 Proceed with reload? [confirm] y
```

reload no-sessions

This command causes the VPN Router to reboot after there are no further logins. The reboot will start after all tunnels into the VPN Router and all management sessions (for example, Telnet) have been closed.

Options can be specified to determine whether the VPN Router turns itself off or reboots, which configuration to use after a reboot, and other settings. You are prompted to confirm whether you want to continue with the reload. If you select yes and if the **reload** command is valid, the system reload will start a short time after all sessions (tunnels and administrative) have disconnected.

After a successful **reload no-sessions** command, the VPN Router will reboot as soon as all sessions—including CLI management sessions—on the VPN Router have terminated. If there are any outstanding **reboot** commands, they will be canceled. Only one reboot can be scheduled at any time.



Note: The Nortel VPN Router 1010, 1050, and 1100 do not have safe mode. Safe mode options are not available on the Nortel VPN Router 1010/1050/1100.

Syntax

```
reload no-sessions [power-off | restart] [boot-safe |
boot-normal] [boot-drive {ide0 | ide1}] [config-file {latest
| factory | <config-name>}] [disable-logins]
[disable-after-restart] [<text>]
```

Parameters

no-sessions	Start the reboot as soon as no more sessions are connected to the VPN Router.
power-off	Turn off the VPN Router after it has completed shutdown.
restart	Restart the VPN Router after it has completed shutdown.
boot-safe	Restart the VPN Router in safe boot mode.
boot-normal	Restart the VPN Router in normal boot mode.
boot-drive	Disk drive from which the VPN Router will reboot.

ide0 | **ide1**	Disk drive from which the bootable image will be loaded.
config-file	Use the specified configuration file after a reboot.
config_name	Name of a previously saved configuration to use on reboot.
latest	Reboot the VPN Router with the latest configuration file.
factory	Reboot the VPN Router with the reset configuration file. This file sets the VPN Router to basic defaults. The contents of the LDAP database and other settings are maintained.
disable-logins	No more logins should be permitted before the reboot occurs.
disable-after-restart	Logins should not be permitted after the reboot. Use this option to support system maintenance tasks after a reboot.
text	Display the reason for a **reload** command. This text will be displayed on the Admin -> Shutdown and Status -> System management pages. If the text parameter contains spaces, enclose it in double quotation marks.

Default

The default settings for this command are determined by any previous **`reload`** command. For the first **`reload`** command, the following defaults apply:

```
restart
boot-drive ide0
config-file latest
```

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Prerequisites

A named configuration file can only be used after it has been created.

Warning messages

Any warnings cause the command to fail. You must re-enter the command after correcting the parameters in error.

```
% Configuration file does not exist.
```

Related commands

reload
reload at
reload cancel
reload in
show reload
shutdown

Example

This example reboots the VPN Router from ide0 using the latest configuration when there are no sessions connected to the VPN Router. New session connections are disabled.

```
CES# reload no-sessions restart disable-logins

 Reload Shutdown after all users log off
 Reload Explanation: Shutdown after all users log off
 After Shutdown: Restart
 Disable New Logins: Yes
 Disable Logins after Restart: No
 Boot Mode: Normal
 Config File: latest
 Boot Drive: /ide0/
 Proceed with reload? [confirm] y
```

rename

This command renames a file or directory in the file system.

Syntax

rename *<url1> <url2>*

Parameters

url1	Original file or directory name. The name can be an absolute path or a relative path.
url2	New file or directory name. The name can be an absolute path or a relative path.

Default

None

Command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% No such file or directory: <url1>
% <url2> already exists
```

Example

```
CES# rename foo.py foobar.py
CES# rename foo/foo.py foobar.py
```

retrieve software

Use this command to retrieve the latest software images for the VPN Router. Use this command before you upgrade the VPN Router.

Syntax

```
retrieve software <host> version <version_number>
[path <path>] uid <user_ID> password <password> [recurse]
```

Parameters

host	Name or IP address of the host remote server that contains the VPN Router software version to be retrieved.
version	Specify the file version.
version_number	Software image file version.
path	Specify the path to the VPN Router software.
path	Path to the directories and files where the VPN Router software is stored.
uid	Specify the user ID for the FTP server.
user_ID	User ID for the FTP server.
password	Specify the user password for the FTP server.
password	FTP server password.
recurse	Retrieve the software version even if this version exists on the VPN Router already.

Default

None

Command mode

Privileged EXEC

Response

```
boot system
```

Next command mode

Privileged EXEC

Warning messages

```
% Authentication failed.
% Cannot establish connection with the host.
% Unable to obtain directory listing from the remote host.
```

Related commands

show software version

Example

```
CES# retrieve software 192.32.250.6 version V04_01.12
uid master password Paris
```

rmdir

This command removes a single directory from the file system.



Caution: Use caution when you execute this command. Directories are deleted without warning.

Syntax

rmdir <*directory*>

Parameters

directory	Name of the directory to delete. The name can be an absolute path or a relative path. A slash (*/*) can be appended to the end of the path.

Default

None

Command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

% Directory does not exist: <*directory*>

Related commands

delete
dir
mkdir

Example

```
CES# rmdir /ide0/foo
CES# rmdir foobar
```

show arp

This command displays the entries in the ARP table.

Syntax

show arp

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

arp
arp timeout
clear arp-cache

Example

```
CES# show arp
LINK LEVEL ARP TABLE
Destination     Gateway   Flags  Ref   Use  Intf MTU OuterCtxt CircMap  RtEntryP
------------------------------------------------------------------------------
47.17.248.1  00:e0:16:7c:61:96  10405  1 0 fei0  1500 2f6ccc8  39 862f0  3890124
------------------------------------------------------------------- -------------
CES#
```

show data-collection-interval

Use this command to display the data collection interval. This interval specifies the number of minutes (from 1 through 5) that the VPN Router waits before it collects new data for the log. By default, this interval is set to 2 minutes.

Syntax

show data-collection-interval

Parameters

None

Default

2 minutes

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

data-collection-interval

Example

```
CES# show data-collection-interval
  Data Collection interval: 2 minutes
CES# configure terminal
CES(config)# data-collection-interval 4
CES(config)# exit
CES# show data-collection-interval
  Data collection interval: 4 minutes
CES#
```

show event-log size

Use this command to display the maximum number of entries stored in the event log.

Syntax

show event-log size

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

event-log size

Example

The following example displays the maximum number of entries for the event log.

```
CES> show event-log size
   Event Log Size: 2000 entries
CES>
```

show health

This command displays information about the overall health of the VPN Router. It allows the administrator to check on areas that may cause problems in the future, as well as to see where problems have been detected already.

Syntax

show health [**alerts** | **warnings** | **disabled** | **all**]

Parameters

alerts	Displays conditions that require immediate administrator attention.
warnings	Displays conditions that must be fixed to avoid an alert condition. It also shows alert conditions.
disabled	Displays services and protocols whose administrative states are set to “disabled.” It also shows warning and alert conditions.
all	Displays all conditions, including those that indicate correct operation.

Default

If no warning level is entered, all health information is displayed. In other words, entering the **show health** command with no options is equivalent to entering **show health all**.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

audible alarm

Example

This example shows the type of output that is displayed when you request alert and warning messages using the **show health** command.

```
CES# show health warnings

Alert:   LAN on slot 2 Interface 1. Device fei1 down
Alert:   Auto backup servers. Can't back up to 12.33.44.123
Alert:   Voltage 2.5 VA.   Voltage out of range
Alert:   Chassis Fan.      Fan not functioning
Warning: Hard Disk 1.      Device /ide1/ not available
Warning: SNMP Servers.     Server not configured
```

show log-file-lifetime

Use this command to display the system log file lifetime. By default, system log files are maintained on the hard drive for 60 days.

Syntax

show log-file-lifetime

Parameters

None

Default

60

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

log-file-lifetime

Example

```
CES# show log-file-lifetime
  Log File Lifetime: 60 days
CES# configure terminal
CES(config)# log-file-lifetime 40
CES(config)# exit
CES# show log-file-lifetime
  Log File Lifetime: 40 days
```

show logging config

This command displays the contents of the configuration log on the screen. This log tracks all changes to the configuration of the VPN Router. The amount of output from this command can be substantial. The output is automatically paginated on the display so that you can see one page at a time.



Note: The Nortel VPN Router 1010, 1050, and 1100 do not support system logging. This command does not apply to these Nortel VPN Router models.

Syntax

show logging config [**date** {<*day*> <*month*> [<*year*>] | <*month*> <*day*> [<*year*>]}] [**normal** | **urgent** | **detailed** | **all**]

Parameters

date	Specify the date for which the configuration log is to be displayed.
day	Day of the month for which the configuration log is to be displayed.
month	Month for which the configuration log is to be displayed.
year	Year for which the configuration log is to be displayed. Type a four-digit value.
normal	Display normal events, including user and system interactions, that indicate VPN Router activity.
urgent	Display events that an administrator should be aware of immediately. In the output, these events are marked with an asterisk. May indicate potential security or access problems. Also, display normal events.
detailed	Display events for Nortel Networks support personnel. Also, display normal and urgent events.
all	Display events for Nortel Networks support personnel to use in troubleshooting the VPN Router. Includes every event that the VPN Router generates. Also, display detailed, normal, and urgent events.

Default

The date defaults to today's date. If the year is omitted, it defaults to the current year. The default display level is normal.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

show logging events
show logging security
show logging syslog

Example

The first example shows the output from the configuration log with urgent messages displayed. The second example shows the output from the configuration log with normal messages displayed.

```
CES# show logging config urgent
  Config Log contents for Friday, July 30, 2001
  *09:54:15 tRootTask 0 : Error in cfg file setting
'IpxIntfOmCls.IpxPrivateLANS[256].$
  *09:54:15 tRootTask 0 : Error in cfg file setting
'IpxIntfOmCls.IPXPublicAddress=N/A$
CES# show logging config
  Config Log contents for Friday, July 30, 2001
   09:52:31 tHttpdTask 0 : Shutdown.Mode changed from 'NONE' to 'NOW' by
user 'admin' $
   09:52:31 tHttpdTask 0 : Reboot[Scheduled Shutdown] created by user
'admin' @ '132.2$
  *09:54:15 tRootTask 0 : Error in cfg file setting
'IpxIntfOmCls.IpxPrivateLANS[256].$
  *09:54:15 tRootTask 0 : Error in cfg file setting
'IpxIntfOmCls.IPXPublicAddress=N/A$
   09:54:31 tSerialConfig 0 : Flash.AdminUid changed from 'admin' to
'sysadmin' by use$
   09:54:31 tSerialConfig 0 : Flash.AdminPassword changed by user '' @ ''
   09:54:31 tSerialConfig 0 : DirBackup.PrimaryHost changed from
'11.33.55.66' to '11.$
   09:54:31 tSerialConfig 0 : DirBackup.PrimaryUsername changed from
'bernard' to 'sys$
   09:54:50 tObjMgr 0 : ObjMgrCls::WriteConfigFile() new configuration
file config/CFG$
```

show logging events

This command displays the contents of the event log. The event log is a detailed record of all events that take place on the system. The event log is maintained in device memory with significant events being saved in the system log and written to disk. The event log retains approximately 2000 entries and discards old entries when it is refreshed. The output from this command can be substantial. The output is automatically paginated so that you can see one page at a time.

This command also allows you to log details about packets that have been dropped by the VPN Router, including packets that are dropped due to filtering rules. Use these options only for troubleshooting: the logging of dropped packets can significantly affect the performance of the VPN Router.



Note: After you set options to log detailed event information, the options remain in effect until you enter the **`clear logging events`** command.

Syntax

```
show logging events [reverse] [ip-drops {all [filtered] |
filtered | none}] [ipx-drops {all | none}] [key-words
<search_terms>]
```

Parameters

reverse	Display events in the log in reverse chronological order (the most recent event is the first one displayed).
ip-drops	Specify the type of dropped IP packets to track in the event log.
ipx-drops	Specify the type of dropped IPX* packets to track in the event log.
all	All dropped IP or IPX packets are to be tracked. For each dropped packet, the source and destination address are kept in the event log for display.
filtered	IP packets dropped due to filter rules are to be tracked. For each packet dropped due to filtering, the packet contents are kept in the event log for display.

none	Dropped IP or IPX packets are not to be tracked.
key-words	Display event log entries that contain the specified words.
search-terms	Search the event log for one or more words. To match log entries that contain one of the specified terms, use the vertical bar (|) as follows: **key-words** <*term1*>**|**<*term2*> . . . To match log entries that contain all the specified terms, use the ampersand (&) as follows: **key-words** <*term1*>**&**<*term2*> . . .

Default

Dropped IP and IPX packets are not tracked.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Warning messages

If you choose to track dropped IP or IPX packets, a confirmation is requested because of the impact on VPN Router performance.

Related commands

```
clear logging events
show logging config
show logging security
show logging syslog
```

Example

The following examples show the amount of detail that is output by this command, depending on the options chosen. The last example disables tracking of dropped IP packets and clears the event log so that no output results from the final command.

```
CES# show logging events
  09/02/2001 11:57:12 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7e88, 00000000$
  09/02/2001 12:01:52 0 FTP Backup [13] Redundant Disk is not available
  09/02/2001 12:01:52 0 FTP Backup [13] Update completed
  09/02/2001 12:02:00 0 DCLog [00] DCManager flushing data to stat file
'20010902.DC'
  09/02/2001 12:02:20 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7b24, 00000000$
  09/02/2001 12:02:20 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7e88, 00000000$
  09/02/2001 12:03:59 0 Security [13] Management: Forced Admin User Off
Due to Timeout$
  09/02/2001 12:04:00 0 Security [12] Session: LOCAL[admin]:2876 logged
out
  09/02/2001 12:04:00 0 Security [13] Management: Forcing admin to
re-supply userid
  09/02/2001 12:04:03 0 Security [11] Session: LOCAL[admin] attempting
login
  09/02/2001 12:04:03 0 Security [01] Session: LOCAL[admin] has no active
sessions
  09/02/2001 12:04:03 0 Security [01] Session: LOCAL[admin] admin has no
active accoun$
  09/02/2001 12:04:03 0 Security [12] Session: LOCAL[admin]:2877 master
admin authenti$
  09/02/2001 12:04:03 0 Security [11] Session: LOCAL[admin]:2877 server
right: MANAGE
  09/02/2001 12:04:03 0 Security [11] Session: LOCAL[admin]:2877 user/
group right: MAN$
  09/02/2001 12:04:04 0 Security [12] Session: LOCAL[admin]:2877
Management: logged in$
  09/02/2001 12:07:36 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7b24, 00000000$
  09/02/2001 12:07:36 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7e88, 00000000$
  09/02/2001 12:12:44 0 PaceJob{0} [00] Calling 0x00ca012c, passing
```

```
011b7b24, 00000000$
  09/02/2001 12:12:44 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7e88, 00000000$
  09/02/2001 12:17:00 0 DCLog [00] DCManager flushing data to stat file
'20010902.DC'
CES# show logging events ip-drops all
  09/02/2001 11:57:12 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7e88, 00000000$
  09/02/2001 12:01:52 0 FTP Backup [13] Redundant Disk is not available
  09/02/2001 12:01:52 0 FTP Backup [13] Update completed
  09/02/2001 12:02:00 0 DCLog [00] DCManager flushing data to stat file
'20010902.DC'
  09/02/2001 12:02:20 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7b24, 00000000$
  09/02/2001 12:02:20 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7e88, 00000000$
  09/02/2001 12:03:59 0 Security [13] Management: Forced Admin User Off
Due to Timeout$
  09/02/2001 12:04:00 0 Security [12] Session: LOCAL[admin]:2876 logged
out
  09/02/2001 12:04:00 0 Security [13] Management: Forcing admin to
re-supply userid
  09/02/2001 12:04:03 0 Security [11] Session: LOCAL[admin] attempting
login
  09/02/2001 12:04:03 0 Security [01] Session: LOCAL[admin] has no active
sessions
  09/02/2001 12:04:03 0 Security [01] Session: LOCAL[admin] admin has no
active accoun$
  09/02/2001 12:04:03 0 Security [12] Session: LOCAL[admin]:2877 master
admin authenti$
  09/02/2001 12:04:03 0 Security [11] Session: LOCAL[admin]:2877 server
right: MANAGE
  09/02/2001 12:04:03 0 Security [11] Session: LOCAL[admin]:2877 user/
group right: MAN$
  09/02/2001 12:04:04 0 Security [12] Session: LOCAL[admin]:2877
Management: logged in$
  09/02/2001 12:07:36 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7b24, 00000000$
  09/02/2001 12:07:36 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7e88, 00000000$
  09/02/2001 12:12:44 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7b24, 00000000$
  09/02/2001 12:12:44 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7e88, 00000000$
```

```
  09/02/2001 12:17:00 0 DCLog [00] DCManager flushing data to stat file
'20010902.DC'
  09/02/2001 12:17:50 0 tHttpdTask [35] DbEventLog.IpVerbose changed
from 'FALSE' to '$
  09/02/2001 12:17:52 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src
0x8f0f010a dst $
  09/02/2001 12:17:54 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src
0x8c10000a dst $
  09/02/2001 12:17:57 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7b24, 00000000$
  09/02/2001 12:17:57 0 PaceJob{0} [00] Calling 0x00ca012c, passing
011b7e88, 00000000$
  09/02/2001 12:17:59 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src
0xe6ea000a dst $

CES# show logging events ip-drops all filtered
  09/02/2001 12:26:17 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src
0x2810000a dst $
  09/02/2001 12:26:17 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src
0x2810000a dst $
  09/02/2001 12:26:18 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src
0x850a090a dst $
  09/02/2001 12:26:19 0 tHttpdTask [35] DbEventLog.FltVerbose changed
from 'FALSE' to $
  09/02/2001 12:26:20 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src
0x841c090a dst $
  09/02/2001 12:26:20 0 IPvfy.03739424{Prv} [00] Pkt(01-20) 45 00 00 ca
b4 59 00 00 05$
  09/02/2001 12:26:20 0 IPvfy.03739424{Prv} [00] Pkt(21-40) 00 8a 00 8a
00 b6 52 31 11$
  09/02/2001 12:26:21 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src
0x841c090a dst $
  09/02/2001 12:26:21 0 IPvfy.03739424{Prv} [00] Pkt(01-20) 45 00 00 4e
b4 5d 00 00 05$
  09/02/2001 12:26:21 0 IPvfy.03739424{Prv} [00] Pkt(21-40) 00 89 00 89
00 3a 80 78 d7$
  09/02/2001 12:26:22 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src
0x841c090a dst $
  09/02/2001 12:26:22 0 IPvfy.03739424{Prv} [00] Pkt(01-20) 45 00 00 4e
b4 5f 00 00 05$
  09/02/2001 12:26:22 0 IPvfy.03739424{Prv} [00] Pkt(21-40) 00 89 00 89
00 3a 80 78 d7$
  09/02/2001 12:26:23 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src
0x841c090a dst $
```

```
  09/02/2001 12:26:23 0 IPvfy.03739424{Prv} [00] Pkt(01-20) 45 00 00 4e
b4 66 00 00 05$
  09/02/2001 12:26:23 0 IPvfy.03739424{Prv} [00] Pkt(21-40) 00 89 00 89
00 3a 80 78 d7$
CES# show logging events ip-drops none
CES# clear logging events
```

show logging history

This command displays the current logging history setting that is being used by the VPN Router.

Syntax

show logging history

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

logging history

Example

This example shows the output for a VPN Router where the logging history is still at the default value.

```
CES# show logging history

  Logging history level is errors.
```

show logging security

This command displays the contents of the security log. The security log records all events concerned with system or user security, including failures and successes.

The amount of output from this command can be substantial. The output is automatically paginated on the display so that you can see one page at a time.



Note: The Nortel VPN Router 1010, 1050, and 1100 do not support system logging. This command does not apply to these Nortel VPN Router models.

Syntax

show logging security [**date** {<*day*> <*month*> [<*year*>] | <*month*> <*day*> [<*year*>]}] [**normal** | **urgent** | **detailed** | **all**]

Parameters

date	Specify the date for which the security log is to be displayed.
day	Day of the month for which the security log is to be displayed.
month	Month for which the security log is to be displayed.
year	Year for which the security log is to be displayed. Type a four-digit value.
normal	Display normal events, including user and system interactions, that indicate VPN Router activity.
urgent	Display events that an administrator should be aware of immediately. In the output, these events are marked with an asterisk. May indicate potential security or access problems. Also, display normal events.
detailed	Display events for Nortel Networks support personnel. Also, display normal and urgent events.
all	Display events for Nortel Networks support personnel to use in troubleshooting the VPN Router. Includes every event that the VPN Router generates. Also, display detailed, normal, and urgent events.

Default

The date defaults to today's date. If the year is omitted, it defaults to the current year. The default display level is normal.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

show logging config
show logging events
show logging syslog

Example

This example shows the security log output for normal messages. The urgent messages are marked with an asterisk (*).

```
CES# show logging security

  *09:54:26 tEvtLgMgr 0 : Security [13] Management: Request for
manager.htm denied, re$
   09:54:29 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2873 master
admin authen$
   09:54:30 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2873
Management: logged $
  *11:05:38 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off
Due to Timeo$
   11:05:39 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2873 logged
out
  *11:05:39 tEvtLgMgr 0 : Security [13] Management: Forcing admin to
re-supply userid
   11:05:40 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2874 master
admin authen$
   11:05:41 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2874
Management: logged $
  *11:26:08 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off
Due to Timeo$
   11:26:09 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2874 logged
out
  *11:26:09 tEvtLgMgr 0 : Security [13] Management: Forcing admin to
re-supply userid
   11:26:11 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2875 master
admin authen$
   11:26:11 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2875
Management: logged $
  *11:48:39 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off
Due to Timeo$
```

```
   11:48:40 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2875 logged
out
  *11:48:40 tEvtLgMgr 0 : Security [13] Management: Forcing admin to
re-supply userid
   11:48:42 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2876
Management: logged $
  *12:03:59 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off
Due to Timeo$
   12:04:00 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2876 logged
out
  *12:04:00 tEvtLgMgr 0 : Security [13] Management: Forcing admin to
re-supply userid
   12:04:03 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2877 master
admin authen$
   12:04:04 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2877
Management: logged $
   12:18:16 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2878 FTP:
logged in from$
   12:19:06 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2878 FTP
Get filename /s$
   12:19:49 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2878 FTP
Get filename /s$
```

show logging syslog

This command displays the contents of the system log. The system log contains all system events that are considered significant enough to be written to disk, including those displayed in the security and configuration logs. The amount of output from this command can be substantial. The output is automatically paginated on the display so that you can see one page at a time.



Note: The Nortel VPN Router 1010, 1050, and 1100 do not support system logging. This command does not apply to these Nortel VPN Router models.

Syntax

show logging syslog [**date** {*<day>* *<month>* [*<year>*] | *<month>* *<day>* [*<year>*]}] [**normal** | **urgent** | **detailed** | **all**]

Parameters

date	Specify the date for which the system log is to be displayed.
day	Day of the month for which the system log is to be displayed.
month	Month for which the system log is to be displayed.
year	Year for which the system log is to be displayed. Type a four-digit value.
normal	Display normal events, including user and system interactions, that indicate VPN Router activity.
urgent	Display events that an administrator should be aware of immediately. In the output, these events are marked with an asterisk. May indicate potential security or access problems. Also, display normal events.
detailed	Display events for Nortel Networks support personnel. Also, display normal and urgent events.
all	Display events for Nortel Networks support personnel to use in troubleshooting the VPN Router. Includes every event that the VPN Router generates. Also, display detailed, normal, and urgent events.

Default

The date defaults to today's date. If the year is omitted, it defaults to the current year. The default display level is normal.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

logging history
logging facility syslog
show logging config
show logging events
show logging security

Example

This example shows the system log output for normal messages. The urgent messages are marked with an asterisk (*).

```
CES# show logging syslog
*14:01:52 tEvtLgMgr 0 : FTP Backup [13] Update completed
*15:01:52 tEvtLgMgr 0 : FTP Backup [13] Redundant Disk is not available
*15:01:52 tEvtLgMgr 0 : FTP Backup [13] Update completed
*15:09:09 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off
Due to Timeo$
15:09:09 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2879 logged
out
*15:09:09 tEvtLgMgr 0 : Security [13] Management: Forcing admin to
re-supply userid
15:09:11 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2880 master
admin authen$
15:09:12 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2880
Management: logged $
*15:27:33 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off
Due to Timeo$
15:27:33 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2880 logged
out
*15:27:37 tEvtLgMgr 0 : Security [13] Management: Request for
manager.htm denied, re$
15:27:39 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2881 master
admin authen$
15:27:40 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2881
Management: logged $
15:27:57 tHttpdTask 0 : DbSysLog.CaptureLevel changed from 'NORMAL' to
'ALL' by use$
15:28:54 tHttpdTask 0 : DbSysLog.CaptureLevel changed from 'URGENT' to
'NORMAL' by $
15:29:04 tEvtLgMgr 0 :Security [12] Session: LOCAL[admin]:2882 loggedout
```

show safe-mode

Use this command to display safe mode parameters.



Note: This command is not available on the Nortel VPN Router 1010, 1050, or 1100. The Nortel VPN Router 1010, 1050, and 1100 do not have safe mode.

Syntax

```
show safe-mode
```

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

safe-mode duration
safe-mode enable

Example

```
CES# show safe-mode
  Safe-mode:            ENABLED
  Safe-mode duration:   5
CES#
```

show serial-port

Use this command to display the parameters for the motherboard serial port.

Syntax

show serial-port

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

baud-rate
menu-access-level
mode
modem-initialization

Example

```
CES# show serial-port
  Serial-port Menu Access Level:    UNRESTRICTED
  Serial-port Mode:                 Serial Menu
  Serial-port Baud Rate:            9600
  Serial-port Modem Initialization: ATZ
CES#
```

show software version

This command displays the software versions that are available on your system for an upgrade.

Syntax

show software version

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

boot system
retrieve software

Example

```
CES# show software version
  Software Version:
         V01_00.00
         V30_01.03
```

show system forwarding

Use this command to display all system forwarding settings.

Syntax

show system forwarding

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

system forwarding proxy-arp branch-office-tunnels enable
system forwarding proxy-arp physical-interfaces enable
system forwarding gratuitous-arp enable
system forwarding tunnel-to-tunnel-traffic EU-to-EU enable
system forwarding tunnel-to-tunnel-traffic EU-to-BO enable
system forwarding tunnel-to-tunnel-traffic BO-to-BO enable

Example

```
CES# show system forwarding
  system forwarding proxy-arp End-User tunnel enabled
  system forwarding proxy-arp Branch-Office tunnel disabled
  system forwarding proxy-arp Physical Interfaces disabled
  system forwarding gratuitous-arp disabled
  system forwarding tunnel-to-tunnel-traffic EU-to-EU disabled
  system forwarding tunnel-to-tunnel-traffic EU-to-BO disabled
  system forwarding tunnel-to-tunnel-traffic BO-to-BO disabled
CES#
```

Chapter 4
Global Configuration mode commands

This chapter describes the Global Configuration CLI commands.

Command	Page
arp	165
async-over-tcp enable	166
async-over-tcp local-ip-address	168
async-over-tcp peer-ip-address	170
async-over-tcp port number	172
async-over-tcp private	174
async-over-tcp public	176
async-over-tcp originator	177
async-over-tcp num-of-ticks	179
audible alarm	180
authentication-banner	181
auto-save-logging enable	182
auto-save-logging max-files	180
console mode	186
crypto exp	186
data-collection-interval	189
enable-ping	190
event-log size	191
exit	193
ftp-server access-list	195
ftp-server passive	196

Command	Page
ftp-server port	198
help	199
hostname	200
http access-list	202
http port	203
https private port	206
ip http server	208
ldap	209
load	211
log-file-lifetime	212
logging history	213
logging save-log	215
logout	217
ping-address	217
ping-interval	219
prompt	220
restrict	221
safe-mode duration	223
safe-mode enable	225
service ssh	226
service ssh sftp	229
show ssh-server	232
snmp-server access-list	233
snmp-server port	235
ssh-server	236
system forwarding gratuitous-arp enable	237
system forwarding nexthop-forward enable	239
system forwarding proxy-arp branch-office-tunnels enable	240
system forwarding proxy-arp physical-interfaces enable	241
system forwarding tunnel-to-tunnel-traffic BO-to-BO enable	243

Command	Page
system forwarding tunnel-to-tunnel-traffic EU-to-BO enable	245
system forwarding tunnel-to-tunnel-traffic EU-to-EU enable	246
system-log-to-file enable	248
telnet access-list	249
telnet port	251
validate	252

arp

Use this command to specify a static Address Resolution Protocol (ARP) entry in the ARP cache. Use the **no** form of the command to delete the static ARP entry.

Syntax

```
arp <ip-address> <hardware-address>
no arp <ip-address>
```

Parameters

ip-address	Specifies the IP address of the ARP entry.
hardware-address	Specifies the MAC address of the ARP entry.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

```
clear arp-cache
show arp
```

Example

The following example configures a static ARP entry.

```
CES(config)# arp 192.34.5.2 00:e0:7b:58:71:e1
```

The following example deletes a static ARP entry.

```
CES(config)# no arp 192.34.5.2
```

async-over-tcp enable

Use this command to enable or disable async-over-tcp function.

Syntax

```
aot enable
no aot enable
```

Parameters

None

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

None

Prerequisites

None

Related commands

None

Example

Example of a successful help for this command:

```
CES(config)# aot enable ?
local-ip-address        Local IP address
num-of-ticks            Number of ticks between frames
originator              Who initiates TCP connection
peer-ip-address         Peer IP address
port number             Port number
private                 Private
public                  Public
<cr>
```

Example of a successful execution:

```
CES(config)# aot enable
CES(config)#

CES(config)# no aot enable
CES(config)#
```

async-over-tcp local-ip-address

Use this command to configure local IP address.

Syntax

aot local-ip-address *<ip address>*

Parameters

None

Default

0.0.0.0

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

None

Prerequisites

None

Related commands

None

Example

Example of a successful help for this command:

```
CES(config)# aot local-ip-address 20.1.1.1 ?
enable                  Enables async over tcp
num-of-ticks            Number of ticks between frames
originator              Who initiates TCP connection
peer-ip-address         Peer IP address
port number             Port number
private                 Private
public                  Public
<cr>
```

Example of a successful execution:

```
CES(config)# aot local-ip-address 20.1.1.1
CES(config)#
```

async-over-tcp peer-ip-address

Use this command to configure peer IP address.

Syntax

aot peer-ip-address

Parameters

None

Default

0.0.0.0

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

None

Prerequisites

None

Related commands

None

Example

Example of a successful help for this command:

```
CES(config)# aot peer-ip-address 30.1.1.1 ?
enable                  Enables async over tcp
local-ip-address        Local IP address
num-of-ticks            Number of ticks between frames
originator              Who initiates TCP connection
port number             Port number
private                 Private
public                  Public
<cr>
```

Example of a successful execution:

```
CES(config)# aot peer-ip-address 30.1.1.1
CES(config)#
```

async-over-tcp port number

Use this command to set the port number.

Syntax

aot port-number <*port number*>

Parameters

None

Default

none

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

None

Prerequisites

None

Related commands

None

Example

Example of a successful help for this command:

```
CES(config)# aot port-number 1000 ?
enable                  Enables async over tcp
num-of-ticks            Number of ticks between frames
originator              Who initiates TCP connection
peer-ip-address         Peer IP address
port number             Port number
private                 Private
public                  Public
<cr>
```

Example of a successful execution:

```
CES(config)# aot local-ip-address 20.1.1.1
CES(config)#
```

async-over-tcp private

Use this command to enable a private port.

Syntax

aot private enable

Parameters

None

Default

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

None

Prerequisites

None

Related commands

None

Example

```
CES(config)# aot port-number 10000 private enable
CES(config)#
```

async-over-tcp public

Use this command to enable a public port.

Syntax

aot public enable

Parameters

None

Default

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

None

Prerequisites

None

Related commands

None

Example

```
CES(config)# aot port-number 10000 public enable
CES(config)#
```

async-over-tcp originator

Use this command to configure originator.

Syntax

aot originator <*self* | *peer*>

Parameters

None

Default

Self

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

None

Prerequisites

None

Related commands

None

Example

Example of a successful help for this command:

```
CES(config)# aot originator ?
peer                    Peer
self                    Self
<cr>
```

Example of a successful execution:

```
CES(config)# aot originator self
CES(config)#
```

async-over-tcp num-of-ticks

Use this command to configure number of ticks between frames. Each tick represents 16.6 milliseconds.

Syntax

aot num-of-ticks <*number*>

Parameters

None

Default

1

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

None

Prerequisites

None

Related commands

None

Example

Example of a successful help for this command:

```
CES(config)# aot num-of-ticks ?
<1-60>
```

Example of a successful execution:

```
CES(config)# aot num-of-ticks 10
CES(config)#
```

audible alarm

This command enables and disables the audible alarm that is sounded on the VPN Router under certain error conditions.

Syntax

```
audible alarm
no audible alarm
```

Parameters

None

Default

Audible alarm is enabled.

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

show health

Example

These commands disable and then reenable the VPN Router alarm.

```
CES(config)# no audible alarm
CES(config)# audible alarm
```

authentication-banner

Use this command to configure the authentication banner message. Use the **no** form of this command to disable the authentication banner message.

Syntax

authentication-banner {**ftp | http | https | serial | ssh | telnet} enable**
no authentication-banner {**ftp | http | https | serial | ssh | telnet}**

Parameters

None

Default

Authentication banner is disabled.

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

banner

Example

These commands enable the banner for HTTP authentication, and then disable the banner.

```
CES(config)# authentication-banner http
CES(config)# no authentication-banner http
```

auto-save-logging enable

Use this command to enable auto-save-logging function. Use the **no** form of this command to disable auto-save-logging.

Syntax

[no] auto-save-logging enable

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

auto-save-logging max-files <*number*>

Example

Example of a successful help for this command:

```
CES# auto-save-logging ?
enable   Enables auto-save-logging function

CES# no auto-save-logging ?
enable   Disables auto-save-logging function
```

Example of a successful enabling of auto-save-logging:

```
CES# auto-save-logging enable
CES#
```

Example of a successful disabling of auto-save-logging:

```
CES# no auto-save-logging enable
CES#
```

auto-save-logging max-files

Use this command to configure the max number of auto-save-logging files.

Syntax

auto-save-logging max files *number*

Parameters

number	Maximum number of saved files

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

auto-save-logging enable
no auto-save-logging enable

Example

Example of a successful help for this command:

```
CES(config)# auto-save-logging ?
max-files   Maximum number of saved files

CES(config)# auto-save-logging max files ?
10
15
20
25
30
5
```

Example of a successful execution:

```
CES(config)# auto-save-logging max files <10>
CES(config)#
```

console mode

This CLI command allows you to emulate CLI commands that were available in earlier versions of Nortel VPN Router software.

This command controls which menu items are visible on the serial port console for the VPN Router, and what CLI commands can be used.

When you use this command is used to place the VPN Router in one of the two restricted modes, only the following CLI commands are available:

Table 6 Restricted mode commands

Restricted 1	Restricted 2
boot	boot
clock	clock
copy	copy
disable	disable
enable	enable
exit	exit
help	help
reload	reload
retrieve	retrieve
terminal	terminal

Because no Global Configuration mode commands are allowed, placing the VPN Router in a restricted mode causes the CLI to return to Privileged EXEC mode on the Telnet session where the command is issued. Other Telnet sessions are not forced back to Privileged EXEC mode, but they only support the CLI command set listed in Table 6.

The VPN Router can be reset to an unrestricted mode on the System > Settings Web management page.

Syntax

console mode {**restricted1** | **restricted2** | **show**}

Parameters

restricted1	The system reset and reload commands to change the IP interface address and mask are enabled within the serial menu.
restricted2	Only the system reload commands are enabled. The reload command in the CLI will only support the boot-safe and boot-normal parameters within the serial console mode.
show	Display the current console mode setting.

Default

The system boots in unrestricted mode, where all commands are enabled.

Command mode

Global Configuration

Next command mode

Global Configuration (`console mode show`) or Privileged EXEC

Related commands

menu-access-level
reload
reload at
reload in
reload no-sessions

Example

This example shows the default console mode setting, and how setting the console mode to restricted forces the user back to Privileged EXEC mode and limits the available CLI commands.

```
CES(config)# console mode show
CONSOLE MODE is set to UNRESTRICTED.
CES(config)# console mode restricted1
CONSOLE MODE has been set to RESTRICTED1.
```

crypto exp

Use this command to configure the number of days from expiration when certificates are considered about to expire.

Syntax

crypto exp

Parameters

<7-365>	Number of days

Default

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

Example

```
CES(config)# crypto exp <value>
CES(config)#
```

data-collection-interval

Use this command to set the data collection interval. This interval specifies the number of minutes (from 1 through 5) that the VPN Router waits before it collects new data for the log. By default, this interval is set to 2 minutes.

Syntax

data-collection-interval {**1** | **2** | **3** | **4** | **5**}

Parameters

None

Default

2 minutes

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show data-collection-interval

Example

```
CES(config)# data-collection-interval 3
CES(config)#
```

enable-ping

Use this command to enable validation of public default routes.

Syntax

enable-ping
no enable-ping

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

ping-interval

Example

```
CES(config)# router static enable-ping
CES(config)# no router static enable-ping
```

event-log size

Use this command to set the number of entries to store in the event log. You can specify a value of 1000 or 2000.

Syntax

event-log size {**1000** | **2000**}

Parameters

None

Default

2000

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show event-log size

Example

The following example sets the event log size to 1000 entries.

```
CES(config)# event-log size 1000
CES(config)#
```

exit

This command allows you to exit any configuration mode or to close an active Telnet session if you use the command when in User EXEC mode.

Syntax

exit

Parameters

None

Default

None

Command mode

Available in all command modes

Next command mode

Either the lower level command mode, or none because the Telnet session is terminated.

Related commands

end

Example

This example shows a user in Global Configuration mode using the **exit** command twice to end in User EXEC mode.

```
CES(config)# exit
CES# exit
CES>
```

ftp access-list

Use this command to change FTP access-list settings.

Syntax

```
ftp access-list <name of acl>
no ftp access-list <name of acl>
```

Parameters

<name of acl>	The name of the access list for FTP.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

no ftp access-list

Example

```
CES(config)# ftp access-list <name>
CES(config)#
```

ftp-server access-list

Use this command to set access lists on a ftp-server.

Syntax

ftp-server access-list <name of acl>
no ftp-server access-list <name of acl>

Parameters

access-list	Sets the name of the access-list
<name of acl>	The name of the access-list for HTTP.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

None

Example

The following example names the access list as group 1.

```
CES(config)# ftp-server access-list group1
CES(config)#
```

ftp-server passive

Use this command to set the ftp-server to passive mode.

Syntax

```
ftp-server passive
no ftp-server passive
```

Parameters

passive	Specifies passive FTP mode.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

None

Example

The following example sets the ftp server to passive mode.

```
CES(config)# ftp-server passive
CES(config)#
```

ftp-server port

Use this command to change port settings on a ftp-server.

Syntax

ftp-server port *<1-65535>*
no ftp-server access-list <name of acl>

Parameters

<1-65535>	Specifies a port number.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

None

Example

The following example sets the port number to 56.

```
CES(config)# ftp-server port 56
CES(config)#
```

help

This command displays a message about how to use the Help system.

Syntax

help

Parameters

None

Command mode

Available in all command modes

Related commands

None

Example

```
CES# help
```

To request help at any point in a command, enter a question mark **(?)**. If nothing matches, the help list is empty and you must back up until the available options appear.

Two styles of Help are provided:

- Full Help is available when you are ready to enter a command argument (**`show ?`**) and describes each possible argument.
- Partial Help is provided when an abbreviated argument is entered and you want to know what arguments match the input (**`show arp ?`**).

hostname

This command allows you to specify the DNS host name for the VPN Router. This name should correspond to the name in the DNS server to identify the management address of the VPN Router that is located on the private network.

Syntax

`hostname` *<string>*

Parameters

string	The DNS name to assign to the VPN Router. This name can have up to 64 characters.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Prerequisites

At least one DNS server should be specified.

Warning messages

```
% Validate against DNS server?
```

Related commands

no hostname
ip domain-name
ip name-server
interface management

Example

This example assigns the name MarketingCES to the VPN Router.

```
CES(config)# hostname MarketingCES
```

http access-list

Use this command to change HTTP access-list settings.

Syntax

```
http access-list <name of acl>}
no http access-list <name of acl>
```

Parameters

<name of acl>	The name of the access list for HTTP.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

no http access-list

Example

```
CES(config)# http access-list <name>
CES(config)#
```

http port

Use this command to change HTTP port settings.

Syntax

http port *<1-65535>*

Parameters

<1-65535>	Specifies a port number.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

no https port

Example

```
CES(config)# http port <value>
CES(config)#
```

https access-list

Use this command to change HTTPS access-list settings.

Syntax

```
https access-list <name of acl>
no https access-list <name of acl>
```

Parameters

<name of acl>	The name of the access list for HTTPS.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

no https access-list

Example

```
CES(config)# https acess-list <name>
CES(config)#
```

https private port

Use this command to change the port used to manage the device.

Syntax

`https private port`

Parameters

<1-65535>	Port number

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

no https private port

Example

```
CES(config)# https private port <value>
CES(config)#
```

ip http server

This command allows you to enable or disable management of the VPN Router using a Web browser. If HTTP management is disabled, the VPN Router can still be managed using the Nortel Networks CLI.

Syntax

```
ip http server
no ip http server
```

Parameters

None

Default

This feature is enabled by default on the VPN Router.

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

```
interface loopback
```

Example

This example shows how to disable management of the VPN Router using a Web browser. The VPN Router can still be configured using the CLI.

```
CES(config)# ip http server
CES(config)# no ip http server
```

ldap

This command allows you to emulate CLI commands that were available in versions of Nortel VPN Router software earlier than Version 3.0.

This command allows you to:

- Start or stop the internal LDAP server on the VPN Router.
- Export the LDAP database to an LDIF file on the VPN Router.
- Import the LDAP database from an LDIF file on the VPN Router.
- Show the current LDAP server status.

Syntax

```
ldap [help] {export | import | show | start | stop}
```

Parameters

help	The command is not executed, but some Help about the command is displayed on the terminal.
export	Export the contents of the LDAP database to the named LDIF file. The LDAP server must be stopped before an ldap export can be performed.
import	Import the contents of the LDAP database from the named LDIF file. The current LDAP database contents are replaced. The LDAP server must be stopped before an ldap import can be performed.
show	Display the status of the LDAP server.

start	Start the LDAP server. This command cannot be performed while the LDAP server is performing an export or import command. This command cannot be executed unless the LDAP server is stopped.
stop	Stop the LDAP server. This command cannot be executed unless the LDAP server is running.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% LDAP server is currently running.
% LDAP server is already running.
% LDAP server is already stopped.
% Invalid LDIF file name.
% LDIF file does not exist.
```

Example

```
CES(config)# ldap show
CES(config)# ldap stop
CES(config)# ldap export
CES(config)# ldap start
```

load

This command allows you to emulate CLI commands that were available in earlier versions of Nortel VPN Router software.

This command allows you to use the bulk load facility to execute a command file that has been previously copied to the VPN Router using FTP. The commands in the file can configure various settings on the VPN Router. This facility is used to bulk configure the VPN Router.

Syntax

load <*filename*>

Parameters

filename	The name of the file on the VPN Router that contains the bulk load commands.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Prerequisites

The LDAP server must be running.

Related commands

ldap

Example

```
CES(config)# load /ide0/system/command/test.cmd
```

log-file-lifetime

Use this command to set the lifetime of the system log files. After the number of days specified as the lifetime, the log file is overwritten. By default, system log files are maintained on the hard drive for 60 days. You can specify a value of 20, 30, 40, or 50 days.

Syntax

log-file-lifetime {**20** | **30** | **40** | **50** | **60**}

Parameters

None

Default

60 days

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show log-file-lifetime

Example

```
CES(config)# log-file-lifetime 40
CES(config)#
```

logging history

This command determines the types of messages that are stored in the system logs. By default, the system logs emergency and alert messages. After the message type level is changed, future messages stored in the system logs must be at or above the new level for them to be saved.

This command affects only syslog messages and affects how messages are stored in all logs on the VPN Router.

On the VPN Router, a warning is displayed if the level set with this command does not agree with the level required for syslog message forwarding as set using the logging facility **syslog** command.



Note: If you set the logging level to “all,” the VPN Router may experience a slight performance degradation because of the large amount of data being written to the system log.

Syntax

logging history {**all** | **detailed** | **normal** | **urgent**}
default logging history

Parameters

all	Log all messages. Use this option only on the instructions of Nortel Networks support personnel.
default	Reset logging level to **normal** (the default level) for future messages.
detailed	Log warning and notification messages, as well as critical and error conditions and emergency and alert messages.
normal	Log critical and error conditions, as well as emergency and alert messages. This setting is the default.
urgent	Log only emergency and alert messages. Urgent events are marked with an asterisk.

Default

If this command is not used, the logging level defaults to normal. The **default logging history** command resets the level to normal for future messages.

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
Does not agree with syslog forwarding settings
```

Related commands

show logging history
show logging syslog

Example

This command sets system logging on the VPN Router to store only emergency and alert messages in the system log.

```
CES(config)# logging history urgent
Logging history level is URGENT
```

This command resets system logging on the VPN Router to the default setting.

```
CES(config)# default logging history
Logging history level is NORMAL
```

logging save-log

Use this command to save event logs to a file.

Syntax

logging save-log *filename*

Parameters

filename	Name of the file for save log

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

None

Prerequisites

None

Related commands

None

Example

Example of a successful help for this command:

```
CES(config)# logging save-log ?
WORD        File name
CES(config)#
```

Example of a successful execution:

```
CES(config)# logging save-log demo
log subdirectory found
event log will be saved into /ide0/system/log/demo
Finished saving event log into /ide0/system/log/demo
CES(config)#
```

logout

This command allows you to log off the VPN Router and terminate the Telnet session. It is equivalent to using the **exit** command in User EXEC mode.

Syntax

logout

Parameters

None

Command mode

Global Configuration

Related commands

exit

Example

```
CES(config)# logout
```

ping-address

Use this command to validate by pinging this address.

Syntax

ping-address

Parameters

None

Default

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

Example

```
CES(config)# ip default-network 3.4.5.0 public ping-address
<ip address>
```

ping-interval

Use this command to validate public default routers at this interval in seconds.

Syntax

`ping-interval`

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

enable-ping

Example

```
CES(config)# router static ping-interval
```

prompt

Use this command to change the default CLI prompt. Use the **no** form of the command to reset the CLI prompt to its default value (CES).

Syntax

prompt <*string*>
no prompt

Parameters

string	Specifies the prompt. You can enter up to 32 characters. If the string contains spaces, enclose it in quotation marks.

Default

CES

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% Illegal character in prompt.
% Invalid input detected at ‘^’ marker.
```

Related commands

hostname

Example

The following example changes the prompt and shows how the new prompt persists as you navigate to other CLI modes and exit and reenter the CLI.

```
CES(config)# prompt “Chicago Central”
Chicago Central(config)# exit
Chicago Central# exit
Chicago Central> exit
Login: admin
Password: *****
Chicago Central>
```

The following example resets the prompt to its default value.

```
Chicago Central(config)# no prompt
CES(config)#
```

restrict

This command allows you to emulate CLI commands that were available in earlier versions of Nortel VPN Router software. Use this command to restrict management access to the VPN Router by allowing only control tunnel connections to it.

Syntax

```
restrict help [all | off | on | show]

restrict {off confirm | on confirm | show}
```

Parameters

help	Display online Help about the **restrict** command. You can display all available Help or you can limit the Help by specifying **off**, **on**, or **show**.
off confirm	Disable restricted mode on the VPN Router.
on confirm	Enable restricted mode on the VPN Router.
show	Display the state of restricted mode on the VPN Router: enabled or disabled.

Default

Unrestricted mode

Command mode

Global Configuration

Next command mode

Global Configuration

Prerequisites

At least one control tunnel must be configured to enable restricted mode.

Warning messages

```
ERROR: The switch is not in restricted mode.
ERROR: There are no active restricted management tunnels.
```

Related commands

bo-conn
menu-access-level
show serial-port

Example

The following example places the VPN Router in restricted mode.

```
CES(config)# restrict on confirm
CES(config)#
```

The following example displays whether the VPN Router is in restricted mode.

```
CES(config)# restrict show
Status: Switch is not in restricted mode.
Note: There are no active restricted control tunnels on this
Switch.
CES(config)#
```

safe-mode duration

Use this command to set the number of minutes that the VPN Router operates in safe mode before it attempts to reboot in normal mode. By default, the safe mode duration is set to 5 minutes.



Note: A change to the safe mode duration setting takes effect the next time that the VPN Router is booted in safe mode.

Syntax

safe-mode duration [<*minutes*>]

Parameters

minutes	Specifies the number of minutes that safe mode is in effect. Enter a value from 1 through 600 minutes. The VPN Router will automatically reboot in normal mode after this time expires.

Default

5 minutes

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

safe-mode enable
show safe-mode

Example

The following example specifies that the next time the VPN Router is booted in safe mode, the VPN Router will reboot in normal mode after 20 minutes.

```
CES(config)# safe-mode duration 20
CES(config)#
```

safe-mode enable

You can reboot the VPN Router in one of two system modes: safe mode or normal mode. Each mode has its own software image, configuration files, and LDAP database. Use this command to enable safe mode. Use the **no** form of this command to disable safe mode and reset the VPN Router to normal mode.

A system booted in safe mode can only accept secured management tunnel establishment. When the secured management tunnel is established, Telnet, HTTP, and FTP traffic can enter the VPN Router; no other VPN traffic is allowed through the secured management tunnel or the VPN Router.

In normal mode, the system operates with the normal software and configuration and transports both VPN traffic and management traffic.



Note: To change the system mode from normal to safe or the reverse, you must restart the VPN Router after you execute the command.

Syntax

```
safe-mode enable
no safe-mode enable
```

Parameters

None

Default

Normal mode (safe mode is disabled)

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

safe-mode-duration
show safe-mode

Example

The following example enables and then disables safe mode.

```
CES(config)# safe-mode enable
CES(config)# no safe-mode enable
CES(config)#
```

service ssh

Use this command to enable and disable, and restart the SSH server.

Syntax

service ssh [sftp-enable] { enable | restart }
no service ssh [sftp-enable] enable

Parameters

enable	Enables the SSH server.
restart	Restarts the SSH server.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Example

The following example enables and restarts the SSH server.

```
CES(config)# service ssh enable
CES(config)# service ssh restart
```

ssh-server access-list

Use this command to configure SSH server access-list settings.

Syntax

```
ssh-server access-list <name of acl>
no ssh-server access-list <name of acl>
```

Parameters

<name of acl>	The name of the access list for the SSH server.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

no ssh-server access-list

Example

```
CES(config)# ssh-server access-list <name>
CES(config)#
```

service ssh sftp

Use this command to enable SSH SFTP. Use the **no** form of this command to disable SSH SFTP.

Syntax

```
service ssh sftp-enable
no service ssh sftp-enable
```

Parameters

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

None

Warning messages

% The change you have made will not take effect until SSH server is restarted.

Example

The following example enables SSH SFTP.

```
CES(config)# service ssh sftp-enable
CES(config)# no service ssh sftp-enable
```

show crypto

Use this command to display encryption module.

Syntax

show crypto

Parameters

show crypto

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

show ssh-server

Example

```
CES(config)# show crypto
Displays encryption module
   Ca                   Displays certification authority
                        policy
   Certificates         Displays certificates
   Enrollment           Displays certificate enrollment
                        requests
   expiration-warning   Displays days from expiration to
                        consider certificate about to expire
   password             Displays if private key command is
                        defined
   server               Displays server certificates
   ssl                  Displays SSL
CES(config)#
```

show ssh-server

Use this command to show the parameters and the state for the SSH server.

Syntax

show ssh-server { port | state }

Parameters

port	Shows the SSH server port.
state	Specifies the state (enabled or disabled) of the SSH server.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

```
ssh-server
show sessions detail
show running-config service available
show services all
```

Example

The following example shows the SSH server port.

```
CES(config)# show ssh-server port
```

snmp-server access-list

Use this command to change access-list settings for a SNMP server.

Syntax

```
snmp-server access-list <name of acl>}
no snmp-server access-list <name of acl>
```

Parameters

<name of acl>	The name of the access list for the SNMP server.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Example

```
CES(config)# snmp-server acess-list <name>
CES(config)#
```

snmp-server port

Use this command to change port settings for a SNMP server.

Syntax

snmp-server port *<1-65535>*
no snmp-server

Parameters

<1-65535>	Specifies a port number.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Example

```
CES(config)# snmp-server port <value>
CES(config)#
```

ssh-server

Use this command to set the parameters for the ssh server.

Syntax

```
ssh-server { port <portnum> | private | public }
no ssh-server { private | public }
```

Parameters

portnum	Specifies the ssh server port.
private	Enables private interface filters on the specified ssh server port.
public	Enables public interface filters on the specified ssh server port.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

show ssh-server
show sessions detail
show services all

Example

```
CES(config)# ssh-server port 24
```

system forwarding gratuitous-arp enable

Use this command to enable or disable the forwarding of gratuitous ARP packets on the VPN Router. A gratuitous ARP packet is an unsolicited ARP request for a node's own IP address. A node may broadcast a gratuitous ARP packet to prevent its ARP entry from timing out on other nodes or to verify that no other node is using the same IP address. DHCP clients use gratuitous ARP to detect address conflicts.

Syntax

system forwarding gratuitous-arp enable
no system forwarding gratuitous-arp enable

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show system forwarding
system forwarding proxy-arp branch-office-tunnels enable
system forwarding proxy-arp physical-interfaces enable
system forwarding tunnel-to-tunnel-traffic BO-to-BO enable
system forwarding tunnel-to-tunnel-traffic EU-to-BO enable
system forwarding tunnel-to-tunnel-traffic EU-to-EU enable

Example

The following example configures the VPN Router to forward gratuitous ARP packets.

```
CES(config)# system forwarding gratuitous-arp enable
  system forwarding proxy-arp gratuitous-arp enabled
CES(config)#
```

The following example configures the VPN Router not to forward gratuitous ARP packets.

```
CES(config)# no system forwarding gratuitous-arp enable
  system forwarding proxy-arp gratuitous-arp disabled
CES(config)#
```

system forwarding nexthop-forward enable

Use this command to apply a filter on traffic between private and tunnel interface.

Syntax

```
system forwarding nexthop-forward enable
no system forwarding nexthop-forward enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Example

```
CES(config)# system forwarding nexthop-forward enable
CES(config)# no system forwarding nexthop-forward enable
```

system forwarding proxy-arp branch-office-tunnels enable

By default, the VPN Router responds to ARP requests for routes created for user tunnels (you cannot change this setting). Use this command to enable or disable Proxy ARP for branch office tunnels.

Syntax

```
system forwarding proxy-arp branch-office-tunnels enable
no system forwarding proxy-arp branch-office-tunnels enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show system forwarding
system forwarding gratuitous-arp enable
system forwarding proxy-arp physical-interfaces enable
system forwarding tunnel-to-tunnel-traffic BO-to-BO enable
system forwarding tunnel-to-tunnel-traffic EU-to-BO enable
system forwarding tunnel-to-tunnel-traffic EU-to-EU enable

Example

The following example configures the VPN Router to respond to ARP requests for routes available through branch office tunnel connections.

```
CES(config)# system forwarding proxy-arp
branch-office-tunnels enable
  system forwarding proxy-arp branch-office-tunnels enabled
CES(config)#
```

The following example configures the VPN Router to ignore ARP requests for routes available through branch office tunnel connections.

```
CES(config)# no system forwarding proxy-arp
branch-office-tunnels enable
  system forwarding proxy-arp branch-office-tunnels disabled
CES(config)#
```

system forwarding proxy-arp physical-interfaces enable

By default, the VPN Router responds to ARP requests for routes created for user tunnels (you cannot change this setting). Use this command to enable or disable Proxy ARP on all physical interfaces.

Syntax

```
system forwarding proxy-arp physical-interfaces enable
no system forwarding proxy-arp physical-interfaces enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
show system forwarding
system forwarding gratuitous-arp enable
system forwarding proxy-arp branch-office-tunnels enable
system forwarding tunnel-to-tunnel-traffic BO-to-BO enable
system forwarding tunnel-to-tunnel-traffic EU-to-BO enable
system forwarding tunnel-to-tunnel-traffic EU-to-EU enable
```

Example

The following example configures the VPN Router to respond to ARP requests for routes available through its physical interfaces.

```
CES(config)# system forwarding proxy-arp physical-interfaces
enable
  system forwarding proxy-arp physical-interfaces enabled
CES(config)#
```

The following example configures the VPN Router to ignore ARP requests for routes available through its physical interfaces.

```
CES(config)# no system forwarding proxy-arp
physical-interfaces enable
  system forwarding proxy-arp physical-interfaces disabled
CES(config)#
```

system forwarding tunnel-to-tunnel-traffic BO-to-BO enable

Use this command to enable or disable the forwarding of branch office-to-branch office traffic. By default, this option is disabled. When you enable this option, a remote user who is located on a branch office connected to the VPN Router can access resources on other branch offices connected to the VPN Router.

Syntax

```
system forwarding tunnel-to-tunnel-traffic BO-to-BO enable
no system forwarding tunnel-to-tunnel-traffic BO-to-BO
enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show system forwarding
system forwarding gratuitous-arp enable
system forwarding proxy-arp branch-office-tunnels enable
system forwarding proxy-arp physical-interfaces enable
system forwarding tunnel-to-tunnel-traffic EU-to-BO enable
system forwarding tunnel-to-tunnel-traffic EU-to-EU enable

Example

The following example enables branch office-to-branch office connections.

```
CES(config)# system forwarding tunnel-to-tunnel-traffic
BO-to-BO enable
CES(config)#
```

The following example disables branch office-to-branch office connections.

```
CES(config)# no system forwarding tunnel-to-tunnel-traffic
BO-to-BO enable
CES(config)#
```

system forwarding tunnel-to-tunnel-traffic EU-to-BO enable

Use this command to enable or disable the forwarding of end user-to-branch office traffic. By default, this option is disabled. When you enable this option, a remote user who is tunneled into the VPN Router can access resources on branch offices that are connected to the VPN Router.

Syntax

system forwarding tunnel-to-tunnel-traffic EU-to-BO enable
no system forwarding tunnel-to-tunnel-traffic EU-to-BO enable

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show system forwarding
system forwarding gratuitous-arp enable
system forwarding proxy-arp branch-office-tunnels enable
system forwarding proxy-arp physical-interfaces enable
system forwarding tunnel-to-tunnel-traffic BO-to-BO enable
system forwarding tunnel-to-tunnel-traffic EU-to-EU enable

Example

The following example enables end user-to-branch office connections.

```
CES(config)# system forwarding tunnel-to-tunnel-traffic
EU-to-BO enable
CES(config)#
```

The following example disables end user-to-branch office connections.

```
CES(config)# no system forwarding tunnel-to-tunnel-traffic
EU-to-BO enable
CES(config)#
```

system forwarding tunnel-to-tunnel-traffic EU-to-EU enable

Use this command to enable or disable the forwarding of end user-to-end user traffic. By default, this option is disabled. When you enable this option, a remote user who is tunneled into the VPN Router can access other remote users who are tunneled into the VPN Router.

Syntax

```
system forwarding tunnel-to-tunnel-traffic EU-to-EU enable
no system forwarding tunnel-to-tunnel-traffic EU-to-EU
enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
show system forwarding
system forwarding gratuitous-arp enable
system forwarding proxy-arp branch-office-tunnels enable
system forwarding proxy-arp physical-interfaces enable
system forwarding tunnel-to-tunnel-traffic BO-to-BO enable
system forwarding tunnel-to-tunnel-traffic EU-to-BO enable
```

Example

The following example enables end user-to-end user connections.

```
CES(config)# system forwarding tunnel-to-tunnel-traffic
EU-to-EU enable
CES(config)#
```

The following example disables end user-to-end user connections.

```
CES(config)# no system forwarding tunnel-to-tunnel-traffic
EU-to-EU enable
CES(config)#
```

system-log-to-file enable

Use this command to enable the VPN Router to write the system log to a file. Use the **no** form of the command to disable writing the system log to a file.

Syntax

```
system-log-to-file enable
no system-log-to-file enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show logging syslog

Example

The following example configures the VPN Router to write the system log to a file.

```
CES(config)# system-log-to-file enable
CES(config)#
```

The following example configures the VPN Router not to write the system log to a file.

```
CES(config)# no system-log-to-file enable
CES(config)#
```

telnet access-list

Use this command to set telnet access-lists.

Syntax

telnet access-list <name of acl>}
no telnet access-list <name of acl>

Parameters

<name of acl>	The name of the access list for Telnet.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Example

The following example sets the access list to group2.

```
CES(config)# telnet access-list group2
CES(config)#
```

telnet port

Use this command to change the ports used to manage the device.

Syntax

telnet port *<1-65535>*
no telnet port *<1-65535>*

Parameters

<1-65535>	Specifies a port number.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Example

The following example sets the port number to 68.

```
CES(config)# telnet port 68
CES(config)#
```

validate

Use this command to validate by pinging at intervals.

Syntax

validate

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

None

Example

CES(config)# ip default-network 1.1.1.42 public **`validate enabled`**

Chapter 5
Creating and using scripts to provision a VPN Router

This chapter provides information about how to create and use scripts to provision single or multiple Nortel VPN Router. You can create a script by typing Nortel VPN Router CLI commands into an ASCII text file or by executing the **`show running-config`** command with a file name specified.



Caution: Before you attempt to provision a Nortel VPN Router using a file generated by the **`show running-config`** command, scan the output file and edit it as described in "Editing the output file" on page 257.

The **`show running-config`** command displays information about the VPN Router's current running configuration in the form of Nortel VPN Router CLI commands. You can display these commands on your PC or workstation terminal or save them in a file.

This chapter provides information about the following topics.

Topic	Page
Creating a script with the show running-config command	256
Editing the output file	257
Guidelines for creating and executing scripts	259
Estimating provisioning time	260
Preparing to run a script file	261
Executing a script	263
show running-config command	263

Creating a script with the show running-config command

To create a script file that you can use to provision one or more VPN Routers, execute the **show running-config** command with the **file-url** option to save the configuration commands in a file. The output file is written to the system disk in the directory **system/runconf** and has the file extension **.cli**. You can then copy the output file to a PC or workstation and edit it (see "Editing the output file" on page 257).

To execute a script, use FTP to copy it to the **/system/prov** directory on the target Nortel VPN Router. As soon as you copy the script file to this directory, the VPN Router executes the commands in the script and produces an output file in the same directory. The name of the output file is the same as the **.cli** file but with the extension **.out** (for example, the file **script.cli** produces the output file **script.out**). You can copy **.out** files back to your workstation to verify whether the commands succeeded and to find and correct any errors.



Note: For examples of **.cli** script files and the resulting **.out** files, see Appendix A, "Sample scripts and output files generated by the show running-config command," on page 2109.

If you want to use the command to capture the entire configuration of the VPN Router, see "Estimating provisioning time" on page 260. To capture specific configuration information using the **show running-config** command, include only a specific configuration area (for example, users or OSPF) on the command line.

For example, to create a file that contains only information about users, enter the following command:

```
show running-config file-url usr.cli profiles users
```

You could edit the output of this command and place the edited file in the **system/prov** directory of another Nortel VPN Router to copy the user accounts.



Note: For the complete syntax of the **show running-config** command, see "show running-config command" on page 263.

Editing the output file

The output generated by the **show running-config** command does not always produce usable scripts that can be applied directly to provision a Nortel VPN Router.



Caution: In many cases, you cannot fully provision a Nortel VPN Router using the unedited output from the **show running-config** command; you must first edit the output script to ensure that the configuration commands are in the correct order.

Some portions of the **show running-config** file output can be used without editing to provision a Nortel VPN Router. For example, you can cut and paste the branch office tunnel configuration from the file generated by the **show running-config** command to create a valid script for provisioning branch office tunnels on a VPN Router. Other portions of the **show running-config** output file that can be used without editing include group configurations and user tunnel configurations.

However, in many cases you cannot use the **show running-config** file output *as is* to fully configure a new or identical Nortel VPN Router without first editing the output file. Before you use the file to completely provision a Nortel VPN Router, you must reorder the commands in the file.



Caution: To use a script generated on a Nortel VPN Router running one version of software to provision a VPN Router that is running a different version of software, you will need to edit the script file very carefully to account for differences in software functionality between the devices along with the required reordering of commands.

Reordering the commands in the output file

If necessary, reorder the configuration commands in the output file generated by the **`show running-config`** command as follows.



Note: It is assumed that the script will be used to provision a Nortel VPN Router whose configuration is set to factory defaults.

1. Services – IPsec, PPTP, L2TP, and L2F should be configured in the script before groups (both user and branch office groups) and before branch office tunnels. (The configuration of these services is generated using the **`show running-config service`** command.)
2. IP interfaces – interface IP addresses should appear in the script before any other object that depends on an interface IP address. For example, interface IP addresses should be configured before static routes, default routes, and routing interfaces.
3. To avoid misconfiguration, the provisioning script must first create certain objects before it can create other objects that depend on them. Table 7 provides a list of dependencies. Using Table 7 as a guide, reorder the configuration commands in the output file.

Table 7 Configuration file dependencies

Configure this object...	Before you configure these objects
Access list	Multicast relay, routing policy
Branch office connection	Routing policy, interface groups, multicast relay, access list
CA certificate	Branch office connection, users, IPsec branch office tunnel
Client policy	User groups
CLIP	Branch office connection
Domain set	User groups
User group	External LDAP, RADIUS authentication, users, interface rules, CA certificates, Firewall rules
Hours	User groups, branch office groups, backup interface
Interface filter	Interfaces (LAN, WAN, and Dial)
Interface group	Backup interface
NAT	Branch office connection

Table 7 Configuration file dependencies (Continued)

Configure this object...	Before you configure these objects
Networks	Branch office connection, user groups, backup interfaces
OSPF area	Routing interfaces, branch office connection
QoS classifier	QoS interface
Server certificate	Branch office connection, users, user groups
Tunnel filters	Branch office connection, user groups
RIP (dynamic routing)	Routing interfaces, branch office connection
Services (global): IPsec, PPTP, L2TP, L2F	Branch office connection, user groups, RADIUS
License key	Advanced Routing (OSPF), Firewall
VRRP[1]	Interfaces (VRRP and IP)
Interfaces (VRRP and IP)[1]	VRRP
Routing policy[1]	Branch office connection

1 Some areas of Nortel VPN Router configuration include circular references; that is, you must provision part of one object, then part of the object that depends on the first object, then another part of the first object, and so on

Guidelines for creating and executing scripts

This section provides guidelines to help you create scripts using the output of the **`show running-config`** command.



Caution: Before you attempt to provision a Nortel VPN Router using a file generated by the **`show running-config`** command, see "Editing the output file" on page 257.

- You cannot execute the **`show running-config`** command with the **`user-friendly`** option to create a script file. The **`user-friendly`** option provides a formatted, indented view of your configuration that can be saved to a file. However, this output cannot be used to provision a VPN Router.



Note: For the complete syntax of the **`show running-config`** command, see "show running-config command" on page 263.

- For VPN Routers with almost identical hardware and software configurations, you can reuse a script created on one VPN Router to provision another VPN Router by making slight modifications to the script. For example, you can delete lines that provision unsupported components or an absent port.
- To provision different Nortel VPN Router models with the same output file, you will need to edit the script file carefully because some functions and hardware used by a specific VPN Router may not be available on another VPN Router. For example, a file generated by the **`show running-config`** command on a Nortel VPN Router 1600 may not necessarily provide the same results if it is executed on a Nortel VPN Router 2700.
- In some cases, the **`show running-config`** command may not capture the complete configuration of a feature if the feature is disabled. For example, when the IP address pool for DHCP relay is set to "Any DHCP Server," the output of the configuration file may not contain information about DHCP servers specified in the DHCP Server area of the Web management screen. You can extract such information from the Web management screens and then add it to the **`.cli`** file.

Estimating provisioning time

Before you execute a script created from the **`show running-config`** command for a VPN Router with large numbers of users or branch office tunnels, consider total provisioning time.



Note: To optimize the provisioning of branch office tunnels, configure the local tunnel end points before you run the provisioning script.

To estimate the total provisioning time, see Table 8.

Table 8 Provisioning time estimates

Operation	Internal LDAP	External LDAP
Provision each new user.	10 seconds	4 seconds
Generate each new user profile using **show running-config** command.	1 second	1 second
Provision each new branch office.	15 seconds	5 seconds
Generate each new branch office using **show running-config** command.	5 seconds	5 seconds

On average it takes from 5 through 15 minutes to generate the complete configuration script when information about the users and branch office tunnels is not required. The following sample command sequence can be used to generate such a limited provisioning script:

```
show running-config admin
show running-config profile access-hours
show running-config profile bo-group
show running-config profile client-policy
show running-config profile domains
show running-config profile filters
show running-config profile groups
show running-config profile nat
show running-config profile networks
show running-config routing
show running-config server
show running-config service
show running-config system
```

Preparing to run a script file

Before you run a script, make sure to edit the configuration commands as described in "Editing the output file" on page 257. The following steps describe how to add the appropriate system commands to a file generated by the **`show running-config`** command in preparation for executing it on a VPN Router.

1. Copy the **.cli** file from the VPN Router to a PC or workstation.
2. Open the file using a text editor (such as Notepad or Wordpad).

Note: To create a script file from scratch, type each command into a text file just as you would type commands at the appropriate CLI prompt.

3. Enter **enable** on the first line of the file.
4. Enter the administrator password on the second line of the file (the default password is “setup”).
5. Enter **configure terminal** on the third line of the file.
6. If you are creating a file, enter the CLI commands that you want to execute.

Note: Use an exclamation point (**!**) to introduce comments in a Nortel VPN Router script (lines that begin with **!** are ignored during provisioning).

7. At the end of the file, enter three **exit** commands.

   The first **exit** command exits Global Configuration mode, the second one exits Privileged EXEC mode, and the last one exits User EXEC mode and therefore, the command line interface.

8. Save the file as an ASCII text file with the extension **.cli**, for example, **c600_config.cli**.

For examples of **.cli** script files and the resulting **.out** files, see Appendix A, “Sample scripts and output files generated by the show running-config command,” on page 2109.”

Executing a script

When the script is ready to execute, you copy it to a specific directory on the VPN Router that you want to provision.



Caution: The script is automatically executed as soon as you transfer it to the **system/prov** directory on the VPN Router.

To execute the script:

1. Open an FTP connection to the management IP address of the VPN Router that you want to provision using the script file.
2. Copy the **.cli** script file to the **system/prov** directory on the VPN Router.

   After you copy the file to the VPN Router, the VPN Router executes the CLI commands specified in the script and generates a **.out** file in the **system/prov** directory with the same name as the **.cli** file that was executed.
3. Use FTP to copy the **.out** file to a PC or workstation to view and edit it.

   The output file contains information about the commands executed and any messages (confirmations, warnings, and errors) generated by the execution of the **.cli** file.



Note: An **add** command that attempts to create an object that already exists will generate an error message.

show running-config command

This section provides information about the **show running-config** command, which you can use as follows:

- Display the active configuration of the VPN Router.
- Save the active configuration to a file.

You can use a file generated with the **show running-config** command as the basis for a new provisioning script, or you can add a new file to an existing script. For information about configuring Nortel VPN Routers with scripts, see "Creating a script with the show running-config command" on page 256.

Syntax

show running-config [**user-friendly**] [**file-url** <*file-name*>] [**admin** [<*type1*>] | **profile** [<*type2*>] | **qos** [<*type3*>] | **routing** [<*type4*>] | **server** [<*type5*>] | **service** [<*type6*>] | **system** [<*type7*>]]

or

show running-config [**user-friendly**] [**file-url** <*file-name*>] **admin** [**administrator** | **backup** | **install-keys** | **snmp** | **trap**]

show running-config [**user-friendly**] [**file-url** <*file-name*>] **profile** [**access-hours** | **bo-conn** | **bo-group** | **client-policy** | **domains** | **filters** | **groups** | **nat** | **networks** | **users**]

show running-config [**user-friendly**] [**file-url** <*file-name*>] **qos** [**bandwidth-management** | **interfaces** | **mf-class**]

show running-config [**user-friendly**] [**file-url** <*file-name*>] **routing** [**access-list** | **car** | **dhcp-relay** | **ecmp** | **interface** | **multicast-relay** | **ospf** | **policy** | **rip** | **static** | **vrrp**]

show running-config [**user-friendly**] [**file-url** <*file-name*>] **server** [**authentication ldap-server** | **dhcp-proxy-server** | **dhcp-server** | **ldap** | **radius**]

show running-config [**user-friendly**] [**file-url** <*file-name*>] **service** [**available** | **firewall** | **fwua** | **ipsec** | **l2f** | **l2tp** | **policy** | **pptp** | **radius** | **ssl** | **syslog** | **tunnel-guard**]

show running-config [**user-friendly**] [**file-url** <*file-name*>] **system** [**accelerator** | **atm** | **audible** | **bri** | **clip** | **dial** | **forwarding** | **identity** | **ipx** | **lan** | **prompt** | **settings** | **time** | **wan**]

Parameters

user-friendly	Display configuration information as formatted, indented output. You can save the output to a file, but you cannot use the file as a script to provision a VPN Router.
file-url	Send output to a file.
file-name	Specifies the name of the file that will contain the command output (type up to 8 characters).
admin	Show administrator configuration.
profile	Show profile configuration.
qos	Show quality of service configuration.
routing	Show routing configuration.
server	Show server configuration.
service	Show service configuration.
system	Show system configuration.
type1	Specifies the type of administrator configuration: **administrator**, **backup**, **install-keys**, **snmp**, or **trap**.
type2	Specifies the type of profile: **access-hours**, **bo-conn**, **bo-group**, **client-policy**, **domains**, **filters**, **groups**, **nat**, **networks**, or **users**.
type3	Specifies the type of quality of service configuration: **bandwidth-management**, **interfaces**, or **mf-class**.
type4	Specifies the type of routing: **access-list**, **car**, **dhcp-relay**, **ecmp**, **interface**, **multicast-relay**, **ospf**, **policy**, **rip**, **static**, or **vrrp**.
type5	Specifies the type of server: **authentication ldap-server**, **dhcp-proxy-server**, **dhcp-server**, **ldap**, or **radius**.
type6	Specifies the type of service: **available**, **demand**, **firewall**, **fwua**, **ipsec**, **l2f**, **l2tp**, **policy**, **pptp**, **radius**, **ssl**, **syslog**, or **tunnel-guard**.
type7	Specifies the type of system configuration: **accelerator**, **atm**, **audible**, **bri**, **clip**, **dial**, **forwarding, identity**, **ipx**, **lan**, **prompt**, **settings**, **time**, or **wan**.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management – Manage
User Management – None

Example

Following are examples of the output generated by the **show running-config** command. For an example of the output displayed by the **user-friendly** option, see the example on page 269.

Note: For examples of how to provision a VPN Router using this command, see Appendix A, "Sample scripts and output files generated by the show running-config command," on page 2109.

The following command displays the running configuration for system identity.

```
CES# show running-config system identity
! System Identity Configuration
ip address 10.0.3.121
ip name-server 0.0.0.0
```

The following command displays the running configuration for servers.

```
CES# show running-config server
radius-server domain-delimiter @
radius-server prefix-delimiter \
radius-server default-group "/Base"
no radius-server error-code-pass-thru enable
no radius-server suffix-remove
no radius-server prefix-remove
aaa authorization network radius
```

```
no radius-server authentication challenge
no radius-server authentication response
no radius-server authentication ms-chap version 1
radius-server authentication ms-chap version 1 rfc-2548
no radius-server authentication ms-chap version 2
radius-server authentication chap
radius-server authentication pap
radius-server retransmit 3
radius-server timeout 3
radius-server primary disabled
radius-server alternate1 disabled
radius-server alternate2 disabled
aaa accounting network radius
accounting radius-server disabled
aaa accounting session update  00:30:00
no aaa accounting timeout enable
no aaa accounting update
aaa accounting update 00:30:00
clear accounting 60
ldap-server source internal
ldap-server internal domain-delimiter @
no ldap-server internal remove-suffix
aaa authentication ldap-server
proxy ldap-server domain-delimiter  @
no proxy ldap-server remove-suffix
proxy ldap-server default-group "/Base"
no proxy ldap-server host master
no proxy ldap-server host slave1
no proxy ldap-server host slave2
no proxy ldap-server digital-certificate
proxy ldap-server mode basic
proxy ldap-server subject-dn " " subject-alt-name " " ca " "
no proxy ldap-server uid
no proxy ldap-server password
no proxy ldap-server ldap-filter
proxy ldap-server server-type 0
no proxy ldap-server pwd-timestamp-attr
proxy ldap-server pwd-life-time 0
no proxy ldap-server contivity-group
no proxy ldap-server filter
no proxy ldap-server ip-address
no proxy ldap-server net-mask
proxy ldap-server timeout 4
ip address-pool local-pool
```

```
ip address-pool external-dhcp
ip address-pool external-dhcp any
ip address-pool external-dhcp cache-size 1
ip address-pool external-dhcp blackout-interval 300
ip address-pool external-dhcp address-release
ip address-pool external-dhcp blackout-interval override
ip address-pool internal-dhcp
ip address-pool internal-dhcp cache-size 1
ip address-pool internal-dhcp blackout-interval 300
ip address-pool internal-dhcp address-release
ip address-pool internal-dhcp blackout-interval override
ip address-pool local-pool blackout-interval 0
ip address-pool local-pool exhausted-amount 70
ip address-pool local-pool unavailable failover
ip dhcp server pool
lease default 0 12 0 0
lease maximum 1 0 0 0
exit
ip dhcp server pool network 172.16.121.0 mask 255.255.255.0
name "test"
lease default 0 12 0 0
lease maximum 1 0 0 0
exit
service dhcp enable
```

Example—display formatted by the user-friendly option

The following example shows the format of configuration information for the same LAN interfaces generated by the **show running-config** command with and without the **user-friendly** option.



Note: You cannot use the output generated with the **user-friendly** option to create a script file.

The following command displays the configuration of LAN interfaces on a VPN Router. You can save this output to a file to create a script.

```
CES# show running-config system lan
interface FastEthernet 0/1
ip address 47.17.248.29 255.255.248.0
filter "deny all"
speed auto
```

```
no dot1q enable
qos ingress-dscp-map enable
qos egress-dscp-map enable
no mac-pause
no mtu
no service dhcp enable
no tcp-mss enable
no tcp-mss
arp timeout 1200
exit
interface FastEthernet 1/1
no shutdown
filter "deny all"
public
speed auto
no dot1q enable
no qos ingress-dscp-map enable
no qos egress-dscp-map enable
no mac-pause
no mtu
no service dhcp enable
no tcp-mss enable
no tcp-mss
arp timeout 1200
exit
CES#
```

The following command displays the same configuration of LAN interfaces using the **user-friendly** option. In user-friendly mode, the output from the **show running-config** command differs from normal mode as follows:

- Commands are grouped into logical sections with titles and are indented according to their CLI configuration mode.
- Commands that set parameters to their default values are not included.



Note: You cannot use output generated by the **user-friendly** option to create a script.

```
CES# show running-config user-friendly system lan
! [System Lan Interface Configurations]
    interface FastEthernet 0/1
!   [CLI mode (config-if)#]
```

```
      ip address 47.17.248.29 255.255.248.0
      filter "deny all"
      qos ingress-dscp-map enable
      qos egress-dscp-map enable
      no service dhcp enable
      exit
!   [CLI mode (config)#]
    interface FastEthernet 1/1
!   [CLI mode (config-if)#]
      filter "deny all"
      no service dhcp enable
      exit
!   [CLI mode (config)#]
! [System Lan Interface Configurations (END)]
!
CES#
```

Chapter 6
Group, filters, users, branch office group configuration commands

This chapter describes group, filter, user, branch office group connectivity, and branch office group IPsec configuration commands. You must first enter the appropriate mode, for example, group connectivity /Base. This chapter includes descriptions of the following commands:

Command	Page
access-hours	275
action	278
action nexthop	279
add-rule	280
address	282
administration group-manage	283
administration switch-manage	285
administration uid	287
administration users-manage	288
antireplay enable	290
authentication (Branch Office Group RIP or Branch Office Group OSPF)	292
authentication (Group IPsec Tunnel)	293
authentication (L2TP, PPTP, L2F)	295
banner	297
bo-group	298
client	300
client-address	302

Command	Page
client auto-connect	303
client auto-connect networks	304
client dynamic-dns enable	306
client failover-tuning	307
client failover-tuning interval	309
client failover-tuning retransmissions	310
client nat interval	311
client policy	312
client screen-saver activation-time	314
client screen-saver password	315
committed rate	316
compress	318
connection	319
contact	320
dead-interval	322
default	323
df-bit	325
direction	327
display-banner	328
dynamic-authenticate	329
encryption	331
encryption ike	333
excess action	336
excess rate	337
exit	339
export bo-static-metric	340
export default-metric	341
export ospf-metric	342
export static-metric	343
filters (Group Connectivity Configuration)	344

Command	Page
filter add	346
filter rule add	348
forced-logoff	350
group (Global Configuration Command)	351
group	353
hello-interval	355
idle-timeout	356
import default-route	357
initial-contact enable	358
ip address	360
ip address-pool	361
ip address-src-	362
ip domain-name	364
ipsec issuer-ca	365
ipsec server-ca (User Configuration)	366
ipsec subject-alt-name	368
ipsec subject-dn	369
ipsec uid (User Configuration)	370
ipsec uid pwchange enable	372
ipsec-transport	373
ipx	374
isakmp-retransmission interval	375
isakmp-retransmission max-attempts	377
keepalive interval	378
keepalive ondemand-conn	379
l2f uid (User Configuration)	380
l2tp uid (User Configuration)	382
login max-attempts	383
logins	384
logoff-notification-interval	385

Command	Page
move-rule	387
nailed-up	388
nat-traversal	389
no bo-group	391
no group	392
nortel-client action	394
nortel-client filter	396
nortel-client message	397
nortel-client version	399
no uid lockout	400
password	401
password-storage	403
pfs	404
poison-reverse	405
port	406
ppp-links max-number	407
pptp uid (User Configuration)	409
priority	410
priority call-admission	411
priority forwarding	413
receive version	414
rekey data-count	415
rekey timeout	417
remove-rule	418
retransmit-interval	419
rsvp	421
rsvp token-bucket	422
send version	423
server	425
show bo-group	427

Command	Page
show filters	428
show groups	430
show users	432
split inverse-tunnel-network	433
split tunneling	435
split tunnel-networks	436
static-ipaddress (Group Connectivity Configuration)	438
static-ipaddress (User Configuration)	439
static-subnet-mask	440
transmit-delay	442
use address	443
use dest-port	444
use nexthop-addr	446
use protocol	447
use src-port	449
user add	450
vendor-id	452
wins address	453

access-hours

This command specifies the time ranges during which access is allowed for users in this group. It is the same for the Group Connectivity Configuration and Branch Office Group IPsec configuration modes.

Syntax

access-hours {**anytime** | **weekdays** | **weekends** | <*name*>}

Parameters

anytime	Access is allowed anytime.
weekdays	Access is allowed only on weekdays.
weekends	Access is allowed only on weekends.
name	User-defined access hours.

Default

Anytime

Command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only available in Connectivity Configuration mode.

Warning messages

```
% Access hours do not exist.
```

Related commands

idle-timeout

Example

```
CES(config-group/con)# access-hours anytime
CES(config-bo_group/con)# access-hours anytime
```

action

This command sets the action for the current filter rule to the named action and is used when defining filter rules.

Syntax

```
action {permit | deny}
```

Parameters

permit	Sets the action for the current filter rule to permit
deny	Sets the action for the current filter rule to deny.

Default

For a new filter rule, the default action is permit.

Command mode

Rule Configuration

Next command mode

Rule Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

address
connection
direction
filter add
protocol
rule add
use
port

Example

These commands modify the existing tunnel filter “permit FTP/in” rule to permit traffic.

```
CES(config)# filter tunnel rule "permit FTP/in"
CES(config-rule)# action permit
CES(config-rule)# exit
```

action nexthop

Use this command to support the next hop selection.

Syntax

action nexthop

Parameters

Default

Command mode

Filter Rule Configuration

Next command mode

Filter Rule Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

Example

```
CES(config/rule)# action nexthop
```

add-rule

This command adds the specified filter rule to the current filter set. Filter sets and filter rules are divided into interface and tunnel types. A tunnel filter set can only contain tunnel filter rules. The same is true for interface filter sets and rules.

Syntax

add-rule <*rulename*>

Parameters

rulename	The name of the rule to add to the current filter. This argument must be enclosed in double quotes if it contains spaces. The rule name cannot contain more than 64 characters.

Default

None

Command mode

Filter Configuration

Next command mode

Filter Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

`% Rule xxx does not exist.`

Related commands

`filter add`
`move-rule`
`remove-rule`
`rule add`

Example

```
CES(config-filter)# add-rule DenyFtpRule
```

address

This command is used to maintain named addresses and sets their IP address and mask values. To add a named address to a filter rule, see the **use address** command. Addresses are used when defining filter rules. The **no** variant of the command is used to delete an existing address definition. Address definitions cannot be deleted if they are being used in any filter rules.

Syntax

address <*address_name*> **ip** <*ip_address*> **mask** <*ip_mask*>
no address <*address_name*>

Parameters

address_name	The name of the address. This must be enclosed in quotes if the name contains spaces. The name cannot contain more than 64 characters.
ip	Indicates IP protocol.
ip_address	The IP address of the address.
mask	Indicates mask will be used.
ip_mask	The IP mask of the address in the form *xxx.xxx.xxx.xxx*.

Default

None

Command mode

Rule Configuration

Next command mode

Rule Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Address definition is in use.
% Invalid IP address.
% Invalid IP mask.
```

Related commands

rule add
use address

Example

In this example an address definition named “TenNet” is defined with the specified IP address and mask values. To add this address to a rule, see the **use address** command.

```
CES(config/rule)# address "TenNet" ip 10.0.0.0 mask
255.255.0.0
```

administration group-manage

Enter group name that user can administer. These rights are specified against a node within the groups tree. If the administrative user is given rights rooted at the /Base group, they can modify any user setting on the VPN Router. See the **administration uid** command to create an administrator account for the user.

Syntax

administration group-manage <*group_name*>

Parameters

group_name	The name of the LDAP group

Default

None

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Warning messages

```
% Group xxx does not exist.
% You need to create an admin account first.
```

Related commands

administration switch-manage
administration users-manage
administration uid

Example

In this example, the user (Mister X) is given an administrative login (george with the password martin) that can change the group settings on the VPN Router for the group /Base/cola/test.

```
CES(config)# user “Mister X” /Base/Cola
CES(config-user)# administration uid “george” password
“martin”
CES(config-user)# administration group-manage /Base/Cola/
test
CES(config-user)# exit
```

administration switch-manage

This command is used to define the management rights for a user definition that has an administrative login. See the **`administration uid`** command to create one.

Syntax

`administration switch-manage` {**`view`** | **`manage`** | **`none`**}

Parameters

view	The administrative login can view device-related settings on the VPN Router.
manage	The administrative login can view and modify device-related settings on the VPN Router.
none	No device management rights are assigned; any pre-existing management rights are revoked.

Default

By default, a new administrative login has no device management rights.

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

The administrative user ID (administrative login) must already be set.

Warning messages

```
% This user does not have an administrative uid.
```

Related commands

administration group-manage
administration users-manage
administration uid

Example

This command modifies the administrative login for this user so that the user can view device settings.

```
CES(config)# user “Mister X” group /Base/Cola
CES(config-user)# administration switch-manage view
CES(config-user)# exit
```

administration uid

This command creates an administration login for a user. It specifies the login ID and password for the user. Use the related commands to define the extent of administrative privileges allowed. Use the **no** form of the command to delete the administration login for this user.

Syntax

```
administration uid <user-id> password <password>
no administration uid
```

Parameters

user-id	Specifies the user ID for the administration login.
password	Specifies a password for the administrator login. The password can have as many as 32 characters but cannot contain spaces.

Default

None

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Warning messages

```
% UID already exists.
```

Related commands

administration group-manage
administration users-manage
administration switch-manage

Example

The following example sets an administrator user ID and password.

```
CES(config-user)# administration uid jsmith password
gwcf2bTd
```

The following example deletes the administrator user ID.

```
CES(config-user)# no administration uid
```

administration users-manage

This command is used to define the user management rights for a user definition that has an administrative login. The user manage rights specify whether the user logging on as an administrative user can view and/or modify user settings on the VPN Router. These rights are specified against a node within the groups tree. If the administrative user is given rights rooted at the /Base group, they can modify any user setting on the VPN Router.

Syntax

administration users-manage {**view** | **manage** | **none**}

Parameters

view	The administrative login can view user-related settings on the VPN Router.
manage	The administrative login can modify and view user-related settings on the VPN Router.
none	No user manage rights.

Default

By default, a new administrative login has no user management rights.

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

The administrative user id (administrative login) must already be set. See the **`administration uid`** command. The specified group must already exist.

Warning messages

```
% This user does not have an administrative uid.
```

Related commands

```
administration switch-manage
administration group-manage
administration uid
```

Example

These commands modify the administrative login for this user so that the administrative login can view settings for user accounts in and below the /Base/Cola group.

```
CES(config)# user “Mister X” group /Base/Cola
CES(config-user)# administration user-manage view
CES(config-user)# exit
```

antireplay enable

Use this command to enable the antireplay service for a group or branch office group. The antireplay service uses session cookies to protect against authentication replay attacks. Use the **no** form of the command to disable this service.

Note: The antireplay service must be disabled if you use IPsec tunnels over LANs or WANs.

Syntax

```
antireplay enable
no antireplay enable
```

Parameters

None

Default

Disabled

Command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Next command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

encryption

Example

The following example enables the antireplay service for the user group /Base.

```
CES(config)# group ipsec /Base
CES(config-group/ipsec)# antireplay enable
CES(config-group/ipsec)#
```

The following example disables the antireplay service for the branch office group /Base/test.

```
CES(config)# bo-group ipsec /Base/test
CES(config-bo_group/ipsec)# no antireplay enable
CES(config-bo_group)#
```

authentication (Branch Office Group RIP or Branch Office Group OSPF)

This command specifies authentication type and parameters for authentication.

Syntax

authentication {**none** | **simple** [**password** <*password*>] | **md5** [**password** <*password*> | **key** <*value*>]}

Parameters

none	Specifies no authentication algorithms will be used.
simple	Specifies the simple authentication algorithm.
md5	Specifies the simple authentication algorithm.
password	Specifies the password for authentication.
password	The password for the authentication. This must be up to 32 characters in length. The password cannot contain spaces.
key	If present, specifies the md5 authentication key. (This is only for Branch Office Group OSPF Configuration.)
value	The key value.

Default

None

Command mode

Branch Office Group RIP or Branch Office Group OSPF Configuration

Next command mode

Branch Office Group RIP or Branch Office Group OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config-bo_group/rip)# authentication simple
CES(config-bo_group/rip)# authentication simple password
Hello
CES(config-bo_group/rip)# authentication none
CES(config-bo_group/ospf)# authentication md5
CES(config-bo_group/ospf)# authentication md5 password
Goodbye
```

authentication (Group IPsec Tunnel)

This command specifies IPsec authentication methods for the group.

Syntax

authentication local {**rsa-sig** [**server-ca** <*ca*>] | **username-password**}

authentication external {**passgo-defender** | **dynamic-securid** | **groupid** <*id*> **password** <*password*> | **username-password**}

authentication external {**dynamic-securid** | **groupid** <*id*> **password** <*password*> | **username-password [ldap|radius]**}

authentication two-factor

no authentication local {**rsa-sig** [**server-ca** <*ca*>] | **username-password**}

no authentication external {**passgo-defender** | **dynamic-securid** | **groupid** <*id*> | **username-password**}

no authentication two-factor

Parameters

rsa-sig	Rivest-Shamir-Adeleman Signature – Entrust certificate authentication.
server-ca	Default server certificate.
ca	Server certificate.
passgo-defender	PassGo OnmiGuard/Defender.
dynamic-securid	Radius Security Dynamic SecurID token.
groupid	Group ID, which provides access to the VPN Router. Subsequent LDAP and RADIUS authentication is verified against the user ID.
id	Group ID.
ldap	Enable the external Lightweight Directory Access Protocol authentication server for two-factor authentication
password	Indicates group password.
password	Group password, which provides access to the VPN Router.
username-password	User name and password.
local	LDAP authentication.
radius	Enable the external Remote Access Dial In User Service authentication server for two-factor authentication
two-factor	Enables or disables two-factor authentication for the group

Default

Enabled except two-factor authentication. If you enable two-factor authentication, the router ignores the RSA configuration.

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config-group)# group ipsec /Base/test1
CES(config-group/ipsec)# authentication local rsa-sig
CES(config-group/ipsec)# authentication local rsa-sig
server-ca "OU=NewCA, c=US"
CES(config-group/ipsec)# no authentication local
username-password
CES(config-group/ipsec)# authentication external
username-password
CES(config-group/ipsec)# no authentication local rsa-sig
server-ca
CES(config-group/ipsec)# exit
CES(config-group)#
```

authentication (L2TP, PPTP, L2F)

This command specifies authentication methods for L2TP, PPTP and L2F. This command is specific to the VPN Router; specify only -CHAP authentication only for PPTP and L2TP tunnels.

Syntax

```
authentication {pap | chap | ms-chap {encryption [none |
rc4-128 | rc4-40 | version [1 | 2]}}
no authentication {pap | chap | ms-chap {encryption [none |
rc4-128 | rc4-40 | version [1 | 2]}}
```

Parameters

version	Version keyword.
1	Version 1 of MS-CHAP.
2	Version 2 of MS-CHAP.
encryption	Encryption keyword.
none	Tunnels requesting no data encryption.
rc4-40	Tunnels requesting 40-bit RC4 encryption are accepted.
rc4-128	Tunnels requesting 128-bit RC4 encryption are accepted.
pap	Password Authentication Protocol.
chap	Challenge Handshake Authentication Protocol.
ms-chap	MS Challenge Handshake Authentication Protocol (for PPTP and L2TP).

Default

Enabled all

Command mode

Group L2F Configuration
Group L2TP Configuration
Group PPTP Configuration

Next command mode

Group L2F Configuration
Group L2TP Configuration
Group PPTP Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config)# group l2tp /Base
CES(config-group/l2tp)# authentication ms-chap version 1
CES(config-group/l2tp)# exit
CES(config)# group l2f /Base
CES(config-group/l2f)# no authentication chap
CES(config-group/l2f)# no authentication pap
CES(config-group/l2f)# exit
CES(config)#
```

banner

This command specifies the login banner for the Nortel VPN Router Client. This banner appears at the IPsec client upon login. This command is only supported by the Nortel VPN Router Client.

Syntax

banner <*line*>
no banner

Parameters

line	Text of the banner in quotes and must be a single line of text.

Default

None

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related Commands

display-banner
ipsec-transport

Example

```
CES(config-group/ipsec)# banner "New banner"
```

bo-group

This command allows you to create a new branch office group or configure the properties of an existing group. It puts the CLI into one of the group configuration modes (connectivity, IPsec, RIP, or OSPF) to allow you to configure those settings for an existing group.

Syntax

bo-group [**add** | **connectivity** | **ipsec** | **rip** | **ospf**] <*group_name*>

Parameters

add	The bo-group should be created.
connectivity	Connectivity properties for the group.
ipsec	IPsec properties for the group.
rip	RIP properties for the group.
ospf	OSPF properties for the group.
group_name	The name of the group to be created or configured. The name must be in double quotes. The name is case sensitive for a new group, but the VPN Router will perform a case-insensitive match with existing group names for uniqueness.

Command mode

Global Configuration

Next command mode

Global Configuration or Branch Office Group Configuration

Required privileges

System Management – Manage
User Management – Manage for the parent of this group

Prerequisites

The parent group must already exist. The group name is validated to make sure that is does not contain a / character. Use quotation marks around a group name if it contains spaces.

Warning messages

```
% Group xxxx already exists.
% Parent group xxxx does not exist.
```

Related commands

no bo-group
show bo-group

Example

```
CES(config)# bo-group add "/Base/test1"
%Group /Base/test1 already exists
CES(config)# bo-group connectivity “/Base test1”
CES(config-bo_group/con#
```

client

This command configures a tunnel filter to enable traffic to external servers that are used by the VPN Router (the VPN Router acts as a client). Use the **no** form of the command to disable traffic to the specified server types.

Syntax

client {**all** | **cmp** | **dns** | **ftp** | **ldap** | **ntp** | **radius** | **tunnelguard**}

no client {**all** | **cmp** | **dns** | **ftp** | **ldap** | **ntp** | **radius** | **tunnelguard**}

Parameters

all	Configure the tunnel filter to enable or disable CMP, DNS, FTP, LDAP Proxy, NTP, and RADIUS traffic.
cmp	Configure the tunnel filter to enable or disable CMP traffic.
dns	Configure the tunnel filter to enable or disable DNS traffic.
ftp	Configure the tunnel filter to enable or disable FTP traffic.
ldap	Configure the tunnel filter to enable or disable LDAP authentication traffic.
ntp	Configure the tunnel filter to enable or disable NTP traffic.

radius	Configure the tunnel filter to enable or disable RADIUS traffic.
tunnelguard	Configure the tunnel filter to enable or disable Tunnel Guard traffic.

Default

All client traffic is disabled in a new tunnel filter set.

Command mode

Tunnel Filter Configuration

Next command mode

Tunnel Filter Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

server

Example

The following example enables DNS and FTP client traffic in the tunnel filter set "Local Clients."

```
CES(config)# filter tunnel "Local Clients"
CES(config-filter)# client dns
CES(config-filter)# client ftp
CES(config-filter)# exit
CES(config)#
```

client-address

This command enables or disables the use of the client-specified address for the L2F, L2TP, PPTP tunnels. This command is common for the L2F, L2TP, and PPTP configuration modes.

Syntax

```
client-address
no client-address
```

Parameters

None

Default

Disabled

Command mode

Group Configuration

Next command mode

Group Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config-group/L2F)# client-address
CES(config-group/L2TP)# no client-address
```

client auto-connect

This command enables or disables client auto-connect for IPsec tunnel. This command is only supported by the Nortel VPN Router Client.

Syntax

```
client auto-connect
no client auto-connect
```

Parameters

None

Default

None

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only supported by the Nortel VPN Router Client.

Related commands

```
client auto-connect networks
client failover-tuning
client nat interval
client policy
client screen-saver
client undefined-networks
```

Example

```
CES(config-group/ipsec)# client auto-connect
```

client auto-connect networks

This command specifies the client auto-connect networks for IPsec tunnel. This command is only supported by the Nortel VPN Router Client.

Syntax

```
client auto-connect networks {any | domains <domains> |
network [domains <domains>]}
no client auto-connect networks
no client auto-connect domains
```

Parameters

any	Any network traffic.
networks	Keyword specifying that configured network routes that you can select will follow.
networks	Currently configured network routes that you can select.
domains	Keyword specifying that domains or hostnames will trigger the autoconnect feature will follow.
domains	Specific domains or hostnames that will trigger the autoconnect feature.

Default

Any network traffic

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Domain does not exist
% Network does not exist
```

Related commands

client auto-connect

Example

```
CES(config-group/ipsec)# client auto-connect networks any
```

client dynamic-dns enable

Use this command to enable or disable dynamic DNS registration for clients running Nortel VPN Router Client software. The DNS server must support dynamic DNS and be configured to allow dynamic DNS registration.

Syntax

```
client dynamic-dns enable
no client dynamic-dns enable
```

Parameters

None

Default

Enabled

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command affects only the Nortel VPN Router Client.

Related commands

client
ip address

Example

The following example disables dynamic DNS registration for systems running Nortel VPN Router Client software.

```
CES(config)# group ipsec /Base/test1
CES(config-group/ipsec)# no client dynamic-dns enable
CES(config-group/ipsec)#
```

The following example enables dynamic DNS registration for systems running Nortel VPN Router Client software.

```
CES(config)# group ipsec /Base/test1
CES(config-group/ipsec)# client dynamic-dns enable
CES(config-group/ipsec)# exit
CES(config)#
```

client failover-tuning

This command enables or disables the client failover-tuning for IPsec tunnel.

Syntax

client failover-tuning
no client failover-tuning

Parameters

None

Default

Enable

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only supported by the Nortel VPN Router Client.

Related commands

client failover-tuning interval
client failover-tuning retransmissions

Example

```
CES(config-group/ipsec)# client failover-tuning
```

client failover-tuning interval

This command specifies the client failover-tuning interval for IPsec tunnel. This command is only supported by the Nortel VPN Router Client.

Syntax

client failover-tuning interval *<hh:mm:ss>*

Parameters

hh:mm:ss	Interval in hours, minutes, and seconds.

Default

00:01:00 minute.

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Response

None

Related commands

client failover-tuning
client failover-tuning retransmissions

Example

```
CES(config-group/ipsec)# client failover-tuning interval
10:15:00
```

client failover-tuning retransmissions

This command specifies the client failover-tuning maximum number of retransmissions for IPsec tunnel. This command is only supported by the Nortel VPN Router Client.

Syntax

client failover-tuning retransmissions <*number*>

Parameters

number	Maximum number of retransmissions. The range is 0 through 9.

Default

3

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

client failover-tuning interval
client failover-tuning

Example

```
CES(config-group/ipsec)# client failover-tuning
retransmissions 5
```

client nat interval

This command sets the NAT keep-alive interval for the UDP encapsulation.

Syntax

client nat interval <*interval*>

Parameters

interval	Keep-alive interval in hours, minutes, and seconds (the range is 0 through 65535) in seconds. Format is *hh:mm:ss*.

Default

18 seconds (00:00:18)

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – View

Prerequisites

None

Example

```
CES(config-group/ipsec)# client nat interval 0:1:15
```

client policy

This command specifies client policy for the VPN Router. Client policy helps prevent potential security violations that could occur when you are using the split tunneling feature. Use the **no** form of the command to remove client policy. This command is only supported by the Nortel VPN Router Client.

Syntax

```
client policy <policy-name>
no client policy
```

Parameters

policy-name	Client policy to use. Client policies contain information on the protocols, ports, and application types (client or server) that are permissible during tunneling.

Default

None

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only supported by the Nortel VPN Router Client.

Warning messages

```
% Policy does not exist.
```

Related commands

`client failover-tuning`

Example

```
CES(config-group/ipsec)# client policy "home users"
```

client screen-saver activation-time

This command specifies the client screen saver activation time required for IPsec tunnel. This command is only supported by the Nortel VPN Router Client.

Syntax

client screen-saver activation-time <*mm*>

Parameters

mm	Time in minutes. The range is 0 through 60. The value 0 will disable it.

Default

5 minutes

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only supported by the Nortel VPN Router Client.

Related commands

client screen-saver password

Example

```
CES(config-group/ipsec)# client screen-saver activation-time
10
```

client screen-saver password

This command enables or disables client screen saver password require for IPsec tunnel.

Syntax

```
client screen-saver password
no client screen-saver password
```

Parameters

None

Default

None

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only supported by the Nortel VPN Router Client.

Related commands

client screen-saver activation-time

Example

```
CES(config-group/ipsec)# client screen-saver password
```

committed rate

This command establishes the User Bandwidth Policy committed rate (Group Connectivity Configuration) and establishes the Branch Office Bandwidth Policy committed rate (Branch Office Group Connectivity Configuration).

Syntax

committed rate <*rate*>

Parameters

rate	Actual rate in bits per second (bits/s), no more than 10 MB/s (switch unit).

Default

56000 bits/s

Command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

excess rate

Example

The following example sets a committed bandwidth of 14.4. Kbps.

```
CES(config-group/con)# committed rate 14400
```

compress

This command enables or disables IPsec Hi/fn LZS compression or PPTP, L2TP, or L2F Microsoft* Point-to-Point Compression (MPPC) packet compression. This command is the same for the Group IPsec, L2F, L2TP, and PPTP configuration modes, and for the Branch Office Group IPsec configuration modes.

Syntax

```
compress
no compress
default compress
```

Parameters

None

Default

Disabled

Command mode

Group [IPsec | L2F | L2TP | PPTP] Configuration
Branch Office Group IPsec Configuration
Branch Office Connection PPTP or L2TP Configuration

Next command mode

Group [IPsec | L2F | L2TP | PPTP] Configuration
Branch Office Group IPsec Configuration
Branch Office Connection PPTP or L2TP Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config-group/ipsec)# compress
CES(config-bo_group/ipsec)# default compress
CES(config/bo-conn/pptp)# compress
CES(config/bo-conn/l2tp)# no compress
```

connection

This command sets the TCP connection for the current filter rule. This command is used when defining filter rules.

Syntax

connection {**established** | **none**}

Parameters

established	Set the TCP connection for the current filter rule to established.
none	Set the TCP connection for the current filter rule to none (do not care).

Default

For a new filter rule, the default TCP connection is none.

Command mode

Rule Configuration

Next command mode

Rule Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

address
port
direction
filter add
protocol
rule add
use
action

Example

The following example modifies the existing tunnel “Deny FTP” filter rule to establish a TCP connection.

```
CES(config)# filter tunnel rule "Deny FTP"
CES(config/rule)# connection established
CES(config/rule)# exit
```

contact

This command creates contact information.

Syntax

contact “<*information*>”
no contact

Parameters

information	The contact information, in quotes.

Default

None

Command mode

Connectivity Configuration

Next command mode

Connectivity Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only available in Connectivity Configuration mode.

Related commands

access-hours

Example

```
CES(config-group/conn)# contact "VPN Admin"
```

dead-interval

This command specifies how long hello packets must not have been seen before its neighbors declare the VPN Router down. To return to the default time, use the **no** form of the command. It is required that the dead-interval be set to 4 times the hello-interval.

Syntax

```
dead-interval <length>
no dead-interval
```

Parameters

length	The integer that specifies the interval in seconds. The range is 1 through 1000.

Default

40 seconds.

Command mode

Branch Office Group OSPF Configuration

Next command mode

Branch Office Group OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Dead Interval value must be at least 4 times
hello-interval.
```

Related commands

hello-interval
retransmit-interval

Example

```
CES(config-bo_group/ospf)# dead-interval 50
CES(config-bo_group/ospf)# no dead-interval
```

default

This command specifies that a value for a specified property or for all properties be inherited from the parent group.

Syntax

default {**all** | <*property*>}

Parameters

all	Inherit all configuration properties from the parent group.
property	Inherit the specified configuration property (for example, IPX or contact) from the parent group.

Default

None

Command mode

Group [Connectivity | IPsec | L2F | PPTP | L2TP] Configuration
Branch Office Group [Connectivity | IPsec | OSPF | RIP] Configuration

Next command mode

Group [Connectivity | IPsec | L2F | PPTP | L2TP] Configuration
Branch Office Group [Connectivity | IPsec | OSPF | RIP] Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is available only in group configuration mode.

Warning messages

```
% Cannot inherit from the group.
```

Related commands

no
add

Example

```
CES(config-group/connectivity)# default all
CES(config-group/connectivity)# exit

CES(config-group/ipsec)# default banner
CES(config-group/ipsec)# exit
```

df-bit

Use this command to set the don't fragment (DF) bit in the outer IP header of an IPsec-encapsulated packet. Depending on the setting of the DF bit in the IP header, packets larger than the MTU configured for the tunnel are either fragmented or dropped.

By default, the VPN Router clears the DF bit in the outer IP header to allow fragmenting (and sending) of packets that are larger than the MTU. You can configure the VPN Router to set the DF bit in the outer IP header or to copy the value for the DF bit that is specified in the inner IP header.



Note: The DF bit setting specified in this configuration mode overrides any other DF bit settings configured in other modes.

Syntax

```
df-bit {clear | copy | set}
```

Parameters

clear	Specifies that the outer IP header will have the DF bit cleared and that the VPN Router may fragment the packet to add the IPsec encapsulation.
copy	Specifies that the VPN Router will copy the DF bit setting in the original packet to the outer IP header.
set	Specifies that the outer IP header will have the DF bit set; however, the VPN Router may fragment the packet if the original packet had the DF bit cleared.

Default

clear

Command mode

Branch Office Group IPsec Configuration

Next command mode

Branch Office Group IPsec Configuration

Required privileges

System Management – None
User Management – Manage

Related commands

None

Example

The following example sets the DF bit on all packets that traverse IPsec tunnels created for the group /Base/test.

```
CES(config)# bo-group ipsec /Base/test
CES(config-bo_group/ipsec)# df-bit set
CES(config-bo_group/ipsec)#
```

The following example copies the DF bit from the inner IP header to the outer header on all packets that traverse IPsec tunnels created for the group /Base/test.

```
CES(config)# bo-group ipsec /Base/test
CES(config-bo_group/ipsec)# df-bit copy
CES(config-bo_group/ipsec)#
```

The following example clears the DF bit from the outer IP header of all packets that traverse IPsec tunnels created for the group /Base/test.

```
CES(config)# bo-group ipsec /Base/test
CES(config-bo_group/ipsec)# df-bit clear
```

direction

This command sets the direction for the current filter rule to the named direction.

Syntax

```
direction {inbound | outbound}
```

Parameters

inbound	Sets the filter rule to inbound.
outbound	Sets the filter rule to outbound.

Default

For a new filter rule, the default direction is inbound.

Command mode

Rule Configuration

Next command mode

Rule Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

action
protocol
use address
use dest-port
use src-port

Example

```
CES(config)# filter tunnel rule “permit ftp/in”
CES(config-rule)# direction inbound
```

display-banner

This command enables or disables the display of the banner when a remote user logs in to the VPN Router. This command is only supported by the Nortel VPN Router Client.

Syntax

display-banner
no display-banner

Parameters

None

Default

Disabled

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

banner

Example

```
CES(config-group/ipsec)# display-banner
```

dynamic-authenticate

Use this command to enable Dynamic password authentication via RADIUS and LDAP Proxy-based authentication systems. Use the no form of this command to use static password authentication.

Syntax

```
dynamic-authenticate
no dynamic-authenticate
```

Parameters

None

Default

Enabled

Command mode

CES

Next command mode

CES

Required privileges

System Management – Manage
User Management – Manage

Prerequisites

None

Related commands

Example

The following example disables dynamic password authentication for systems running Nortel VPN Router Client software.

```
CES(config)#user "test admin" /Base/test
CES(config-user)#administration ?
User administration configuration
  no dynamic-authenticate
```

The following example enables dynamic password authentication for systems running Nortel VPN Router Client software.

```
CES(config)#user "test admin" /Base/test
CES(config-user)#administration ?
User administration configuration
  dynamic-authenticate  Set administrator to authenticate
                        dynamically
CES(config-user)#administration dy
CES(config-user)#administration dynamic-authenticate ?
  <cr>

CES(config-user)#administration dynamic-authenticate
CES(config-user)#
CES(config)#
```

encryption

This command enables encryption algorithms for IPsec tunneling. Use the **no** form of the command to disable an algorithm. If you do not specify any arguments on the command line, all encryption algorithms are enabled or disabled. You can enter this command in both Group IPsec Configuration mode and Branch Office Group IPsec Configuration mode.

Syntax

encryption {**3des-md5** | **3des-sha1** | **aes128-sha1** | **aes256-sha1** | **des40-md5** | **des40-sha1** | **des56-md5** | **des56-sha1** | **hmac-md5** | **hmac-sha1** | **md5** | **sha1**}

no encryption {**3des-md5** | **3des-sha1** | **aes128-sha1** | **aes256-sha1** | **des40-md5** | **des40-sha1** | **des56-md5** | **des56-sha1** | **hmac-md5** | **hmac-sha1** | **md5** | **sha1**}

default encryption

Parameters

3des-md5	Triple DES with MD5 integrity.
3des-sha1	Triple DES with SHA1 integrity.
aes128-sha1	128-bit AES with SHA1 integrity.
aes256-sha1	256-bit AES with SHA1 integrity.
des40-md5	40-bit DES with MD5 integrity.
des40-sha1	40-bit DES with SHA1 integrity.
des56-md5	56-bit DES with MD5 integrity.
des56-sha1	56-bit DES with SHA1 integrity.
hmac-md5	Hashing Message Authentication Code Message Digest 5.
hmac-sha1	Hashing Message Authentication Code Secure Hash Algorithm.
md5	Authentication only with MD5 integrity.
sha1	Authentication only with SHA1 integrity.

Default

Encryption defaults to parent or to box-wide settings (see IPsec command).

Command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Next command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is available only in group or branch office group IPsec configuration mode.

Related commands

encryption ike

Example

The following example enables encryption with 56-bit DES with MD5 integrity for the /Base group and for the /Base/test branch office group.

```
CES(config)# group ipsec /Base
CES(config-group/ipsec)# encryption des56-md5
CES(config-group/ipsec)# exit
CES(config)# bo-group ipsec “/Base/test”
CES(config-bo_group/ipsec)# encryption des56-md5
CES(config-bo_group/ipsec)# exit
CES(config)#
```

The following example configures the group /Base/test to inherit all its encryption algorithms from the parent group (/Base).

```
CES(config)# bo-group ipsec “/Base/test”
CES(config-bo_group/ipsec)# default encryption
CES(config-bo_group/ipsec)# exit
```

encryption ike

This command specifies IKE encryption and Diffie-Hellman group for IPsec tunneling. Use the **no** form of the command to disable an algorithm-Diffie-Hellman group combination. You can enter this command in both Group IPsec Configuration mode and Branch Office Group IPsec Configuration mode. One or more settings can be active for group mode; only one setting is active for branch office group mode.

Syntax

Group IPsec Configuration mode:

```
encryption ike {128aes-group2 | 128aes-group5 |
128aes-group8 | 256aes-group5 | 256aes-group8 | 3des-group2
| 3des-group7 | des56-group1}

no encryption ike {128aes-group2 | 128aes-group5 |
128aes-group8 | 256aes-group5 | 256aes-group8 | 3des-group2
| 3des-group7 | des56-group1}
```

Branch Office Group IPsec Configuration mode:

```
encryption ike {128aes-group2 | 128aes-group5 |
128aes-group8 | 3des-group2 | 3des-group7 | des56-group1}

default encryption ike
```

Parameters

128aes-group2	128-bit AES with SHA1 under Group 2 (1024-bit prime).
128aes-group5	128-bit AES with Group 5 (1536-bit prime).
128aes-group8	128-bit AES with Group 8 (ECC 283-bit field).
256aes-group5	256-bit AES with Group 5 (1536-bit prime).
256aes-group8	256-bit AES with Group 8 (ECC 283-bit field).
3des-group2	Triple DES with Group 2 (1024-bit prime).
3des-group7	Triple DES with Group 7 (ECC 163-bit field).
des56-group1	56-bit DES with Group 1 (768-bit prime).

Default

IKE settings default to parent or box-wide settings.

Command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Next command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is available only in IPsec configuration mode.

Related commands

encryption

Example

The following example enables 56-bit DES with Group 1 encryption for the group /Base and enables triple DES with Group 7 encryption for the branch office group /Base/test.

```
CES(config)# group ipsec /Base
CES(config-group/ipsec)# encryption ike des56-group1
CES(config-group/ipsec)# exit
CES(config)# bo-group ipsec /Base/test
CES(config-bo_group/ipsec)# encryption ike 3des-group7
CES(config-bo_group)# exit
CES(config)#
```

The following example enables the branch office group /Base/test to inherit its encryption algorithm settings from its parent group.

```
CES(config)# bo-group ipsec /Base/test
CES(config-bo_group/ipsec)# default encryption
CES(config-bo_group/ipsec)# exit
CES(config)#
```

excess action

This command establishes the User Bandwidth Policy excess action (Group Connectivity Configuration).

This command establishes the Branch Office Bandwidth Policy excess action for the group (Branch Office Group Connectivity Configuration).

Syntax

```
excess action {mark | drop}
```

Parameters

mark	Excess traffic is marked.
drop	Excess traffic is dropped.

Default

mark

Command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

committed rate

Example

```
CES(config-group/con)# excess action drop

CES(config-bo_group/con)# excess action mark
```

excess rate

This command establishes the User Bandwidth Policy excess rate for the group (Group Connectivity Configuration) and the Branch Office Bandwidth Policy excess rate for the group (Branch Office Group Connectivity Configuration).

Syntax

excess rate <*rate*>

Parameters

rate	Actual rate in bits/s up to 10,000,000 (10 Mb/s).

Default

128000 bps

Command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Rate does not exist.
% Excess rate must be greater than or equal to committed
rate.
```

Related commands

committed rate

Example

```
CES(config-group/con)# excess rate 512000
CES(config-bo_group/con)# excess rate 512000
```

exit

This command exits from the current mode. All changes are applied to the underlying database and the CLI returns to the previous mode. Error messages arising from data validation will be displayed as appropriate.

Syntax

exit

Command mode

Group Configuration
Group Connectivity Configuration
Group IPsec Configuration
Group PPTP Configuration
Group L2F Configuration
Group L2TP Configuration
Filter configuration
User configuration
BO configuration

Next command mode

As appropriate

Example

```
CES(config-group)# exit
```

export bo-static-metric

This command specifies the default metric values for RIP configuration.

Syntax

```
export bo-static-metric <value>
no export bo-static-route-metric
```

Parameters

value	The integer that specifies the static routes metric (the range is 1 through 15).

Default

Disable

Command mode

Branch Office Group RIP Configuration

Next command mode

Branch Office Group RIP Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

```
export static-metric
export default-metric
export ospf-metric
```

Example

```
CES(config-bo_group/rip)# export bo-static-metric 7
```

export default-metric

This command specifies the default metric value for RIP configuration.

Syntax

export default-metric <*value*>
no export default-routes-metric

Parameters

value	The integer that specifies the static routes metric (the range is 1 through 15).

Default

Disable

Command mode

Branch Office Group RIP Configuration

Next command mode

Branch Office Group RIP Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

export static-metric
export ospf-metric
export bo-static-metric

Example

```
CES(config-bo_group/rip)# export default-metric 7
```

export ospf-metric

This command specifies the OSPF route metric value for RIP configuration.

Syntax

export ospf-metric <*value*>
no export ospf-routes-metric

Parameters

value	The integer that specifies the static routes metric (the range is 1 through 15).

Default

Disable

Command mode

Branch Office Group RIP Configuration

Next command mode

Branch Office Group RIP Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

export bo-static-metric
export default-metric
export static-metric

Example

```
CES(config-bo_group/rip)# export ospf-metric 7
```

export static-metric

This command specifies the static route metric value for RIP configuration.

Syntax

export static-metric <*value*>
no export static-routes-metric

Parameters

value	The integer that specifies the static routes metric (the range is 1 through 15).

Default

Disable

Command mode

Branch Office Group RIP Configuration

Next command mode

Branch Office Group RIP Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

export bo-static-metric
export default-metric
export ospf-metric

Example

```
CES(config-bo_group/rip)# export static-metric 7
```

filters (Group Connectivity Configuration)

This command specifies the filters set to use for the group.

Syntax

filters <*description*>

Parameters

description	The name of the filter set that the group should use.

Default

The “permit all” filter set.

Command mode

Connectivity Configuration

Next command mode

Connectivity Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only available in Connectivity Configuration mode.

Warning messages

```
% Filter does not exist.
```

Related commands

show filters tunnel

Example

```
CES(config-group/conn)# filters "permit all"
CES(config-group/conn)# exit
```

filter add

This command places the user into filter configuration mode for the given *rulename* or *filtername*. The changes to the configuration of the filter set or rule do not apply until the user enters the **exit** command to leave configuration mode. At that stage all changes apply as updates to the named rule or filter set.

If the optional **add** parameter is specified, the command creates the named rule or filter set and stays in Global Configuration mode. A filter set that is created in this way will have no filter rules and allow no server traffic. This effectively makes it a deny-all filter set. A rule created this way will effectively be a deny all inbound TCP rule.

There are two types of rules and filters, interface and tunnel.

- Interface filters and rules are applied to specific IP interfaces on the VPN Router.
- Tunnel filters and rules are applied to groups and ensure that all users who are members of a given group use a set of filters that determines the type of traffic through the VPN Router for that user.

Note that the same *rulename* or *filtername* can exist as an interface filter and as a tunnel filter with different definitions.

Syntax

```
filter {interface | tunnel} {[add] <filtername> | rule [add]
<rulename>}
no filter {interface | tunnel} {rule <rulename> |
<filtername>}
```

Parameters

interface	Specifies that this is an interface filter or rule that must be applied to the IP interfaces defined on the VPN Router.
tunnel	Specifies that this is a tunnel filter or rule that must be applied to the groups defined on the VPN Router.
add	Optional parameter specifying that the rule or filter set should be created. If omitted, the rule or filter set should already exist and it will be modified.
filtername	The name of the filter to create or modify.
no	This is the command used to delete an existing rule or filter set. The filter set cannot be deleted if it is in use by a group or an IP interface.
rule	Specifies the command will edit or create a rule instead of a filter.
rulename	The name of the rule to create or modify. This must be enclosed in quotes if the name contains spaces. The name cannot contain more than 64 characters.

Command mode

Global Configuration

Next command mode

Filter Configuration or
Global Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Filter xxx does not exist.
% Filter xxx already exists.
% Filter xxx is in use.
% No entries found
% Rule xxx already exists
```

Related commands

None

Example

```
CES(config)# filter tunnel add DenyFtp
CES(config)# filter tunnel DenyFtp
CES(config-filter)# exit
CES(config)# filter interface rule add “Permit Some”
```

filter rule add

This command creates a new filter rule or enters into rule configuration mode for the named rule. The settings for the filter rule do not apply until you leave rule configuration mode. If you specify the optional **add** parameter, the command creates the named rule. (A second command without the **add** parameter is needed to configure the rule.) Otherwise, the command enters rule configuration mode, where subsequent commands will modify the configuration of the named filter rule.

There are two types of filter rules, interface and tunnel.

- Interface filters are applied to specific IP interfaces on the VPN Router.
- Tunnel filters are applied to groups and ensure that all users who are members of a given group use a set of filters that determines the type of traffic through the VPN Router for that user.

Note that the same *rulename* can exist in both interface and tunnel rules with different definitions.

Syntax

```
filter {interface | tunnel} rule [add] <rulename>
no filter {interface | tunnel} rule <rulename>
```

Parameters

add	Optional parameter specifying that the rule should be created.
rulename	The name of the rule to either create or modify. This must be enclosed in quotes if the name contains spaces. The name cannot contain more than 64 characters.

Command mode

Filter Configuration

Next command mode

Filter Configuration or Rule Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Rule xxx already exists.
% Rule xxx does not exist.
```

Related commands

filter

Example

```
CES(config)# rule "Deny FTP"
CES(config-rule)# protocol ip
CES(config-rule)# exit
```

forced-logoff

Use this command to force a group of user tunnels or branch office tunnels to log off at a specified time.

Syntax

forced-logoff *<hh:mm:ss>*

Parameters

hh:mm:ss	Specifies the time that the logoff will occur. Type the time in hours, minutes, and seconds, for example, 05:30:00 for 5:30 AM and 17:30:00 for 5:30 PM. You can enter time values from 00:00:01 through 119:59:59.

Default

00:00:00 (forced logoff is disabled)

Command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage
User Management – None

Example

The following example logs off users in the testgroup “group” at 10:45 a.m.

```
CES(config)# group connectivity “/Base/testgroup”
CES(config-group/con)# forced-logoff 10:45:00
CES(config-group/con)#
```

The following example logs off users in the branch office group “pubsgroup” at 10:45 PM.

```
CES(config)# bo-group connectivity “/Base/pubsgroup”
CES(config-bo_group/con)# forced-logoff 22:45:00
CES(config-bo_group/con)#
```

group (Global Configuration Command)

This command creates a new user group or configures the properties of the existing group. It puts the CLI into one of the group configuration modes (connectivity, IPsec, RIP, or OSPF) to allow you to configure the settings for an existing group. To create a new group, use the `group add` form of the command. The groups on a VPN Router from a hierarchy with /Base as the root of the hierarchy for the internal LDAP server. The root of the hierarchy for an external LDAP server is defined in the properties of the external server.

Syntax

Global Configuration mode:

group {**add** | **connectivity** | **ipsec** | **l2f** | **l2tp** | **pptp**} <*group_name*>

Parameters

add	The branch office group should be created.
connectivity	Enters mode where connectivity properties can be modified.
ipsec	Enters mode where IPsec properties can be modified for the group.
l2f	Enters mode where L2F properties can be modified for the group.
l2tp	Enters mode where L2TP properties can be modified for the group.
pptp	Enters mode where PPTP properties can be modified for the group.
group_name	The name of the group to be created or modified. If this name does not start with /, then the *parent_group* parameter must be present. The name must be in double quotes if it contains spaces. The name is case sensitive.

Command mode

Global Configuration

Next command mode

Group Configuration or Global Configuration

Required privileges

System Management – Manage
User Management – Manage for the parent of this group

Prerequisites

The parent group must already exist. The group name is validated to make sure that is does not contain a / character.

Warning messages

```
% Entry already exists.
% Group xxxx does not exist.
```

Related commands

no group
show groups

Example

```
CES(config-group)# add "/Base/TestGroup"
CES(config-group)# group add "/Base/TestGroup/test1"
```

group

This command is used to specify the group that a user account should belong to.

Syntax

group *<group_name>*

Parameters

group_name	The name of the group that will contain this definition. The name can contain spaces, in which case it must be enclosed in double quotes.

Default

None

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

User Configuration mode:

System Management – Any
User Management – Manage

Warning messages

User Configuration mode:

```
% Group xxx does not exist.
% LDAP: Already exists
```

For the second warning, the user name already exists in the group specified.

Related commands

user add

Example

This example changes the group to which user Paris belongs.

```
CES(config)# user "Paris" group /Base/country
CES(config-user)# group /Base
CES(config-user)# exit
```

hello-interval

This command specifies the interval between hello packets for OSPF configuration. To return to the default time, use the **no** form of the command.

Syntax

hello-interval <*length*>
no hello-interval

Parameters

length	The integer that specifies the interval in seconds (1-1000).

Default

10

Command mode

Branch Office Group OSPF Configuration

Next command mode

Branch Office Group OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

None

Related commands

dead-interval
retransmit-interval

Example

```
CES(config-bo_group/ospf)# hello-interval 5
CES(config-bo_group/ospf)# no hello-interval
```

idle-timeout

This command specifies the amount of time for which a connection must be idle before timing out.

Syntax

idle-timeout <*time*>
default idle-timeout

Parameters

time	The idle time in the format *hh:mm:ss.*

Default

00:15:00 (fifteen minutes)

Command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage None
User Management – None

Related commands

access-hours
forced logoff

Example

```
CES(config-group/con)# idle-timeout 00:15:30
CES(config-bo_group/con)# idle-timeout 01:15:30
```

import default-route

This command enables or disables the import default route.

Syntax

import default-route
no import default-route

Parameters

None

Default

None

Command mode

Branch Office Group RIP Configuration

Next command mode

Branch Office Group RIP Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config-bo_group/rip)# import default-route
CES(config-bo_group/rip)# no import default-route
```

initial-contact enable

This command causes existing connections to be torn down if an incoming connection has the same user ID. If you enable this option, you configure the VPN Router to accept ISAKMP initial contact payloads on aggressive mode client connections. In Branch Office Group IPsec Configuration mode, this option applies only to ABOT responder tunnels. Use the **no** form of the command to disable this option.

Syntax

```
initial-contact enable
no initial-contact enable
```

Parameters

None

Default

Disabled

Command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Next command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

encryption

Example

The following example configures the VPN Router to accept ISAKMP initial contact payloads for the user group /Base.

```
CES(config)# group ipsec /Base
CES(config-group/ipsec)# initial-contact enable
CES(config-group/ipsec)#
```

The following example configures the VPN Router not to accept ISAKMP initial contact payloads for the branch office group /Base/test.

```
CES(config)# bo-group ipsec /Base/test
CES(config-bo_group/ipsec)# no initial-contact enable
CES(config-bo_group)#
```

ip address

This command sets a primary or secondary IP address for the DNS that is located on your private network. This DNS address ID is provided by the server to tunnel clients at setup and is used through the tunnel. This command is supported by the Nortel VPN Router Client in Configuration Connectivity mode. This command is also available in the IPsec, L2F, L2TP, and PPTP Configuration modes.

Syntax

ip address <*ip_address*> [<*secondary*>]
default ip address

Parameters

ip_address	IP address for the DNS.
secondary	Specifies that the configured address is a secondary IP address.

Default

No DNS IP addresses defined for the VPN Router.

Command mode

Group IPsec | L2F | L2TP | PPTP Configuration

Next command mode

Group IPsec | L2F | L2TP | PPTP Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

wins address
ip domain-name

Example

```
CES(config-group/ipsec)# ip address 123.45.5.44

CES(config-group/l2tp)# ip address 123.45.5.44

CES(config-group/pptp)# ip address 123.45.5.44

CES(config-group/l2f)# ip address 0.0.0.0

CES(config-group/ipsec)# ip address 123.45.5.44 secondary
```

ip address-pool

This command enables an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or point-to-point interfaces. The address-pool will be used by remote users to access this VPN Router.

Syntax

ip address-pool *<pool>*
default ip address-pool
no ip address-pool

Parameters

pool	Name of the address pool.

Default

Default pool

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management – Manage None
User Management – None

Warning messages

```
% IP address pool does not exist.
```

Example

```
CES(config-group/con)# ip address-pool "pool_name"
```

ip address-src

This command specifies the type of source from which to obtain an IP address.

Syntax

ip address-src {**address-pool** |**internal-dhcp** |**external-dhcp**}

Parameters

None

Default

address-pool

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management – Manage None
User Management – None

Warning messages

```
% Internal DHCP Server is not enabled.
```

Example

```
CES(config-group/con)# ip address-src external-dhcp
```

ip domain-name

This command specifies the domain name that will be used while the IPsec tunnel is connected. This command is supported by the Nortel VPN Router Client in Group IPsec Configuration mode.

Syntax

```
ip domain-name <string>
default ip domain-name
no ip domain-name
```

Parameters

string	Domain name. If domain name contains spaces, enclose it in quotation marks.

Default

None

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ip address

Example

```
CES(config-group/ipsec)# ip domain-name “West Coast”
```

ipsec issuer-ca

This command sets the valid issuer certificate authority for IPsec certificates authentication.

Syntax

ipsec issuer-ca cert

Parameters

cert	Valid issuer certificate authority.

Default

None

Command mode

Branch Office Connection IPsec Certificate Configuration

Next command mode

Branch Office Connection IPsec Certificate Configuration

Required privileges

System Management – Manage
User Management – Manage (user configuration), None (Branch office mode)

Related commands

ipsec server-ca (**BO Configuration**)

Example

```
CES(config/bo-conn/ipsec)# ipsec issuer-ca “cn=testbeta,
o=mycompany”
```

ipsec server-ca (User Configuration)

This command sets the local identity server certificate. Use it when you edit user definitions to specify the certificate used when validating a user connecting with a IPsec tunnel.

Syntax

ipsec server-ca <*server_cert*>
no ipsec server-ca
default ipsec server-ca

Parameters

server_cert	The name of the server-certificate to use.
no	If present, then a server certificate is not used.
default	If present, then the server certificate value is inherited from the group to which the user belongs.

Default

The server-certificate setting is inherited from the group within which the user is contained.

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – Manage
User Management – Manage

Prerequisites

The server certificate must already be installed on the VPN Router.

Warning messages

```
% Certificate xxxx does not exist.
```

Example

The following command instructs the Nortel VPN Router to use the group's server-certificate.

```
CES(config-user)# default ipsec server-ca
```

ipsec subject-alt-name

This command specifies a Subject Alternative name in place of a Subject DN, and specifies the format of the name.

Syntax

ipsec subject-alt-name <*name*> [**type** {<*ip_address*> | <*email*> | <*dns*>}]

Parameters

name	A character string representing the alternative name.
type	Format of the name.
ip_address	IP address (for example, 192.168.34.21).
email	Email name (for example, net_admin@company.com).
dns	DNS name (for example, VPN Router.cleveland.company.com.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ipsec subject-dn

Example

```
CES(config)# ipsec subject-alt-name Paris type dns
```

ipsec subject-dn

This command sets the subject distinguished name.

Syntax

ipsec subject-dn <*dnName*>

Parameters

dnName	The subject distinguished name.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ipsec issuer-ca
ipsec server-ca
ipsec subject-alt-name

Example

```
CES(config/bo-conn)# ipsec subject-dn “mycompany”
```

ipsec uid (User Configuration)

Use this command to specify the user ID and password to allow IPsec access privileges for this user. Note that the user ID for IPsec accounts is typically, though not required to be, a fully qualified domain name (FQDN). Use the **no** form of the command to delete the IPsec user ID.

Syntax

ipsec uid <*user_id*> **password** <*password*>
no ipsec uid [**lockout**]

Parameters

user_id	Specifies the IPsec user ID.
password	Specifies a password for the IPsec user ID. The password can have as many as 32 characters but cannot contain spaces.
lockout	Unlock the account.

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Related commands

ipsec uid pwchange enable
l2f uid
l2tp uid
pptp uid

Example

The following example specifies the user ID and password for IPsec connections by this user.

```
CES(config-user)# ipsec uid jsmith password 4DfHzB
```

The following example deletes the IPsec user ID.

```
CES(config-user)# no ipsec uid
```

ipsec uid pwchange enable

Use this command to force Nortel VPN Router Client users to change their IPsec password the next time that they log in to the Nortel VPN Router server. Use the **no** form of the command to remove the requirement to change the password.



Note: This command applies only to users logging in through the Nortel Networks Nortel VPN Router Client.

Syntax

```
ipsec uid pwchange enable
no ipsec uid pwchange enable
```

Parameters

None

Default

Disabled

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Related commands

ipsec uid

Example

The following example forces the Nortel VPN Router Client user “fred” to change the IPsec password at the next login:

```
CES(config)# user fred “/Base/New York/Sales”
CES(config-user)# ipsec uid pwchange enable
CES(config-user)#
```

The following example removes the requirement that the user change the IPsec password at the next login:

```
CES(config)# user fred “/Base/New York/Sales”
CES(config-user)# no ipsec uid pwchange enable
CES(config-user)#
```

ipsec-transport

This command enables support for IPsec tunnel credentials for Nortel VPN Router clients. Use the **no** form of the command to disable this option.

Syntax

ipsec-transport
no ipsec-transport

Parameters

None

Default

None

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

banner

Example

The following example configures the VPN Router to allow IPsec tunnel credentials from Nortel VPN Router Clients for the group /Base.

```
CES(config)# group ipsec /Base
CES(config-group/ipsec)# ipsec-transport
CES(config-group/ipsec)#
```

ipx

This command enables and disables the Internetwork Packet Exchange Protocol (IPX) for the group.

Syntax

ipx
no ipx
default ipx

Parameters

None

Default

Disable

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management – Manage None
User Management – None

Example

```
CES(config-group icon)# ipx
```

isakmp-retransmission interval

This command specifies the maximum number of seconds between ISAKMP retransmission attempts for a branch office group.

Syntax

```
isakmp-retransmission interval <value>
default isakmp-retransmission interval
```

Parameters

value	Retransmission interval (0 through 10000 seconds).

Default

16

Command mode

Branch Office Group IPsec Configuration

Next command mode

Branch Office Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

isakmp-retransmission max-attempts

Example

```
CES(config-bo_group/ipsec)# isakmp-retransmission interval
16
```

isakmp-retransmission max-attempts

This command specifies the maximum number of ISAKMP retransmission attempts.

Syntax

isakmp-retransmission max-attempts <*value*>
default isakmp-retransmission max-attempts

Parameters

value	Maximum attempts (the range is 0 through 9).

Default

4

Command mode

Branch Office Group IPsec Configuration

Next command mode

Branch Office Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

isakmp-retransmission interval

Example

```
CES(config-bo_group/ipsec)# isakmp-retransmission
max-attempts 3
```

keepalive interval

This command specifies how long an IPsec connection can remain inactive before the VPN Router initiates the keepalive mechanism to determine whether the peer connection is lost.

Syntax

keepalive interval <*hh:mm:ss*>
default keepalive interval

Parameters

hh:mm:ss	Specifies the amount of time that no data passes over this connection. When this interval expires, the VPN Router attempts to verify whether the other side of the connection is still active. You can enter a value from 1 second through 60 minutes.

Default

60 seconds (00:01:00)

Command mode

Branch Office Group IPsec Configuration

Next command mode

Branch Office Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

keepalive ondemand-conn

Example

The following command resets the keepalive interval to 3 minutes (120 seconds).

```
CES(config-bo_group/ipsec)# keepalive 00:03:00
```

keepalive ondemand-conn

This command enables or disables the keepalive feature for on-demand connections. If you enable keepalive, the VPN Router attempts to verify connectivity with the remote peer after no data has been exchanged for the length of time specified with the **keepalive interval** command.

Syntax

```
keepalive ondemand-conn
no keepalive ondemand-conn
default keepalive ondemand-conn
```

Parameters

None

Default

Disabled

Command mode

Branch Office Group IPsec Configuration

Next command mode

Branch Office Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

keepalive interval

Example

```
CES(config-bo_group/ipsec)# keepalive ondemand-conn
CES(config-bo_group/ipsec)# no keepalive ondemand-conn
```

l2f uid (User Configuration)

Use this command to specify the user ID (including the domain, for example, gwbush@whitehouse.gov) and password to allow L2F (Layer 2 Forwarding) access privileges for this user if you are not externally authenticating the user. Use the **no** form of the command to delete the L2F user ID.

Syntax

l2f uid <*user_id*> **password** <*password*>
no l2f uid [**lockout**]

Parameters

user_id	Specifies the L2F user ID for this user.
password	Specifies a password for the L2F user ID. The password can have as many as 32 characters but cannot contain spaces.
lockout	Unlock the account.

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Related commands

ipsec uid
l2tp uid
pptp uid

Example

The following example adds the user ID and password for L2F connections by this user.

```
CES(config-user)# l2f uid jsmith password MTbdwcf2
```

The following example deletes the L2F user ID.

```
CES(config-user)# no l2f uid
```

l2tp uid (User Configuration)

Use this command to specify the user ID and password to allow L2TP (Layer 2 Tunneling Protocol) access privileges for this user if you are not externally authenticating the user. Use the **no** form of the command to delete the L2TP user ID.

Syntax

```
l2tp uid <user_id> password <password>
no l2tp uid [lockout]
```

Parameters

user_id	Specifies the L2TP user ID for this user.
password	Specifies a password for the L2TP user ID. The password can have as many as 32 characters but cannot contain spaces.
lockout	Unlock the account.

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Related commands

ipsec uid
l2f uid
pptp uid

Example

The following example specifies the user ID and password for L2TP connections by this user.

```
CES(config-user)# l2tp uid jsmith password G8t4fe
```

The following command deletes the L2TP user ID.

```
CES(config-user)# no l2tp uid
```

login max-attempts

Use this command to specify the maximum number of login attempts to lock out an account. After the specified number of unsuccessful login attempts, the user account will be locked. To unlock the user account, use the **no uid lockout** User Configuration command or similar commands for L2F, L2TP, and PPTP.

Syntax

login max-attempts <*value*>

Parameters

value	Maximum login attempts (0 through 255).

Default

3

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management – Manage None
User Management – None

Related commands

no uid lockout

Example

```
CES(config-group/con)# login max-attempts 7
```

logins

This command specifies the maximum number of logins that IPsec clients in the group will be allowed.

Syntax

logins <*number*>
default logins

Parameters

number	Number of logins (the range is 0 through 65535). A value of zero causes no maximum to be specified.

Default

2

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management – Manage None
User Management – None

Related commands

ppp-links max-number

Example

```
CES(config-group/con)# logins 3
```

logoff-notification-interval

Use this command to specify how long before session timeout a user is notified.

Syntax

logoff-notification-interval *<hh:mm:ss>*

Parameters

hh:mm:ss	Specifies how long before session timeout a user is notified. Type the time in hours, minutes, and seconds, for example, 05:30:00 for 5:30 AM and 17:30:00 for 5:30 PM. You can enter time values from 00:00:01 through 119:59:59.

Default

00:00:00 (logoff-notification-interval is disabled)

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage
User Management – None

Example

The following example logs off users in the group “testgroup” at 10:45 AM.

```
CES(config)# group connectivity /Base
CES(config-group/con)# logoff-notification-interval 2:00:00
CES(config-group/con)#
```

move-rule

This command changes the order of a filter rule within the current filter set. The filter rules are applied in order from top to bottom. There is an assumed “deny all” rule as the last rule in a filter set.

Syntax

move-rule <*rulename*> {**up** | **down**}

Parameters

rulename	The name of the rule to move within the current filter. This must be enclosed in quotes if the name contains spaces. The filter rule named must be present in the filter set.
up	Move the rule to a higher priority.
down	Move the rule to a lower priority.

Command mode

Filter Configuration

Next command mode

Filter Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The filter rule to be moved must be in the filter set being modified.

Warning messages

```
% Rule xxx does not exist.
% Rule cannot be given higher priority.
% Rule cannot be given lower priority.
```

Related commands

add-rule
remove-rule

Example

```
CES(config-filter)# move-rule DenyFtpRule up
```

nailed-up

This command enables or disables nailed-up tunnels for the branch office group. The default form causes the tunnel to inherit the value from the parent group.

Syntax

nailed-up
no nailed-up
default nailed-up

Parameters

None

Default

Disable

Command mode

Branch Office Group Connectivity Configuration

Next command mode

Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

None

Example

```
CES(config-bo_group/con)# nailed-up
CES(config-bo_group/con)# no nailed-up
```

nat-traversal

This command enables or disables IPsec NAT traversal. Use the **no** form of the command to disable the UDP encapsulation for the group.

Syntax

```
nat-traversal {ipsec_nat_detect | nat-detect}
no nat-traversal
```

Parameters

ipsec-nat-detect	Auto-detect IPsec capable NAT.
nat-detect	Encapsulate when NAT detected.

Default

Disable

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – View

Prerequisites

None

Example

```
CES(config-group/ipsec)# nat-traversal nat-detect
```

no bo-group

This command deletes an existing branch office group. It can also be used to delete a subtree of the group database that is rooted by the specified group. The group cannot be deleted if it is used by RADIUS to obtain default settings for RADIUS users.

Syntax

no bo-group <*group_name*> [**purge** | **recurse** [**purge**]]

Parameters

group_name	The name of the group to be deleted. The name can in double quotes. The name is case-insensitive.
recurse	All groups that are children of this group are also to be deleted. If this parameter is not present and the group to be deleted is the parent of other groups, the group deletion will fail.
purge	All branch office connections which belong to this group are to be deleted. If not present, then the group deletion will fail if this group or any subgroups have any connections. This parameter is not available if the administrator does not have User manage rights that encompass this group and all subgroups.

Command mode

Branch Office Group Configuration

Next command mode

Branch Office Group Configuration

Required privileges

System Management – Manager
User Management – Manage for this group.

Prerequisites

The Branch Office Group /Base on the internal LDAP server can never be deleted. The Branch Office Group cannot be deleted if it used by RADIUS, or if it contains any subgroups used by RADIUS.

Warning messages

```
% Branch Office Group xxx contains subgroups.
% Branch Office Group xxx contains connections.
% No such group exists.
```

Related commands

add

Example

```
CES(config-group)# no bo-group "/Base/test1"
```

no group

This command deletes an existing group. It can also be used to delete a subtree of the group database that is rooted by the specified group. The group cannot be deleted if it is used by RADIUS to obtain default settings for RADIUS users.

Syntax

```
no group <group_name> [delete-users | recurse]
[delete-users]]
```

Parameters

group_name	The name of the group to be deleted. The name is case-insensitive.
recurse	All groups that are children of this group are also to be deleted. If this parameter is not present and the group to be deleted is the parent of other groups, the group deletion will fail.
delete-users	All users which belong to this group are to be deleted. If not present then the group deletion will fail if this group or any subgroups have any users. This parameter is not available if the administrator does not have User manage rights that encompass this group.

Command mode

Group Configuration

Next command mode

Group Configuration

Required privileges

System Management – Manage
User Management – Manage for this group

Prerequisites

The group /Base on the internal LDAP server can never be deleted. The group cannot be deleted if it used by RADIUS, or if it contains any subgroups used by RADIUS.

Warning messages

```
% Group xxx does not exist.
% Group xxx contains subgroups.
% Group xxx contains users.
% Group xxx is used by RADIUS to get default settings.
```

Related commands

group
users

Example

```
CES(config-group)# no group "/Base/test1"
```

nortel-client action

This command specifies the action to take when the Nortel VPN Router Client does not meet the version requirements. See the **nortel-client version** command.

Syntax

nortel-client action [**none** | **send-message** | **send-message-filter** | **send-message-logoff**]

Parameters

none	Take action when client does not meet version requirements.
send-message	Display message to user and take no further.
send-message-filter	Display message to user and apply filter to all communication with this user.
send-message-logoff	Display message and log user off the VPN Router.

Default

None

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

None

Related commands

nortel-client message
nortel-client version
nortel-client filter

Example

```
CES(config-group/ipsec)# nortel-client action Send message
```

nortel-client filter

This command specifies the filter to be used. See the nortel-client action command for details.

Syntax

nortel-client filter <*filename*>

Parameters

filename	The name of the filter set.

Default

Permit all

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Warning messages

% Filter does not exist

Related commands

nortel-client version
nortel-client action
nortel-client message

Example

```
CES(config-group/ipsec)# nortel-client filter "Permit all"
```

nortel-client message

This command specifies the message to be sent. See the **nortel-client action** command for details.

Syntax

nortel-client message "<*string*>**"**
no nortel-client message

Parameters

string	Message string, up to 64 characters. String must be in quotation marks if it contains spaces.

Default

None

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

None

Parameters

None

Related commands

nortel-client version
nortel-client action
nortel-client filter

Example

```
CES(config-group/ipsec)# nortel-client message "Update your
client software"
```

nortel-client version

This command specifies the minimum allowable Nortel Networks Nortel VPN Router Client version.

Syntax

nortel-client version <*version_number*>

Parameters

version_number	Specifies the minimum Nortel VPN Router Client version allowed to connect to the VPN Router. Use help to determine available values.

Default

None

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

None

Related commands

nortel-client message
nortel-client action
nortel-client filter

Example

```
CES(config-group/ipsec)# nortel-client version 3.7
```

no uid lockout

Use this command to unlock the user account. After the specified number of unsuccessful login attempts user account has been locked. To change the number of login attempts, use the **login max-attempts** Group Connectivity Configuration command.

Syntax

no {**ipsec** | **l2f** | **l2tp** | **pptp**} **uid lockout**

Parameters

ipsec	Turn off lockout for IPsec tunnel.
l2f	Turn off lockout for L2F tunnel.
l2tp	Turn off lockout for L2TP tunnel.
pptp	Turn off lockout for PPTP tunnel.

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Related commands

login max-attempts

Example

The following command unlocks the IPsec user ID.

```
CES(config-user)# no ipsec uid lockout
```

password

This command, with keyword **management**, enables and disables the password management commands for the group: Maximum Password Age, Minimum Password Length and allow Alphabetic Passwords only, and enables or disables remote users to log in with alphabetic passwords only. By default, password management is disable. To be able to specify password parameters, first enable the password management.

Syntax

```
password {alphabetic | management | max-age <age> |
min-length <length>}
no password {alphabetic | management}
```

Parameters

alphabetic	Require remote users to log in with alphabetic passwords only. With **no**, users are not limited in passwords.
management	Enable password management commands. With **no**, turns off password management.
max-age	Set the maximum password age; the number of days after which the login password expires.
age	Password age; range is from 0 (no password expiration) through 180 days (about 6 months).
min-length	Set the minimum length for passwords.
length	The minimum length (a value from 3 to 16 alphanumeric characters).

Default

Password management: disable

Password max-age: 30 days

Password min-length: 16 characters

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config-group/con)# password alphabetic
CES(config-group/con)# no password alphabetic
CES(config-group/con)# password management
CES(config-group/con)# no password management
CES(config-group/con)# password min-length 8
CES(config-group/con)# password max-age 25
```

password-storage

This command enables or disables password storage on the client. This command is only supported by the Nortel VPN Router Client.

Syntax

```
password-storage
no password-storage
```

Parameters

None

Default

Disable

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only available in IPsec configuration mode.

Example

```
CES(config-group/ipsec)# password-storage
```

pfs

This command enables or disables Perfect Forward Secrecy (PFS) for the group.

Syntax

```
pfs
no pfs
default pfs
```

Parameters

None

Default

None

Command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Next command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only available in IPsec configuration mode.

Example

```
CES(config-group/ipsec)# pfs
CES(config-bo_group/ipsec)# no pfs
```

poison-reverse

This command enables or disables poison reverse for the Branch Office Group RIP.

Syntax

```
poison-reverse
no poison-reverse
```

Parameters

None

Default

Disabled

Command mode

Branch Office Group RIP Configuration

Next command mode

Branch Office Group RIP Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config-bo_group/rip)# poison-reverse
```

port

This command creates or modifies the named port definition. Port definitions are used in filter rules.

Syntax

```
port <portname> <portnumber>
no port <portname>
```

Parameters

portname	The name of the port to create or modify. This must be enclosed in quotes if the name contains spaces. The name cannot contain more than 64 characters.
portnumber	The number of the named port. The number must be in the range 0 through 65535.

Command mode

Rule Configuration

Next command mode

Rule Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Port name xxx is too long.
```

Example

```
CES(config/rule)# port "ftp" 21
```

ppp-links max-number

This command specifies the maximum number of PPP links per login for the group.

Syntax

ppp-links max-number <*number*>

Parameters

number	Number of logins (PPP links).

Default

2

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management – Manage None
User Management – None

Related commands

logins
pptp uid

Example

```
CES(config-group/con)# ppp links max-number 5
```

pptp uid (User Configuration)

Use this command to specify the user ID and password to allow PPTP (Point-to-Point Tunneling Protocol) access privileges for this user if you are not externally authenticating the user. Use the **no** form of the command to delete the PPTP user ID.

Syntax

```
pptp uid <user_id> password <password>
no pptp uid [lockout]
```

Parameters

user_id	Specifies the PPTP user ID for this user.
password	Specifies a plain-text password for the PPTP user ID. The password can have as many as 32 characters but cannot contain spaces.
lockout	Unlock the account.

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Related commands

ipsec uid
l2f uid
l2tp uid

Example

The following command adds the user ID and password for PPTP connections by this user.

```
CES(config-user)# pptp uid jsmith password hashbrowns
```

The following command deletes the PPTP user ID for this user.

```
CES(config-user)# no pptp uid
```

priority

This command specifies the router priority level, which helps to determine the designated router for this network. To return to the default value, use the **no** form of the command.

Syntax

priority *<number>*
no priority

Parameters

number	The integer that specifies the priority (0-255).

Default

1

Command mode

Branch Office Group OSPF Configuration

Next command mode

Branch Office Group OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

dead-interval
authentication
hello-interval
retransmit-interval
transmit-delay

Example

```
CES(config-bo_group/ospf)# priority 2
```

priority call-admission

This command specifies the call admission priority level for the group. This command is the same for the Group Connectivity Configuration and Branch Office Group IPsec configuration modes.

Syntax

priority call-admission {**low** | **medium** | **high** | **highest**}

Parameters

low	Low priority.
medium	Medium priority.
high	High priority.
highest	Highest priority.

Default

Highest priority

Command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage None
User Management – None

Related commands

priority forwarding

Example

```
CES(config-group/con)# priority call-admission high
CES(config-bo_group/con)# priority call-admission medium
```

priority forwarding

This command specifies the forwarding priority level to sessions for users in this group. This command is the same for the Group Connectivity Configuration and Branch Office Group IPsec configuration modes.

Syntax

```
priority forwarding {low | medium | high | highest}
```

Parameters

low	Low priority.
medium	Medium priority.
high	High priority.
highest	Highest priority.

Default

Low priority

Command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage None
User Management – None

Related commands

priority call-admission

Example

```
CES(config-group/con)# priority forwarding high
CES(config-bo_group/con)# priority forwarding highest
```

receive version

This command specifies a version for receiving RIP information. To return to the default value, use the **no** form of the command.

Syntax

```
receive version {1 | 2 | none | both}
no receive version
```

Parameters

1	Only RIP version 1 is accepted.
2	Only RIP version 2 is accepted.
none	No RIP information will be received.
both	Both RIP versions 1 and 2 are accepted.

Default

None

Command mode

Branch Office Group RIP Configuration

Next command mode

Branch Office Group RIP Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

send version

Example

```
CES(config-bo_group/rip)# receive version 1
```

rekey data-count

This command specifies the number of KB of data that you expect to transmit via the tunnel using a single encryption key. This command is the same for the Group Connectivity Configuration and the Branch Office Group IPsec Configuration modes. Setting this parameter to 0 disables the rekey data count. Use the default keyword to inherit this setting from the parent group.

Syntax

rekey data-count <*data*>
default rekey data-count

Parameters

data	Amount of data to transmit through the tunnel before a rekey occurs.

Default

0 KB

Command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Next command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

rekey timeout

Example

```
CES(config-group/ipsec)# rekey data-count 7
```

rekey timeout

This command limits the life time of a single key for encryption data. Use the default keyword to inherit this setting from the parent group.

Syntax

```
rekey timeout <time>
default rekey timeout
```

Parameters

time	Key life time, in the format *hh*:*mm*:*ss*. The maximum time is 23:59:59. A value of 00:00:00 disables the rekey time out. For best results, the rekey timeout should be set to no less than 1 hour.

Default

08:00:00 (8 hours)

Command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Next command mode

Group IPsec Configuration
Branch Office Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

rekey data-count

Example

```
CES(config-group/ipsec)# rekey timeout 05:00:00
```

remove-rule

This command removes the specified filter rule from the current filter set.

Syntax

remove-rule <*rulename*>

Parameters

rulename	The name of the rule to remove from the current filter set. This must be enclosed in quotes if the name contains spaces.

Command mode

Filter Configuration

Next command mode

Filter Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The *rulename* specified must be contained in the current filter set.

Warning messages

```
% Rule xxx does not exist in this filter set.
```

Related commands

add-rule
move-rule

Example

In this example, the filter rule DenyFtpRule is removed from the tunnel filter set named "Deny Ftp."

```
CES(config)# filter tunnel "Deny Ftp"
CES(config-filter)# remove-rule DenyFtpRule
CES(config-filter)# exit
```

retransmit-interval

This command specifies the time between link state advertisement retransmissions for adjacencies belonging to the interface. To return to the default time, use the **no** form of the command.

Syntax

retransmit-interval <*length*>
no retransmit-interval

Parameters

length	The integer that specifies the interval in seconds (1-1000).

Default

5 seconds

Command mode

Branch Office Group OSPF Configuration

Next command mode

Branch Office Group OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

hello-interval
dead-interval

Example

```
CES(config-bo_group/ospf)# retransmit-interval 50
CES(config-bo_group/ospf)# no retransmit-interval
```

rsvp

This command enables and disables RSVP for the group. Use **no** to disable and **default** to use the parent group setting.

Syntax

```
rsvp
no rsvp
default rsvp
```

Parameters

None

Default

Enable

Command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage None
User Management – None

Related commands

```
rsvp token-bucket rate
rsvp token-bucket depth
```

Example

```
CES(config-group/con)# rsvp
```

rsvp token-bucket

This command establishes RSVP token bucket depth and RSVP token bucket rate. Use **default** to use the setting of the parent group.

Syntax

```
rsvp [token-bucket {depth <depth> | rate <value>}]
default rsvp [token-bucket {depth | rate}]
```

Parameters

depth	Keyword to set depth.
depth	Token bucket depth in bytes.
rate	Keyword to set RSVP token bucket rate.
value	RSVP token bucket rate in Kbps.

Default

None

Command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Next command mode

Group Connectivity Configuration
Branch Office Group Connectivity Configuration

Required privileges

System Management – Manage None
User Management – None

Related commands

rsvp

Example

```
CES(config-group/con)# rsvp token-bucket depth 3500
CES(config-group/con)# rsvp token-bucket rate 28
```

send version

This command specifies a RIP version. To return to the default value, use the **no** form of the command.

Syntax

```
send version [1 | 2 | off]
no send version
```

Parameters

1	Version 1.
2	Version 2.
off	No version specified.

Default

None

Command mode

Branch Office Group RIP Configuration

Next command mode

Branch Office Group RIP Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

receive version

Example

```
CES(config-bo_group/rip)# send version 1
```

server

This command configures a tunnel filter to allow access to services that reside on the VPN Router (the VPN Router acts as a server). Use the **no** form of the command to disallow access to the specified service types by clients tunneling into the VPN Router.

Syntax

```
server {all | ftp | http | https | identification | ping |
radius | snmp | telnet}

no server {all | ftp | http | https | identification | ping |
radius | snmp | telnet}
```

Parameters

all	Configure the tunnel filter to enable or disable access to FTP, HTTP, HTTPS, identification, ping, RADIUS, SNMP, and Telnet services on the VPN Router.
ftp	Configure the tunnel filter to enable or disable access to FTP services on the VPN Router.
http	Configure the tunnel filter to enable or disable access to HTTP services on the VPN Router.
https	Configure the tunnel filter to enable or disable access to HTTPS services on the VPN Router.
identification	Configure the tunnel filter to enable or disable access to identification services on the VPN Router.
ping	Configure the tunnel filter to enable or disable ping access to the VPN Router.
radius	Configure the tunnel filter to enable or disable access to RADIUS services on the VPN Router.
snmp	Configure the tunnel filter to enable or disable access to SNMP services on the VPN Router.
telnet	Configure the tunnel filter to enable or disable access to Telnet services on the VPN Router.

Default

All access to VPN Router services is disabled in a new tunnel filter set.

Command mode

Tunnel Filter Configuration

Next command mode

Tunnel Filter Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

client

Example

The following example enables access to HTTP and FTP services residing on the VPN Router in the tunnel filter set “Local Servers.”

```
CES(config)# filter tunnel "Local Servers"
CES(config-filter)# server http
CES(config-filter)# server ftp
CES(config-filter)# exit
CES(config)#
```

show bo-group

This command lists the branch office groups defined on the VPN Router. It can also be used to display the configuration of individual branch office groups. This command is similar to **`show group`**.

Syntax

`show bo-group` [[**`ipsec`** | **`connectivity`** | **`ospf`** | **`rip`**] <*`group_name`*>]

Parameters

connectivity	Show branch office group connectivity settings.
ipsec	Show branch office group IPsec settings.
rip	Show branch office group RIP settings.
ospf	Show branch office group OSPF settings.
group_name	If present, then show settings for named group. The name must be enclosed in double quotes if it contains any spaces.

Command mode

Branch Office Group Configuration

Next command mode

Branch Office Group Configuration

Required privileges

System Management – View
User Management – None

Warning messages

```
% Branch Office Group xxx does not exist.
```

Related commands

bo-group add
no bo-group
show group

Example

```
CES(config-group)# show bo-group
CES(config-group)# show bo-group ipsec /Base
```

show filters

This command displays the filters defined on the VPN Router and/or their configuration.

Syntax

show filters {**tunnel** | **interface**} [<*filtername*> [**details**]]
show filters {**tunnel** | **interface**} [**rules** [<*rulename*>]]

Parameters

interface	The rules or filters to be listed apply to interfaces.
tunnel	The rules or filters to be listed apply to tunnels.
filtername	The name of the filter set. If present, displays information for that filter set. This must be enclosed in quotes if the name contains spaces.
details	Display detail information for the filter set.
rule	Display rules.
rulename	Name of the rule.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Any
User Management – View

Warning messages

```
% Filter xxx does not exist.
% No such rule exists.
```

Related commands

`filter add`

Example

```
CES(config)# show filters tunnel
Tunnel Filters:
deny all
Entrust PKI
permit all
permit only dns/ftp single server
permit only dns/ftp
permit only dns/http single server
permit only dns/http
permit only dns/netbios
permit only dns/nntp
permit only dns/smtp/pop3
permit only dns/telnet
CES(config)# show filters tunnel “deny all”
1 : deny all/in
2 : deny all/out
CES(config)# show filters tunnel “deny all” details
```

show groups

This command lists the groups defined on the VPN Router. It can also be used to display the configuration of individual groups.

Syntax

show groups [[**connectivity** | **ipsec** | **l2f** | **l2tp** | **pptp**] <*group_name*>]

Parameters

connectivity	Show group connectivity settings.
ipsec	Show group IPsec settings.
l2f	Show group L2F settings.
l2tp	Show group L2TP settings.
pptp	Show group PPTP settings.
group_name	Show settings for the named group. The name must be enclosed in double quotes if it contains any spaces.

Command mode

Group Configuration

Next command mode

Group Configuration

Required privileges

System Management – View
User Management – None

Warning messages

```
% Group xxx does not exist.
```

Related commands

group add
no group

Example

```
CES(config-group)# show groups

CES(config-group)# show groups l2tp /Base
```

show users

This command displays the users defined on the VPN Router and their configuration.

Syntax

show users {**group** | <*username*>} <*groupname*>

Parameters

username	Show information about this user.
groupname	Show information about users in this group. If no user name is specified, lists all users in this group.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Any
User Management – View

Warning messages

```
% Group xxx does not exist.
% User xxx does not exist.
```

Related commands

user
no user

Example

```
CES# show users group /Base
CES(config-group)# show users "Jane Doe" /Base
```

split inverse-tunnel-network

This command is used to specify the network to use when split tunneling is set to use inverse or inverse-local.

Syntax

split inverse-tunnel-network *<network>*
no split inverse-tunnel-network *<network>*

Parameters

network	Network to which you want to send encrypted tunnel traffic. This is a user specified command. See the network add command.

Default

None

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only available in IPsec configuration mode.

Related commands

split tunnel-networks
split inverse-tunnel-networks
split value
no split
network add

Warning messages

```
% Network does not exist.
```

Examples

```
CES(config-group/ipsec)# split inverse-tunnel-network “My
Network”
```

split tunneling

This command enables split tunneling, as well as sets the split tunnel type. Use the **no** form of this command to disable split tunneling. Split tunneling allows you to configure specific network routes that are downloaded to the client.

Syntax

```
split tunneling {enabled | inverse | inverse-local}
no split tunneling {enabled | inverse | inverse-local}
```

Parameters

None

Default

Disabled

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required Privileges

System Management – Manage
User Management – None

Prerequisites

This command is only available in IPsec configuration mode.

Related commands

```
split tunnel-networks
split inverse-tunnel-networks
split value
no split
```

Example

To enable split tunneling:

```
CES(config-group/ipsec)# split tunneling enable
```

To enable inverse split tunneling:

```
CES(config-group/ipsec)# split tunneling inverse
```

To enable inverse split tunneling for locally accessible networks:

```
CES(config-group/ipsec)# split tunneling inverse-local
```

To enable split tunneling for a group:

```
CES(config-group/ipsec)# split tunneling enable
CES(config-group/ipsec)#
```

To disable split tunneling for a group:

```
CES(config-group/ipsec)# no split tunneling enable
CES(config-group/ipsec)#
```

split tunnel-networks

This command specifies one of the networks to which you want to send encrypted tunnel traffic only.

Syntax

```
split tunnel-networks <network>
no split tunnel-networks
```

Parameters

network	Network to which you want to send encrypted tunnel traffic. This is a user-specified parameter. See the **network add** command.

Default

None

Command mode

Group IPsec Configuration

Next command mode

Group IPsec Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only available in IPsec configuration mode.

Warning messages

```
% Network does not exist.
```

Related commands

network add

Example

```
CES(config-group/ipsec)# split tunnel-networks "My network"
```

static-ipaddress (Group Connectivity Configuration)

This command enables and disables the static IP addresses for the group.

Syntax

static-ipaddress
no static-ipaddress

Parameters

None

Default

Enabled

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management – None
User Management – None

Example

```
CES(config-group/conn)# static-ipaddress
```

static-ipaddress (User Configuration)

Set the static IP address for a user. This is the IP address that will be assigned to the user's computer once the connection has been established.

If the user does not have a specified static IP address, they will be assigned an address from an IP address pool. If this command is used to specify a static IP address, then this user can only establish a single tunnel. The *ip_address* value is not checked for uniqueness. It is possible to specify the same static IP address value for more than one user definition.

Syntax

static-ipaddress <*ip_address*>

Parameters

ip_address	IP address assigned to the remote user when a tunnel connection is established.

Default

By default, a user tunneling into the VPN Router is assigned an IP address from an address pool.

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Related commands

static-subnet-mask
user add

Example

The following command sets the remote user's static IP address to 10.0.0.1:

```
CES(config-user)# static-ipaddress 10.0.0.1
```

static-subnet-mask

Set the remote user's mask associated with their static IP address for IPsec connections.

Syntax

static-subnet-mask <*mask*>

Parameters

mask	IP subnet mask.

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

The static-ipaddress must also be set.

Warning messages

```
% Non contiguous subnet mask is disallowed.
```

Related commands

`static-ipaddress`

Example

The following command sets the IP address for this user to 10.0.0.1. If the user establishes an IPsec tunnel, the subnet mask will be set to 255.255.0.0.

```
CES(config-user)# static-ipaddress 10.0.0.1
CES(config-user)# static-subnet-mask 255.255.0.0
```

transmit-delay

This command specifies the time to transmit a link state update packet on the interface. Use **no** to specify no transmit delay. To return to the default value, use the **no** form of the command.

Syntax

```
transmit-delay <length>
no transmit-delay
default transmit-delay
```

Parameters

length	The time in seconds. The range is 1 through 65532 seconds.

Default

1

Command mode

Branch Office Group OSPF Configuration

Next command mode

Branch Office Group OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

dead-interval

Example

```
CES(config-bo_group/ospf)# transmit-delay 5
```

use address

This command sets the destination address for the current filter rule to the named address. The specified address must exist before it must be used. See the `address` command.

Syntax

use address <*addressname*>

Parameters

addressname	The name of the destination address to use for the current filter rule. This must be enclosed in double quotation marks if the name contains spaces.

Command mode

Rule Configuration

Next command mode

Rule Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% No such address exists.
```

Related commands

action
address
direction
use dest-port
use protocol
use src-port

Example

```
CES(config)# filter interface rule "myrule"
CES(config-rule)# use address any
```

use dest-port

This command sets the destination port of the current filter rule to the named port. The port specified must already exist. See the **port** command.

Syntax

use dest-port {**eq** | **gt** | **gteq** | **lt** | **lteq** | **neq**} <*portname*>

Parameters

eq	Specifies that the name of the destination port for the rule is equal to the specified port name.
gt	Specifies that the name of the destination port for the rule is greater than the specified port name.
gteq	Specifies that the name of the destination port for the rule is greater than or equal to the specified port name.
lt	Specifies that the name of the destination port for the rule is less than the specified port name.
lteq	Specifies that the name of the destination port for the rule is less than or equal to the specified port name.
neq	Specifies that the name of the destination port for the rule is not equal to the specified port name.
portname	Specifies the name of the destination port to use for the current rule. If the port name contains spaces, enclose it in quotation marks.

Command mode

Rule Configuration

Next command mode

Rule Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% No such port exists.
```

Related commands

action
direction
port
use address
use protocol
use src-port

Example

```
CES(config)# filter interface rule "Deny FTP"
CES(config-rule)# use dest-port eq any
CES(config-rule)#
```

use nexthop-addr

This command allows you to configure next hop selection, source address and destination address

Syntax

use nexthop-addr

Parameters

nexthop-addr <value>	The next hop address in dotted-decimal notation.
src-addr <value>	The source address in dotted-decimal notation.
dest-addr <value>	The destination address in dotted-decimal notation.

Default

Command mode

Filter Rule Configuration

Next command mode

Filter Rule Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

Example

```
CES(config/rule)# use nexthop-addr
<value>[src-addr<value>[dest-addr<value>]]
```

use protocol

This command sets the protocol for the current filter rule. The protocol specified must already exist. See the **protocol** command.

Syntax

use protocol <*protocolname*>

Parameters

protocolname	The name of the protocol to use for the current rule. This must be enclosed in quotes if the name contains spaces.

Command mode

Rule Configuration

Next command mode

Rule Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% No such protocol exists.
```

Related commands

action
direction
protocol
use address
use dest-port
use src-port

Example

```
CES(config)# filter tunnel rule "Deny FTP"
CES(config-rule)# use protocol ip
```

use src-port

This command sets the source port for the current rule to the named port. The port specified must already exist. See the **port** command.

Syntax

use src-port {**eq** | **gt** | **gteq** | **lt** | **lteq** | **neq**} <*portname*>

Parameters

eq	Specifies that the name of the source port for the rule is equal to the specified port name.
gt	Specifies that the name of the source port for the rule is greater than the specified port name.
gteq	Specifies that the name of the source port for the rule is greater than or equal to the specified port name.
lt	Specifies that the name of the source port for the rule is less than the specified port name.
lteq	Specifies that the name of the source port for the rule is less than or equal to the specified port name.
neq	Specifies that the name of the source port for the rule is not equal to the specified port name.
portname	Specifies the name of the source port to use for the current rule. If the port name contains spaces, enclose it in quotation marks.

Command mode

Rule Configuration

Next command mode

Rule Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only available in Rule Configuration mode.

Warning messages

```
% No such port exists.
```

Related commands

action
direction
port
use protocol
use address
use dest-port

Example

```
CES(config)# filter interface rule tunnel "Deny FTP"
CES(config-rule)# use src-port eq ftp
CES(config-rule)#
```

user add

This command adds a user definition and enters user's information. The **no** form is used to delete a user definition. On the VPN Router, a user definition controls the types of tunnels (IPsec, PPTP, etc.) that a user can establish to the VPN Router, how they authenticate themselves, and properties that are established for the user session.

Syntax

```
user [add] <username> <groupname>
no user <username> <groupname>
```

Parameters

add	Optional parameter specifying that the user should be created.
username	The user account name. It can contain spaces, in which case it must be enclosed in double quotes, and must contain less than 129 characters.
groupname	The name of the user's group. In the form /base/name1/subname2. The name can contain spaces, in which case it must be enclosed in double quotes.

Default

None

Command mode

Global Configuration

Next command mode

User Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

The named group must exist.

Warning messages

```
% Group xxx does not exist.
% User xxx does not exist.
% Entry already exists.
```

Related commands

group

Example

```
CES(config)# user fred /Base/New York/Sales
CES(config-user)#
```

vendor-id

This commands enables, disables, or defaults the vendor ID.

Syntax

```
vendor-id
default vendor-id
no vendor-id
```

Parameters

None

Default

None

Command mode

Branch Office Group IPsec Configuration

Next command mode

Branch Office Group IPsec Configuration

Required privileges

Branch Office Configuration:

System Management – Manage
User Management – None

Example

```
CES(config-bo_group/ipsec)# vendor-id
```

Wins address

This command sets a primary or secondary IP address for the WINS. To remove a WINS address, specify 0.0.0.0 for the IP address.

Syntax

wins address <*ip_address*> [**secondary**]

Parameters

ip_address	IP address of the WINS server.
secondary	Specifies that the configured address is a secondary IP address. If omitted, the primary WINS IP address is set.

Default

No IP addresses defined for the VPN Router.

Command mode

Group IPsec | L2F | L2TP | PPTP Configuration

Next command mode

Group IPsec | L2F | L2TP | PPTP Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command is only available in connectivity configuration mode.

Related commands

ip address

Example

```
CES(config-group/ipsec)# wins address 123.45.5.44
CES(config-group/l2f)# wins address 123.45.5.4
CES(config-group/pptp)# wins address 123.45.5.12
CES(config-group/ipsec)# wins address 123.45.5.44 secondary
```

Chapter 7
Event log commands

This chapter describes event logging commands.

Command	Page
logging capture-filter entity add	456
logging capture-filter entity remove	458
logging capture-filter severity add	461
logging capture-filter severity remove	463
logging display-filter entity add	465
logging display-filter entity remove	467
logging display-filter severity add	470
logging display-filter severity remove	472
show logging capture-filter	474
show logging capture-filter entity all	475
show logging capture-filter entity	478
show logging capture-filter severity all	480
show logging capture-filter severity	481

logging capture-filter entity add

Use this command to add entities or sub-entities or both to capture filter.

Syntax

logging capture-filter entity add {all | *entity-name* **|** *entity-name sub-entity-name*}

Parameters

all	Add all entities and sub-entities.
entity-name	Add all sub-entities of a particular entity.
entity-name sub-entity-name	Add a sub-entity of a particular entity.

Default

All entities and sub-entities of capture filter are default to ON.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

% Capture filter Entity(*entity-name*) Sub-entity(*sub-entity-name*) already exists.

Prerequisites

None

Related commands

logging capture-filter entity remove {all | *entity-name* | *entity-name sub-entity-name***}**

Example

Example of a successful help for this command:

```
CES(config)# logging capture-filter ?
entity      Configures entity, sub-entity
severity    Configures severity

CES(config)# logging capture-filter entity ?
add         Adds entity, sub-entity
remove      Removes entity, sub-entity

CES(config)# logging capture-filter entity add ?
all         Adds all entities and sub-entities
hardware
io
mgmt
os
other
routing
security
system
tunnel
```

Example of a successful execution:

```
CES(config)# logging capture-filter entity add routing vrrp
CES(config)#
CES(config)# logging capture-filter entity add routing
CES(config)#
CES(config)# logging capture-filter entity add all
CES(config)#
```

logging capture-filter entity remove

Use this command to remove entities or sub-entities or both to capture filter.

Syntax

logging capture-filter entity remove {all | *entity-name* **|** *entity-name sub-entity-name***}**

Parameters

all	Remove all entities and sub-entities.
entity-name	Remove all sub-entities of a particular entity.
entity-name sub-entity-name	Remove a sub-entity of a particular entity.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

% Capture filter Entity(*entity-name*) Sub-entity(*sub-entity-name*) does not exist.

Prerequisites

None

Related commands

logging capture-filter entity add {all | *entity-name* **|** *entity-name sub-entity-name***}**

Example

Example of a successful help for this command:

```
CES(config)# logging capture-filter ?
entity      Configures entity, sub-entity
severity    Configures severity

CES(config)# logging capture-filter entity ?
add         Adds entity, sub-entity
remove      Removes entity, sub-entity

CES(config)# logging capture-filter entity remove ?
all         Removes all entities and sub-entities
hardware
io
mgmt
os
other
routing
security
system
tunnel
```

Example of a successful execution:

```
CES(config)# logging capture-filter entity remove routing
vrrp
CES(config)#
CES(config)# logging capture-filter entity remove routing
CES(config)#
CES(config)# logging capture-filter entity remove all
CES(config)#
```

logging capture-filter severity add

Use this command to add severities to capture filter.

Syntax

logging capture-filter severity add {all | *severity name***}**

Parameters

severity-name	Name of the severity to be added.

Default

All severities of capture filter are default to ON except debug.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

% Capture filter Severity(*severity-name*) already exists.

Prerequisites

None

Related commands

logging capture-filter severity remove {all | *severity-name*}

Example

Example of a successful help for this command:

```
CES(config)# logging capture-filter ?
entity      Configures entity, sub-entity
severity    Configures severity

CES(config)# logging capture-filter severity ?
add         Adds severity
remove      Removes severity

CES(config)# logging capture-filter severity add ?
alert
all         Adds all severities
crit
debug
emerg
err
info
notice
warning
CES(config)#
```

Example of a successful execution:

```
CES(config)# logging capture-filter severity add info
CES(config)#
CES(config)# logging capture-filter severity add all
CES(config)#
```

logging capture-filter severity remove

Use this command to remove severities from capture filter.

Syntax

logging capture-filter severity remove {all | *severity-name***}**

Parameters

severity-name	Name of severity to be removed.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

% Capture filter Severity(*severity-name*) does not exist.

Prerequisites

None

Related commands

logging capture-filter severity add {all | *severity-name*}

Example

Example of a successful help for this command:

```
CES(config)# logging capture-filter ?
entity      Configures entity, sub-entity
severity    Configures severity
CES(config)#

CES(config)# logging capture-filter severity ?
add         Adds severity
remove      Removes severity
CES(config)#

CES(config)# logging capture-filter severity remove ?
alert
all         Removes all severities
crit
debug
emerg
err
info
notice
warning
CES(config)#
```

Example of a successful execution:

```
CES(config)# logging capture-filter severity remove info
CES(config)#
CES(config)# logging capture-filter severity remove all
CES(config)#
```

logging display-filter entity add

Use this command to add entities or sub-entities or to display filter.

Syntax

logging display-filter entity add {all | *entity-name* **|** *entity-name sub-entity-name***}**

Parameters

all	Add all entities and sub-entities.
entity-name	Add all sub-entities of a particular entity.
entity-name sub-entity-name	Add a sub-entity of a particular entity.

Default

All entities and sub-entities of display filter are default to ON.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

% Display filter Entity(*entity-name*) Sub-entity(*sub-entity-name*) already exist.

Prerequisites

None

Related commands

logging display-filter entity remove {all | *entity-name* | *entity-name sub-entity-name***}**

Example

Example of a successful help for this command:

```
CES(config)# logging display-filter ?
entity      Configures entity, sub-entity
severity    Configures severity

CES(config)# logging display-filter entity ?
add         Adds entity, sub-entity
remove      Removes entity, sub-entity

CES(config)# logging capture-filter entity add ?
all         Adds all entities and sub-entities
hardware
io
mgmt
os
other
routing
security
system
tunnel
```

Example of a successful execution:

```
CES(config)# logging display-filter entity add routing vrrp
CES(config)#
CES(config)# logging display-filter entity add routing
CES(config)#
CES(config)# logging display-filter entity add all
CES(config)#
```

logging display-filter entity remove

Use this command to remove entities or sub-entities from display filter.

Syntax

logging display-filter entity remove {all | *entity-name* **|** *entity-name sub-entity-name***}**

Parameters

all	Removes all entities and sub-entities
entity-name	Removes all sub-entities for a particular entity
entity-name sub-entity-name	Removes a sub-entity of a particular entity

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

% Display filter Entity(*entity-name*) Sub-entity(*sub-entity-name*) does not exist.

Prerequisites

None

Related commands

logging display-filter entity add {all | *entity-name* **|** *entity-name sub-entity-name***}**

Example

Example of a successful help for this command:

```
CES(config)# logging display-filter ?
entity      Configures entity, sub-entity
severity    Configures severity

CES(config)# logging display-filter entity ?
add         Adds entity, sub-entity
remove      Removes entity, sub-entity

CES(config)# logging display-filter entity remove ?
all         Removes all entities and sub-entities
hardware
io
mgmt
os
other
routing
security
system
tunnel
```

Example of a successful execution:

```
CES(config)# logging display-filter entity remove routing
vrrp
CES(config)#
CES(config)# logging display-filter entity remove routing
CES(config)#
CES(config)# logging display-filter entity remove all
CES(config)#
```

logging display-filter severity add

Use this command to add severity to display filter.

Syntax

logging display-filter severity add {all | *severity-name***}**

Parameters

severity-name	Name of the severity to be added

Default

All severities of display filter are default to ON except debug.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

% Display filter severity(*severity-name*) already exist.

Prerequisites

None

Related commands

logging display-filter severity remove {all | *severity-name*}

Example

Example of a successful help for this command:

```
CES(config)# logging display-filter ?
entity      Configures entity, sub-entity
severity    Configures severity

CES(config)# logging display-filter severity ?
add         Adds severity
remove      Removes severity

CES(config)# logging display-filter severity add ?
alert
all         Adds all severities
crit
debug
emerg
err
info
notice
warning
CES(config)#
```

Example of a successful execution:

```
CES(config)# logging display-filter severity add info
CES(config)#
CES(config)# logging display-filter severity add all
CES(config)#
```

logging display-filter severity remove

Use this command to remove severities from display filter.

Syntax

logging display-filter severity remove {all | *severity-name***}**

Parameters

severity-name	Name of severity to be removed

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

% Display filte severity(*severity-name*) does not exist.

Prerequisites

None

Related commands

logging display-filter severity add {all | *severity-name*}

Example

Example of a successful help for this command:

```
CES(config)# logging display-filter ?
entity      Configures entity, sub-entity
severity    Configures severity

CES(config)# logging display-filter severity ?
add         Adds severity
remove      Removes severity

CES(config)# logging display-filter severity remove ?
alert
all         Removes all severities
crit
debug
emerg
err
info
notice
warning
CES(config)#
```

Example of a successful execution:

```
CES(config)# logging display-filter severity remove info
CES(config)#
CES(config)# logging display-filter severity remove all
CES(config)#
```

show logging capture-filter

Use this command to display configured entities, sub-entities, and severities for capture filter.

Syntax

```
show logging capture-filter
```

Parameters

None

Default

None

Command mode

Privileged Exec

Next command mode

Privileged Exec

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

show logging capture-filter entity
show logging capture-filter entity all
show logging capture-filter severity
show logging capture-filter severity all

Example

Example of a successful help for this command:

```
CES# show logging capture-filter ?
entity   Displays entities and sub-entities
severity Displays severities
<cr>
```

Example of a successful execution:

```
CES# show logging capture-filter
No event-log capture filter entity or sub-entity configured.
No event-log capture filter severity configured.
CES#
```

show logging capture-filter entity all

Use this command to display all available entities and sub-entities for capture filter.

Syntax

show logging capture-filter entity all

Parameters

None

Default

None

Command mode

Privileged Exec

Next command mode

Privileged Exec

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

show logging capture-filter
show logging capture-filter entity

Example

Example of a successful help for this command:

```
CES# show logging capture-filter entity ?
all      Displays all available entities and sub-entities
<cr>

CES# show logging capture-filter entity all ?
<cr>
```

Example of a successful execution:

```
CES# show logging capture-filter entity all
Entity: os, Sub-entity: general

Entity: hardware, Sub-entity: general
Entity: hardware, Sub-entity: fastenet
Entity: hardware, Sub-entity: gigenet

Entity: io, Sub-entity: general
Entity: io, Sub-entity: langeneral
Entity: io, Sub-entity: wangeneral
Entity: io, Sub-entity: wanserial
Entity: io, Sub-entity: wanppp
Entity: io, Sub-entity:wanfr
Entity: io, Sub-entity: wan1
Entity: io, Sub-entity: wan3

Entity: mgmt, Sub-entity: general
Entity: mgmt, Sub-entity: groupsbo
Entity: mgmt, Sub-entity: general
Entity: mgmt, Sub-entity: groupsbo
Entity: mgmt, Sub-entity: groupsusers
Entity: mgmt, Sub-entity: guidedconfig
Entity: mgmt, Sub-entity: healthcheck
Entity: mgmt, Sub-entity: ldap
Entity: mgmt, Sub-entity: ldapschema
Entity: mgmt, Sub-entity: profiles
Entity: mgmt, Sub-entity: quickstart
Entity: mgmt, Sub-entity: serialui
Entity: mgmt, Sub-entity: snmpagent
Entity: mgmt, Sub-entity: snmpibs
Entity: mgmt, Sub-entity: snmptraps
Entity: mgmt, Sub-entity: upgradewizard
Entity: mgmt, Sub-entity: webbrowser
Entity: mgmt, Sub-entity: accountingradius
Entity: mgmt, Sub-entity: nncli
Entity: mgmt, Sub-entity: nncliclivetool
Entity: mgmt, Sub-entity: nncliclivepar ser
Entity: mgmt, Sub-entity: featuregraphing
Entity: mgmt, Sub-entity: objectmanager
Entity: mgmt, Sub-entity: inthttpdaemon
Entity: mgmt, Sub-entity: intother
Entity: mgmt, Sub-entity: intunknown
```

```
Entity: mgmt, Sub-entity: intbulkload

CES#
```

show logging capture-filter entity

Use this command to display configured entities and sub-entities for capture filter.

Syntax

show logging capture-filter entity

Parameters

None

Default

None

Command mode

Privileged Exec

Next command mode

Privileged Exec

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

show logging capture-filter
show logging capture-filter entity all

Example

Example of a successful help for this command:

```
CES# show logging capture-filter entity ?
all      Displays all available entities and sub-entities
<cr>
```

Example of a successful execution:

```
CES# show logging capture-filter entity
Configured event-log capture filter entity, sub-entity:

Entity : routing,    Sub-entity : general
Entity : routing,    Sub-entity : bgp
Entity : routing,    Sub-entity : clip
Entity : routing,    Sub-entity : fem
Entity : routing,    Sub-entity : ospf
Entity : routing,    Sub-entity : qos
Entity : routing,    Sub-entity : rip
Entity : routing,    Sub-entity : routing
Entity : routing,    Sub-entity : rps
Entity : routing,    Sub-entity : rtm
Entity : routing,    Sub-entity : vrrp
Entity : routing,    Sub-entity : direct
Entity : routing,    Sub-entity : mrtm
Entity : routing,    Sub-entity : igmp
Entity : routing,    Sub-entity : static
Entity : routing,    Sub-entity : intfgrp
```

show logging capture-filter severity all

Use this command to display all available severities for capture filter.

Syntax

show logging capture-filter severity all

Parameters

None

Default

None

Command mode

Privileged Exec

Next command mode

Privileged Exec

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

show logging capture-filter severity

Example

Example of a successful help for this command:

```
CES# show logging capture-filter ?
entity   Displays entities and sub-entities
severity Displays severities
<cr>

CES# show logging capture-filter severity ?
all      Displays all available severities
<cr>

CES# show logging capture-filter severity all ?
<cr>
```

Example of a successful execution:

```
CES# show logging capture-filter severity all
Available severity:
alert
crit
debug
emerg
err
info
notice
warning
CES#
```

show logging capture-filter severity

Use this command to display all configured severities for capture filter.

Syntax

```
show logging capture-filter severity
```

Parameters

None

Default

None

Command mode

Privileged Exec

Next command mode

Privileged Exec

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

show logging capture-filter severity all

Example

Example of a successful help for this command:

```
CES# show logging capture-filter severity ?
all      Displays all available severities
<cr>
```

Example of a successful execution:

```
CES# show logging capture-filter severity
Configured event-log capture filter severity:
alert
info
CES#
```

Chapter 8
Branch office connection configuration commands

This chapter describes the branch office connection configuration commands.

Command	Page
bo-conn	486
compress	488
conn-type	489
filter	490
group	491
ipsec authentication	493
ipsec issuer-ca	494
ipsec relative-dn	496
ipsec server-ca	498
ipsec subject-alt-name	499
ipsec subject-dn	500
l2tp authentication	502
l2tp concentrator	503
l2tp ipsec-data-protection	504
l2tp stateless-mode	506
local-endpoint	507
local-gateway	508
local-network	510
mtu	511
mtu enable	513

Command	Page
nat	514
pptp authentication	515
remote-endpoint	517
remote-endpoint host	518
remote-network	520
routing	521
show bo-conn	523
state	524
tunnel-type	525

bo-conn

This command allows a user to configure, add, or delete a branch office connection or a control tunnel.

Syntax

```
bo-conn add <name> <grpname> [conn-type {initiator |
peer2peer | responder} | control-tunnel]
bo-conn <name> <grpname>
no bo-conn <name> <grpname>
```

Parameters

add	Add a branch office connection or a control tunnel.
control-tunnel	Specifies a branch office control tunnel
conn-type	Type of branch office connection. If omitted, a peer-to-peer (peer2peer) connection is created.
name	Name of a branch office connection.
grpname	Name of a branch office group.
no	Delete a branch office connection.

Default

None

Command mode

Global Configuration

Next command mode

Branch Office Connection or Global Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The specified branch office group must exit.

Warning messages

```
% Branch Office Connection already exists.
% No such group/connection exists
% Branch Office Connection xxx does exist.
```

Example

```
CES(config)# bo-conn add atob /base/cli
CES(config)# bo-conn add btoc /base control-tunnel
CES(config)# bo-conn atob /base/cli
CES(config)# no bo-conn atob /base/cli
```

compress

This command enables or disables the IPsec Hi/fn LZS compression or the PPTP, L2TP, or L2F Microsoft Point-to-Point Compression (MPPC) packet compression. This command is the same for the Group IPsec, L2F, L2TP, and PPTP configuration, and the Branch Office Group IPsec configuration modes. The **default** keyword defaults the compression value to that of the parent group.

Syntax

```
compress
no compress
default compress
```

Parameters

None

Default

Disable

Command mode

Group [IPsec | L2F | L2TP | PPTP] Configuration
Branch Office Group IPsec Configuration
Branch Office Connection PPTP or L2TP Configuration

Next command mode

Group [IPsec | L2F | L2TP | PPTP] Configuration
Branch Office Group IPsec Configuration
Branch Office Connection PPTP or L2TP Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ip domain-name

Example

```
CES(config-group/ipsec)# compress
CES(config-bo_group/ipsec)# compress
CES(config/bo-conn/pptp)# compress
CES(config/bo-conn/l2tp)# no compress
```

conn-type

This command specifies the peer-to-peer or asymmetric connection type.

Syntax

conn-type {**peer2peer** | **initiator** | **responder**}

Parameters

peer2peer	Peer-to-peer branch office connection type.
initiator	An asymmetric Branch Office tunnel type, where the branch user ID is used instead of the local IP address endpoint.
responder	An asymmetric Branch Office tunnel type, where the branch user ID is used instead of the remote IP endpoint.

Default

peer2peer

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config/bo-conn)# conn-type peer2peer
```

filter

This command sets a tunnel filter to be used for the configured connection.

Syntax

filter <*filterName*>

Parameters

filterName	The name of a tunnel filter.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

% Filter does not exist

Related commands

show filter tunnel

Example

```
CES(config/bo-conn)# filter myfilter
```

group

Use this command to specify which branch office group the current branch office connection belongs to. With this command, you can move an existing branch office connection to a different existing group.

Syntax

group *<boGroupName>*

Parameters

boGroupName	Specifies the branch office group name that you are moving the connection to. The branch office group must already be configured.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The branch office group and the connection must already exist.

Warning messages

```
% Branch Office Connection <name> does not exist
% Branch Office Group <name> does not exist
```

Related commands

bo-conn
show bo-conn

Example

```
CES(config)# bo-conn Test /Base
CES(config/bo_conn)# group /Base/HwGroup
CES(config/bo_conn)# exit
CES(config)#
```

ipsec authentication

This command specifies the authentication type for an IPsec tunnel and specifies a preshared password for the tunnel (both endpoints must use the same password).

Syntax

ipsec authentication certificates
ipsec authentication [**initiator-uid** <user-id>]
{*hex-pre-shared-key* <hex-key> | **text-pre-shared-key** <text-key> |
certificate-and-hex-pre-shared-key <hex-key> |
certificate-and-text-pre-shared-key <text-key>}

Parameters

certificate-and-hex-pre-shared-key	Enable two-factor authentication with a hexadecimal preshared key for branch office tunnels.
certificate-and-text-pre-shared-key	Enable two-factor authentication with a text preshared key for branch office tunnels.
certificates	Use digital certificates for IPsec tunnel authentication.
initiator-uid	Specify an initiator ID if you are configuring an ABOT connection.
hex-pre-shared-key	Specify a hexadecimal string (up to 32 characters) to be used for authentication. You must use the same string on both the local and remote IPsec tunnel end points.
text-pre-shared-key	Specify an alphanumeric string (up to 32 characters) to be used for authentication. You must use the same string on both the local and remote IPsec tunnel end points.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Example

The following example configures a text shared key for the branch office tunnel.

```
CES(config)# bo-conn test /Base
CES(config/bo-conn)# ipsec authentication
text-pre-shared-key secret
CES(config/bo-conn)#
```

ipsec issuer-ca

This command sets the valid issuer certificate authority for IPsec certificates authentication.

Syntax

ipsec issuer-ca <*cert*>

Parameters

cert	Valid issuer certificate authority.

Default

None

Command mode

User Configuration

Next command mode

Branch Office Connection IPsec Certificate Configuration
User Configuration

Required privileges

System Management – Manage
User Management – Manage (user configuration), None (Bo mode)

Warning messages

```
% Issuer CA does not exist
```

Related commands

ipsec server-ca (**BO Configuration**)

Example

```
CES(config-user)# ipsec issuer-ca “cn=testbeta, o=mycompany”
```

ipsec relative-dn

Use this command to create a relative distinguished name for IPsec branch office tunnels. Enter one of the seven options to execute the command correctly. Only one parameter can be entered at a time. If you need to configure several parameters, enter separate command lines. Use the **no** form of the command to delete configured attributes.

Syntax

ipsec relative-dn {**common-name** <*name*> | **country** <*country*> | **email** <*email*> | **locality** <*locality*> | **state** <*state*> | **organization** <*organization*> | **organizational-unit** <*unit-name*>}

no ipsec relative-dn {**common-name** | **country** | **email** | **locality** | **state** | **organization** | **organizational-unit**}

Parameters

name	Specifies the DN common name.
country	Specifies the DN country name.
email	Specifies the DN e-mail address.
locality	Specifies the DN locality name.
state	Specifies the DN common name.
organization	Specifies the DN organization name.
unit-name	Specifies the DN organizational unit name.
negotiated	Specifies that the IP address for the local interface will be negotiated with the remote PPP peer.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ipsec subject-alt-name
ipsec subject-alt-name

Example

The following example configures the relative distinguished name “main” located in “boston” for the IPsec branch office connection.

```
CES(config/bo_conn)# ipsec relative-dn common-name main
CES(config/bo_conn)# ipsec relative-dn locality boston
CES(config/bo_conn)#
```

The following example deletes the relative distinguished name located in “boston” for IPsec branch office connection.

```
CES(config/bo_conn)# no ipsec relative-dn locality boston
CES(config/bo_conn)#
```

ipsec server-ca

This command sets the server certificate.

Syntax

ipsec server-ca <*cert*> [**server-alt-name** <*altName*> **type** {**dns** | **email** | **ip-address**}]

Parameters

cert	Server certificate.
altName	Alternate name for specified server certificate.
type	Format of the name.
ip-address	IP address format.
email	Email name format.
dns	DNS name format.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Server certificate does not exist
% Server certificate alternate name does not exist
```

Related commands

ipsec issuer-ca
ipsec subject-dn

Example

```
CES(config/bo-conn)# ipsec server-ca “cn=server cert 2048
v03, st=ma, l=acton, ou=ipsec ces device, o=mycompany, c=us”
```

ipsec subject-alt-name

This command specifies a Subject Alternative name in place of a Subject DN, and specifies the format of the name.

Syntax

ipsec subject-alt-name <*name*> [**type** {**ip-address** | **email** | **dns**}]

Parameters

name	A character string representing the alternative name.
type	Format of the name.
ip-address	IP address (for example, 192.168.34.21).
email	Email name.
dns	DNS name (for example, gateway.cleveland.company.com.

Default

None

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ipsec subject-dn

Example

```
CES(config/bo_conn)# ipsec subject-alt-name Paris type dns
```

ipsec subject-dn

This command sets the subject distinguished name. Enclose in double quotation marks if subject DN contains spaces.

Syntax

ipsec subject-dn <*dnName*>

Parameters

dnName	The subject distinguished name.

Default

None

Command mode

User Configuration

Next command mode

User Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ipsec issuer-ca
ipsec server-ca
ipsec subject-alt-name

Example

```
CES(config/bo-conn)# ipsec subject-dn “mycompany”
```

l2tp authentication

This command enables the encryption authentication type and disables all the other types of encryption for L2TP tunnels.

Syntax

```
l2tp authentication local-uid <uid> [peer-uid <uid>
peer-password <password>]

l2tp authentication {none | rc4_40 | rc4_128}
[local-uid <uid>] [peer-uid <uid> peer-password <password>]
```

Parameters

local-uid	Specify the user name on the local gateway.
peer-uid	Specify the user name on the remote gateway.
peer-password	Specify the password for the user ID on the remote gateway.
none	Specify MS-CHAP V2 unencrypted as the authentication method.
rc4_40	Specify MS-CHAP V2 RC4-40 encryption as the authentication method.
rc4_128	Specify MS-CHAP V2 RC4-128 encryption as the authentication method.

Default

None

Command mode

Branch Office Connection L2TP Configuration

Next command mode

Branch Office Connection L2TP Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% No local UID was specified for authentication type L2TP.
% No peer UID was specified for authentication type L2TP.
```

Example

```
CES(config/bo-conn)# l2tp authentication rc4_128 local-uid
Fred peer-uid Bob peer-password ABBA
CES(config/bo-conn)# l2tp authentication rc4_40
CES(config/bo-conn)# l2tp authentication local-uid Bill
```

l2tp concentrator

This command sets the L2TP Access Concentrator (LAC) by using a LAC ID or disables it.

Syntax

l2tp concentrator <*lacId*>
no l2tp concentrator

Parameters

lacId	Specifies the LAC ID.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config/bo-conn)# l2tp concentrator lacId1
```

l2tp ipsec-data-protection

This command sets the minimum level of the IPsec data transport protection type for L2TP tunnels.

Syntax

```
l2tp ipsec-data-protection {none | des40 | des56 | 3des | ah}
```

Parameters

3des	Triple DES
des40	40 bit DES
des56	56 bit DES
none	Not required
ah	Authentication only

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config/bo-conn)# ipsec data-protection des56
```

l2tp stateless-mode

This command enables or disables the stateless mode for compression or encryption for an L2TP tunnel.

Syntax

```
l2tp stateless-mode
no l2tp stateless-mode
```

Parameters

None

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config/bo-conn)# l2tp stateless-mode
```

local-endpoint

This command sets the local IP address on the public interface on the local gateway if the connection type is responder or peer to peer.

Syntax

local-endpoint <*interfaceIp*>

Parameters

interfaceIp	The local gateway public interface IP address to use for the connection.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Physical interface xxx does not exist.
% Only a peer-to-peer branch office requires a local
endpoint.
```

Related commands

remote-endpoint

Example

```
CES(config/bo-conn)# local-endpoint 10.0.4.94
```

local-gateway

Use this command to specify the local gateway interface for asynchronous branch office tunnel initiator connections. Use the **no** form of the command to delete the local gateway interface.

Syntax

local-gateway <*slot*>/<*port*>[.<*subinterface*>]
no local-gateway

Parameters

slot	Specifies the slot number for the local gateway interface. Type an integer from 0 through 6.
port	Specifies the port number for the local gateway interface. Type an integer from 1 through 4.
subinterface	Specifies the subinterface number for an ATM virtual circuit (type **1**).

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show bo-conn

Example

The following example specifies the local gateway interface as slot 1 port 1.

```
CES(config/bo-conn)# local-gateway 1/1
CES(config/bo-conn)#
```

The following example specifies ATM VC 1 on interface 3/1 as the local gateway interface.

```
CES(config)# bo-conn testconn1 /Base
CES(config/bo-conn)# conn-type initiator
CES(config/bo-conn)# local-gateway 1/1
```

The following example deletes the local gateway interface.

```
CES(config/bo-conn)# no local-gateway
CES(config/bo-conn)#
```

local-network

This command sets the local network for the configured connection. For a branch office connection, it takes the name for a network. For a control tunnel, it takes the management IP address of the gateway or an IP address other than the management IP address; a NAT will be created underneath.

Syntax

local-network *<networkName>*

Parameters

networkName	For a branch office, the network name of an accessible network behind the local gateway. The network must already be defined.

Default

None

Command mode

Branch Office Connection Routing Static Configuration

Next command mode

Branch Office Connection Routing Static Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Local network xxx does not exist.
```

Example

```
CES(config/bo-conn)# routing static
CES(config/bo-conn/routing_static)# local-network mynetwork
```

mtu

Use this command to reset the maximum transmission unit (MTU) for a branch office tunnel. The MTU specifies the largest tunnel packet that can be sent; if a packet to be sent is larger than the configured MTU, the packet is fragmented or dropped. Use the **no** form of the command to reset the MTU value to its default value (1788 bytes).

Syntax

mtu <*bytes*>
no mtu

Parameters

bytes	Specifies the maximum transmission unit in bytes. Enter a value from 576 through 1788 bytes.

Default

1788

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

mtu enable
show bo-conn

Example

The following example sets the MTU for the branch office tunnel “test” to 1400 bytes.

```
CES(config)# bo-conn test /Base
CES(config/bo_conn)# mtu 1400
CES(config/bo_conn)#
```

The following example resets the MTU size for the branch office tunnel “test” to its default value (1788 bytes).

```
CES(config)# bo-conn test /Base
CES(config/bo_conn)# no mtu
CES(config/bo_conn)#
```

mtu enable

Use this command to enable a user-configured maximum transmission unit (MTU) for a branch office tunnel. The MTU specifies the largest tunnel packet that can be sent; if a packet to be sent is larger than the configured MTU, the packet is fragmented or dropped. Use the **no** form of the command to disable the use of a configured MTU value over the branch office tunnel.



Note: If you disable the MTU on the tunnel, the tunnel MTU is derived from the interface MTU.

Syntax

```
mtu enable
no mtu enable
```

Parameters

None

Default

Enabled

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

mtu
show bo-conn

Example

The following example disables the use of a configurable MTU for the branch office tunnel “test.”

```
CES(config)# bo-conn test /Base
CES(config/bo_conn)# no mtu enable
CES(config/bo_conn)#
```

The following example sets the MTU for the branch office tunnel “test” to 1500 bytes and enables the use of the edited MTU.

```
CES(config)# bo-conn test /Base
CES(config/bo_conn)# mtu 1500
CES(config/bo_conn)# mtu enable
CES(config/bo_conn)#
```

nat

This command sets the NAT name to be used for the network of the local gateway.

Syntax

nat *<natName>*

Parameters

natName	NAT name for an accessible network of the local gateway. This NAT set must already exist.

Default

None

Command mode

Branch Office Connection Static Routing Configuration

Next command mode

Branch Office Connection Static Routing Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config/bo-conn/routing_static)# nat myNat
```

pptp authentication

This command enables the encryption authentication type and disables all other types of encryption for PPTP tunnels.

Syntax

pptp authentication local-uid <*uid*> [**peer-uid** <*uid*> **peer-password** <*password*>]

pptp authentication {**none** | **rc4_40** | **rc4_128**} [**local-uid** <*uid*>] [**peer-uid** <*uid*> **peer-password** <*password*>]

Parameters

local-uid	Specify the user name on the local gateway.
peer-uid	Specify the user name on the remote gateway.
peer-password	Specify the password for the user ID on the remote gateway.
none	Specify MS-CHAP V2 unencrypted as the authentication method.
rc4_40	Specify MS-CHAP V2 RC4-40 encryption as the authentication method.
rc4_128	Specify MS-CHAP V2 RC4-128 encryption as the authentication method.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% No local UID was specified for authentication type PPTP.
% No peer UID was specified for authentication type PPTP.
```

Example

```
CES(config/bo-conn)# pptp authentication rc4_128 local-uid
Fred peer-uid BOB peer-password ABBA
CES(config/bo-conn)# pptp authentication rc4_40
```

remote-endpoint

Use this command to specify the remote gateway's public interface IP address for the connection, if the connection type is initiator or peer-to-peer.

Syntax

remote-endpoint <*IP_address*>

Parameters

IP_address	Specifies the remote gateway's public interface IP address.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% A responder branch office does not require a remote
endpoint.
```

Related commands

local-endpoint
remote-endpoint host

Example

The following example specifies the remote tunnel end point address for this tunnel connection.

```
CES(config)# bo-conn test1 /Base
CES(config/bo-conn)# remote-endpoint 10.0.3.90
CES(config/bo-conn)#
```

remote-endpoint host

Use this command to specify the remote end point of an IPsec asynchronous branch office tunnel as a DNS name instead of an IP address. This command is available only when the tunnel type is set to “initiator.”

Syntax

remote-endpoint host <*dns-name*>

Parameters

dns-name	Specifies the DNS name of the remote tunnel end point.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The branch office tunnel type must be set to “initiator.” Also, a DNS server must be configured to resolve the DNS name that you specify.

Related commands

local-endpoint
remote-endpoint

Example

The following example sets the tunnel type to “initiator” and specifies a DNS name for the remote end point of the IPsec ABOT.

```
CES(config)# bo-conn test1 /Base
CES(config/bo_conn)# conn-type initiator
CES(config/bo_conn)# remote-endpoint host ces1.public.com
CES(config/bo_conn)#
```

remote-network

This command allows you to add, edit, or delete a remote network.

Syntax

edit remote-network <*ipAddr*> **mask** <*maskIp*> **state** {**enable** | **disable**} **cost** <*cost*>

no remote-network <*ipAddr*> **mask** <*maskIp*>

remote-network <*ipAddr*> **mask** <*maskIp*> **state** {**enable** | **disable**} **cost** <*cost*>

Parameters

edit	Keyword to edit the remote network.
no	Delete a remote network.
mask	Keyword for indicating mask to specify a network.
state	Keyword for indicating state of a network.
cost	Keyword for indicating cost of a network.
ipAddr	The IP address for the network.
maskIp	The IP address for the mask of a network.
cost	The cost for the network (1 through 10000).
enable	Enable a network.
disable	Disable a network.

Default

None

Command mode

Branch Office Connection Configuration
Routing Static Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

local-network

Example

```
CES(config/bo-conn/routing_static)# remote-network
11.11.11.11 mask 255.255.0.0 state enable cost 12

CES(config/bo-conn/routing_static)# edit remote-network
11.11.11.11 mask 255.255.0.0 state disable cost 13

CES(config/bo-conn/routing_static)# no remote-network
11.11.11.11 mask 255.255.0.0
```

routing

This command configures the routing type for the connection, configures the routing settings for a connection and for static routing, and puts the CLI into the corresponding routing configuration mode. For Control Tunnel, only static routing is available.

Syntax

routing {**type** {**static** | **dynamic**} | **static** | **ospf** {**area-id** <*area-id*> **cost** <*cost*> | **enable** | **disable**} | **rip** {**cost** <*cost*> | **enable** | **disable**}}

Parameters

type	Sets the routing type to either static or dynamic.
static	Enters the static routing configuration mode.
dynamic	Set the routing type as dynamic.
ospf	Allows configuration of the OSPF settings.
area-id	The area ID for this connection.
area-id	Specified area ID, in IP address format.
cost	Cost of the OSPF area ID for this connection or for the RIP interface.
cost	Specifies the cost for the OSPF area ID or the RIP interface. For RIP, enter a value from 1 through 15.
rip	Enters RIP configuration mode.
enable	Enable OSPF or RIP.
disable	Disable OSPF or RIP.

Default

None

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Static Routing Configuration
Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% OSPF Area does not exist
```

Example

```
CES(config/bo-conn)# routing ospf area-id 1.1.1.1 cost 10

CES(config/bo-conn)# routing ospf disable

CES(config/bo-conn)# routing rip enable
```

show bo-conn

This command displays all branch office connections or all of the attributes for a specified connection.

Syntax

show bo-conn [<*connection_name*> <*grp_name*>]

Parameters

connection_name	Name of branch office connection for which to display attributes. If omitted, all branch office connection names will be displayed.
grp_name	Name of the connection's branch office group.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

bo-conn [**add**]
no bo-conn

Example

```
CES(config)# show bo-conn
CES(config)# show bo-conn atob /Base
```

state

This command enables or disables the connection configured.

Syntax

state {**disable** | **enable**}

Parameters

disable	Disables the connection configured.
enable	Enables the connection configured.

Default

Branch office configurations are enabled.

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

bo-conn

Example

```
CES(config/bo-conn)# state disable
```

tunnel-type

This command allows the user to change the type of the branch office tunnel.

Syntax

tunnel-type {**ipsec** | **l2tp** | **pptp**}

Parameters

None

Default

IPsec

Command mode

Branch Office Connection Configuration

Next command mode

Branch Office Connection Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ipsec authentication
l2tp authentication
pptp authentication

Example

```
CES(config/bo-conn)# tunnel-type pptp
```

Chapter 9
Access-hours, client policy, domains, and networks commands

This chapter describes client policy, domains, and networks commands.

Command	Page
access-hours	527
client-policy	529
domain add	530
network add	532
show access-hours	534
show client-policy	535
show domains	536
show networks	538

access-hours

This command adds and modifies the access hours, which specifies the time ranges when access is allowed for users in this group. The **no** variant deletes access hours. You can specify the without the **add** command to modify existing access hours.

Syntax

```
access-hours [add] <hours> [<day> <time-range>]
no access-hours <hours> [<day>]
```

Parameters

add	Specifies that the access-hours should be created.
hours	Access hours, which can contain spaces (enclosed in quotation marks) and must be fewer than 129 characters.
day	Day of the week.
time-range	Time range from 00:00:00 through 23:59:59.

Default

Default access hours include Anytime, Weekdays, and Weekends. If you add the access-hours and do not specify the time range, it is equivalent to Anytime.

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% These access hours already exist.
% Access hours do not exist.
```

Related commands

show client-policy

Example

```
CES(config-group)# access-hours add test1 Monday
00:00:01-12:00:00 Sunday 12:00:00-23:59:00
CES(config-group)# access-hours add NewHours
CES(config-group)# no access-hours test1
```

client-policy

This command adds a client policy or modifies an existing policy to define allowed applications. The **no** variant is used to delete a client policy or assigned applications.

Syntax

```
client-policy [add] <policy> [port <value> protocol {tcp | udp} type {client | server}]

no client-policy <policy> [port <value> protocol {tcp | udp} type {client | server}]
```

Parameters

add	Specifies that the policy or policy applications should be created.
policy	The client policy name. It can contain spaces, in which case it must be enclosed in double quotes. This must contain less than 129 characters.
port	Indicates that a port number needs to be added, edited, or deleted.
value	The port number that needs to be added, edited or deleted. The range is 0-65535.
protocol	The protocol that needs to be added, edited, or deleted.
type	The type of application that needs to be added, edited, or deleted.
server	Type of server application.
client	Type of client application.
tcp	TCP protocol.
udp	UDP protocol.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% Policy does not exist.
% No permitted applications specified.
% The application already exist.
```

Related commands

show client-policy

Example

```
CES(config-group)# client-policy add test1 port 12 protocol
tcp type client
CES(config-group)# client-policy test2 port 15 protocol udp
type client
CES(config-group)# no client-policy test1
CES(config-group)# no client-policy test2 port 15 protocol
udp type client
```

domain add

This command adds a domain set, including the domains in it. The **no** variant is used to delete a domain set or domain in the domain set.

Syntax

domain add <*domain_set*> [**domain-name** <*domain_name*>]
no domain <*domain_set*> [**domain-name** <*domain_name*>]

Parameters

add	Specifies that the domain or domain set should be created.
domain_set	The domain set. It can contain spaces, in which case it must be enclosed in double quotes. This must contain less than 129 characters.
domain-name	The name of the domain that needs to be added or edited. If this parameter is not present and this is an **add** command, then the **group-name** command must be used while in user configuration mode.
domain_name	The name of the domain. The name can contain spaces, in which case it must be enclosed in double quotes.

Default

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% Domain already exists.
% Domain set already exists.
% Domain does not exist.
% Domain set does not exist.
```

Related commands

show domains

Example

```
CES(config-group)# domain add France
CES(config-group)# domain add France domain-name Paris
CES(config-group)# domain add France domain-name Bordo
CES(config-group)# domain add France domain-name Leon
CES(config-group)# no domain France domain-name Leon
CES(config-group)# no domain France
```

network add

This command adds a network and allows you to assign IP addresses and subnet masks to the network. The **no** variant is used to delete a network or assigned IP addresses and subnet masks.

Syntax

network add <*network*> **ip** <*ip_address*> **mask** <*ip_address*>
no network <*network*> [**ip** <*ip_address*> **mask** <*ip_address*>]

Parameters

add	Specifies that the network or network set should be created.
network	The network name. It can contain spaces, in which case it must be enclosed in double quotes. This must contain less than 129 characters.
ip	The IP address of the network that needs to be added or deleted.
mask	The IP subnet mask of the network that needs to be added or deleted.
ip_address	IP address (A.B.C.D).

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% Network already exists.
% Network does not exist.
% Network IP or subnet mask does not exist.
% Network is currently assigned to configuration of Branch
Office xxxx.
```

Related commands

show networks

Example

```
CES(config-group)# network add test1 ip 123.21.22.78 mask
255.255.255.0
CES(config-group)# network add test1 ip 123.221.22.78 mask
255.255.255.0
CES(config-group)# network add test3 ip 133.21.22.78 mask
255.255.255.0
CES(config-group)# no network test1 ip 123.21.22.78 mask
255.255.255.0
CES(config-group)# no network test3
```

show access-hours

This command displays the currently configured access hours.

Syntax

show access-hours [<*hours*>]

Parameters

hours	Give detailed output for the specified access hours.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% These access hours do not exist.
```

Related commands

show domains
access-hours add

Example

```
CES(config-group)# show access-hours
 Anytime
 Weekdays
 Weekends

CES(config-group)# show access-hours weekends
Days     Hours Allowed:
Saturday 00:00:00 to 23:59:59
Sunday   00:00:00 to 23:59:59
```

show client-policy

This command displays the currently configured client policies.

Syntax

show client-policy [<*policy*>]

Parameters

policy	Give detailed output for the specified client policy.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Prerequisites

None

Warning messages

```
% Policy does not exist.
% No permitted applications specified.
```

Related commands

client-policy

Example

```
CES(config-group)# show client-policy
```

show domains

This command displays the currently configured sets of domains that you can use when specifying the Client Auto Connect feature.

Syntax

show domains [<*domain_set*>]

Parameters

domain_set	Show domains group.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% Domain does not exist.
% Domain set does not exist.
```

Related commands

show networks
show groups

Example

```
CES(config-group)# show domains

 France
 England

CES(config-group)# show domains France

 Paris
 Leon
 Bordo
```

show networks

This command displays the currently configured network routes that you can select when specifying split tunneling or branch offices.

Syntax

show networks [<*route*>]

Parameters

route	Show settings for specified route.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% Network does not exist.
```

Related commands

show domains
show groups

Example

```
CES(config-group)# show networks

 Base
 Management
 Paris

CES(config-group)# show networks Paris

125.25.21.2 255.255.0.0
192.32.25.25 255.255.0.0
```

Chapter 10
IP address pool commands

This chapter describes the commands used to configure local IP address pools and DHCP proxy on the gateway.

Command	Page
ip address-pool	542
show ip local pool	547

ip address-pool

Use this command to specify how the gateway obtains IP addresses to assign to remote clients that need to connect to the private network. Addresses can come from an internal address pool or from an external DHCP server.

Syntax

For local-pool:

```
ip address-pool local-pool [add | blackout-interval |
default | exhausted-amount | unavailable | WORD | <cr>]

no ip address-pool local-pool [<cr> | default | WORD]
```

For exernal DHCP:

```
ip address-pool external-dhcp

ip address-pool external-dhcp address-release

ip address-pool external-dhcp blackout-interval override

ip address-pool external-dhcp blackout-interval <300-86400>

ip address-pool external-dhcp cache-size <1-5000>

ip address-pool external-dhcp any

ip address-pool external-dhcp primary A.B.C.D [secondary |
tertiary]

ip address-pool external-dhcp secondary E.F.G.H [tertiary]

ip address-pool external-dhcp tertiary I.J.K.L

no ip address-pool external-dhcp

no ip address-pool external-dhcp address-release

no ip address-pool external-dhcp blackout-interval override
```

For internal DHCP:

```
ip address-pool internal-dhcp

ip address-pool internal-dhcp address-release

ip address-pool internal-dhcp blackout-interval override

ip address-pool internal-dhcp blackout-interval <300-86400>

ip address-pool internal-dhcp cache-size <1-5000>

no ip address-pool internal-dhcp

no ip address-pool internal-dhcp address-release

no ip address-pool internal-dhcp blackout-interval override
```

Parameters

add	Adds a new local address pool.
address-release	Specifies whether the DHCP proxy server on the gateway immediately releases an IP address back to the external DHCP server when a tunnel session terminates.
blackout-interval	Specifies the number of seconds that the gateway waits before it reassigns a released IP address to a new client.
cache-size	Specifies the local DHCP cache size. The local DHCP cache maintains the IP addresses obtained from remote DHCP servers.
default	Designates this pool as the default IP address pool.
exhausted-amount	Specifies the exhausting limit of an IP address pool that triggers the SNMP traps.
external-dhcp	Configures the gateway to obtain IP addresses for remote clients from an external DHCP server.
internal-dhcp	Configures the gateway to obtain IP addresses for remote clients from an internal DHCP server.

ip-address (primary, secondary, or `tertiary`)	Provides IP addresses for the specified DHCP servers. Type the IP addresses of the servers that provides DHCP service.
local-pool	Configures the gateway to obtain IP addresses for remote clients from an internal address pool.
unavailable	Specifies the action that the gateway takes if a user requests an address from a named pool and there are no addresses available.

Default

local

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

`ip dhcp proxy-server`
`ip local pool`

Example

The following example configures the gateway to obtain IP addresses for remote clients from an address pool maintained by a remote DHCP server.

```
CES(config)# ip address-pool external-dhcp
```

The following example configures the gateway to obtain IP addresses for remote clients from a local address pool. (To configure a local address pool, use the **ip local pool** command.)

```
CES(config)# ip address-pool local-pool
```

show ip dhcp proxy-server

Use this command to display the configuration of the DHCP proxy server on the gateway.

Syntax

show ip dhcp proxy-server

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

ip address-pool
ip dhcp proxy-server
ip dhcp proxy-server address-release
ip dhcp proxy-server blackout-interval
ip dhcp proxy-server blackout-interval override
ip dhcp proxy-server cache-size

Example

The following example shows the type of output that you see when the gateway can request service from any DHCP server.

```
CES# show ip dhcp proxy-server
DHCP Proxy Server Configuration
Internal DHCP server:    Enabled
DHCP Cache size:    1
Immediate Address Release:    Enabled
DHCP Blackout Interval:    300
Override Blackout Interval
when no addresses are available:    Enabled
External DHCP server:    Enabled
Type:    Any
DHCP Cache size:    1
Immediate Address Release:    Enabled
DHCP Blackout Interval:    300
Override Blackout Interval
when no addresses are available:    Enabled
Address Pools:    Enabled
```

The following example shows the type of output that you see when the gateway is configured to request service from specified DHCP servers.

```
CES# show ip dhcp proxy-server

   Name       Begin         End      Mask      Total      InUse
 default   10.20.20.10 10.20.20.19              10          0
 test1     10.20.20.20 10.20.20.29              10          0

Address Pool Exhausted Amount: 70%
Address Pool Blackout Interval: 0
   If Named Pool Unavailable: Deny address request
```

show ip local pool

Use this command to display configuration information about the local address pools configured on the gateway.

Syntax

show ip local pool [<*pool-name*>]

Parameters

pool-name	Specifies the name of a local address pool, for example, **default** or **mypool**. Use this parameter to display information about the specified local address pool only.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Address pool <pool-name> does not exist.
```

Related commands

ip address-pool
ip local pool
ip local pool blackout-interval
ip local pool unavailable

Example

The following example shows the type of output displayed when you enter the command with no address pool specified. In this example, the default address pool includes two address ranges.

```
CES# show ip local pool

    Name      Begin            End              Mask        Total   InUse

default     133.22.11.100    133.22.11.155    255.255.248.0    56    0
default     144.44.55.6      144.44.55.100                     95    0
mypool      123.22.11.2      123.22.11.80     255.255.0.0      79    0


Address Pool Blackout Interval:    0
     if Named Pool Unavailable:    Failover
```

The following example displays information about one address pool only.

```
CES# show ip local pool mypool

    Name      Begin            End              Mask        Total   InUse

mypool      123.22.11.2      123.22.11.80     255.255.0.0      79     0


Address Pool Blackout Interval:    0
     if Named Pool Unavailable:    Failover
```

Chapter 11
Administrator, system identity, time, Syslog, and NTP commands

This chapter describes system identity, system time, syslog, software upgrade and administration configuration commands.

Command	Page
adminname	553
clock dst-observance	555
clock set	557
clock timezone	558
compress-files enable	560
create diskette	562
create recovery	564
create safe-mode-config	565
default language	567
dns-proxy enable	568
erase config-file	569
exception backup	571
ftp-coredump	575
ftp-coredump enable	577
hostname	578
idle-timeout	579
ip address	581
ip domain-name	582
ip name-server	583

Command	Page
license	584
logging	586
ntp	588
ntp authentication-key	589
ntp broadcast server	590
ntp multicast server	591
ntp server	592
reformat diskette	594
retrieve backup	596
save current-config-file	598
scheduler manageability	599
show admin settings	601
show clock	602
show compress-files	603
show config-files	605
show current-config-file	606
show exception backup	607
show ftp-coredump	609
show hosts	610
show ip name-server	611
show license	613
show ntp	614
show scheduler	616
show status statistics admin	617
show status statistics hardware	620
show status statistics interfaces	624
show status statistics network	627
show status statistics resources	634
show status statistics routing	640
show status statistics security	642

Command	Page
show status statistics system	645
show syslog-host	652
show system accelerator	653
show system accelerator statistics	656
split-dns enable	659
system accelerator auto-recovery enable	660
system accelerator enable	662
verify system	663

adminname

Use this command to set the administrator login name and password. This login name and password is for the default administrator account that allows you to connect to the gateway for management only. This account is the only account that you can use to connect to the gateway over a serial line.

Note: The password is not validated. For example, the password can be set to the same string as the administrator name.

Syntax

adminname <*name*> **password** <*password*>

Parameters

name	Specifies the user name for the administrator account. This name can have as many as 32 characters but cannot contain spaces.
password	Specifies a password for the administrator account. The password can have as many as 32 characters but cannot contain spaces.

Default

If this command is not used, the administrator account name defaults to admin and the password defaults to setup.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Adminname too long
% Password too long
```

Example

This command sets the Nortel VPN Router administrator name to big_one and the administrator password to kixroute66.

```
CES# adminname big_one password kixroute66
```

clock dst-observance

This command sets the daylight saving time.

Syntax

`clock dst-observance`

Parameters

auto	Sets the daylight saving time to change automatically.
none	No daylight savings time.
noam	North American time.
extnoam	North American extended time.
weeu	Western Europe time.
uk	United Kingdom and Ireland time.
au	Australia time.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

clock timezone
show clock

Example

The following example sets the daylight savings time to automatically change.

```
CES# clock dst-observance auto
```

clock set

This command manually sets the system clock.

Syntax

clock set *<hh:mm:ss day month year>*

clock set *<hh:mm:ss month day year>*

Parameters

hh:mm:ss	Current time in hours, minutes, and seconds.
day	Current day (date) of the month.
month	Current month (by name).
year	Current year; type four digits, for example, 2004.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

clock timezone
show clock

Example

```
CES# clock set 11:25:30 5 February 2004
CES# clock set 11:25:30 February 5 2004
```

clock timezone

This command manually sets the system time zone.

Syntax

clock timezone <*zone*>

Parameters

zone is the name of the time zone to be displayed when standard time is in effect. Enter one of the following values:

bet	(GMT -11:00) Bering
hst	(GMT -10:00) Hawaii Standard Time
yst	(GMT -9:00) Yukon Standard Time
pst	(GMT -8:00) Pacific Standard Time
mst	(GMT -7:00) Mountain Standard Time
cst	(GMT -6:00) Central Standard Time
est	(GMT -5:00) Eastern Standard Time
ast	(GMT -4:00) Atlantic Standard Time
glte	(GMT -3:00) Greenland Time
ost	(GMT -2:00) Oscar Time
at	(GMT -1:00) Azores Time
gmt	(GMT) Greenwich Mean Time
cet	(GMT +1:00) Central Europe Time
nt	(GMT +2:00) Nile Time
ukt	(GMT +3:00) Ukraine Time
cat	(GMT +4:00) Caspian Sea Time
pte	(GMT +5:00) Pakistan Time
kt	(GMT +6:00) Kazakh Time
wast	(GMT +7:00) Java Time (West Australian Standard)
cct	(GMT +8:00) China Coast Time
jt	(GMT +9:00) Japan Time
mit	(GMT +10:00) Mariana Islands Time
cit	(GMT +11:00) Caroline Islands Time
nzst	(GMT +12:00) New Zealand Standard Time

Default

GMT

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management – Manage
User Management – None

Related commands

clock set
show clock

Example

```
CES# clock timezone pst
```

compress-files enable

Use this command to enable compression of the system log, accounting log, and LDIF files. Use the **no** form of the command to disable compression.

Syntax

compress-files enable
no compress-files enable

Parameters

None

Default

No compression

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show compress-files

Example

The following example enables file compression.

```
CES# configure terminal
CES(config)# compress-files enable
CES(config)#
```

The following example disables file compression.

```
CES(config)# no compress-files enable
CES(config)#
```

create diskette

Use this command to create a recovery diskette that you can use to restore the file system to the hard drive of the gateway in the event of a hard disk problem. This command creates a boot sector on the diskette and copies the system software files that are required to boot the gateway from the diskette.

The recovery diskette is included with your gateway. You can also use this command to create additional copies of the recovery diskette.

Note: You cannot use a recovery diskette for the Nortel VPN Router 1000 or the Nortel VPN Router 600 gateway because these devices do not have floppy drives. However, on the Nortel VPN Router 600, the recovery image is stored in PROM; you can invoke it by pressing a switch on the back of the unit. For more information, see *Getting Started with the Nortel VPN Router 600*.

After the recovery diskette is created (approximately 2 minutes), a message indicates the success or failure of the operation. If a recovery diskette was not created, follow the instructions provided by the gateway.

Syntax

```
create diskette
```

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Floppy drive not ready.
```

Related commands

create recovery
reformat diskette

Example

The following example creates a diskette on the gateway.

```
CES# create diskette
% Are you sure you want to create a recovery diskette?
(Yes/No)yes
Diskette Created.
CES#
```

create recovery

Use this command to create a recovery image on a diskette or in flash memory. You can use the recovery image to restore the file system to the hard drive of the gateway in the event of a hard disk problem. This command copies the system software files that are required to boot the gateway. After you execute this command, a message indicates whether the recovery image was created successfully, and if the image was not created, provides instructions.



Note: The Nortel VPN Router 600 and the Nortel VPN Router 1010, 1050, and 1100 do not have floppy drives. Use this command to create a recovery image in flash memory.

Syntax

```
create recovery
```

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Floppy drive not ready.
```

Related commands

create diskette

Example

The following example creates a recovery image in flash memory.

```
CES# create recovery
% Are you sure you want to update flash? (Yes/No)yes
 Creating Recovery file . . .
 Created.
CES#
```

create safe-mode-config

Use this command to create a safe mode configuration file. To create a safe mode configuration file, you must first enable safe mode using the **safe-mode enable** command.

Syntax

create safe-mode-config

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Error. To execute this command, safe mode must be enabled.
! Enable safe mode. Do not boot the device in safe mode.
```

Related commands

erase config-file
safe-mode enable
save current-config-file
show config-files
show current-config-file

Example

The following example creates a safe mode configuration file on the gateway.

```
CES(config)# create safe-mode-config
Created : /ide0/system/safe/config/CFG00011.DAT
CES(config)#
```

default language

This command specifies the default language that you want to use for the graphical user interface (GUI) on your gateway.

Although the gateway can be configured to be in either English or Japanese languages, *Japanese is no longer supported*. The Nortel VPN Router 1010/1050/1100 can only be configured in English.

Syntax

default language {**english** | **japanese**}

Parameters

english	The default language is English.
japanese	Not supported.

Default

English

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

adminname
show admin settings

Example

```
CES(config)# default language english
```

dns-proxy enable

This command enables DNS proxy on the gateway, enabling the gateway to act as a DNS server for the private side. Use the **no** form of this command to disable DNS proxy.

Syntax

```
dns-proxy enable
no dns-proxy enable
```

Parameters

None

Default

Enabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip name-server
show ip name-server
split-dns enable

Example

The following example disables DNS proxy.

```
CES(config)# no dns-proxy enable
CES(config)#
```

The following example reenables split DNS.

```
CES(config)# dns-proxy enable
CES(config)#
```

erase config-file

Use this command to delete a configuration file on the gateway.

Syntax

erase config-file {<*file-name*>}

Parameters

file-name	Specifies the name of the configuration file to be deleted. The file name can have up to eight alphanumeric characters.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

create safe-mode-config
save current-config-file
show config-files
show current-config-file

Example

The following example displays the names of the configuration files on the gateway and then deletes one of the files.

```
CES(config)# show config-files
CFG0731.DAT
CFG0802.DAT
CFG0806.DAT
CES(config)# erase config-file CFG0731.DAT
CES(config)# show config-files
CFG0802.DAT
CFG0806.DAT
CES(config)#
```

exception backup

Use this command to define backup FTP servers for the gateway. A backup FTP server receives a copy of the LDAP database, configuration file, and other system files that have changed since the last backup. After you configure a backup FTP server, you must explicitly enable the server to accept backup files.

The gateway supports up to three backup FTP servers; the Nortel VPN Router 4500, 4600, and 5000 also support the use of the internal redundant disk for backups. Use the **no** version of this command to revert to default values for the backup FTP servers.

Syntax

```
exception backup {1 | 2 | 3} {<ip-address> | <host-name>}
[<file-path>] [interval <hours> | time <hh:mm>]
username <user-name> password <password>

exception backup {1 | 2 | 3} {enable | disable}{sftp}

exception backup redundant {interval [<hours>] | time
[<hh:mm>]}

exception backup now

exception backup advanced {1 | 2 | 3} {full | partial}

exception backup advanced {1 | 2 | 3} {[configuration] [log]
[system]}

exception backup advanced {1 | 2 | 3} {every | sunday |
monday | tuesday | wednesday | thursday | friday | saturday}

default exception backup

no exception backup {1 | 2 | 3 | redundant}{sftp}

no exception backup advanced {1 | 2 | 3} {{full | partial} |
{[configuration] [log] [system]} | {every | sunday | monday
| tuesday | wednesday | thursday | friday | saturday}}
```

Parameters

1, 2, 3, redundant	Specifies the number of the backup server or, for the Nortel VPN Router 4*x*00 only, the redundant internal disk.
ip-address	Specifies the IP address of the backup server in dotted-decimal notation.
host-name	Specifies the DNS host name for the backup server.
file-path	Specifies the directory path on the backup server where the files will be written. **Note:** The specified directory must already exist on the backup server.
interval	Specifies the number of hours between backups. If you do not specify an interval or a time, backups take place every 5 hours.
hours	Specifies the number of hours between backups. For a remote backup server (1, 2, or 3), enter a value from 1-8064. For the redundant internal disk in the Nortel VPN Router 4*x*00, enter a value from 1-24.
time	Specifies a time for the backup.
*hh***:***mm*	Specifies the actual time for the backup. Type the value in this format: *hh*:*mm*, for example, **time 14:22**.
user-name	Specifies the user name that the gateway will use to establish the FTP connection to the backup server.
password	Specifies the user password that the gateway will use to establish the FTP connection to the backup server.
enable	Enables backup on the specified FTP server.
disable	Disables backup on the specified FTP server.
sftp	Use sftp to transfer files.
now	Back up to all enabled backup servers now.
advanced	Specifies that you will supply fine-tuning parameters for backups, such as the days that backups will be done and the files that will be backed up.
full	Specifies that full backups will be performed, that is, system, configuration, and log files will be backed up. The gateway performs a full backup by default.
partial	Specifies that not all files will be backed up. You specify the files to back up (configuration, log, or system files, or a combination of these) on another command line.

configuration	Specifies that only configuration files will be backed up.
log	Specifies that only log files will be backed up.
system	Specifies that only system files will be backed up.
every	Specifies that backups will be performed every day.
sunday . . . **saturday**	Specifies that backups will be performed on the specified day. To schedule backups for more than one day, you must enter separate commands for each day.

Default

Full backups are performed every day at 5-hour intervals.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Redundant backup is not available on this model
```

Related commands

show exception backup

Example

The following example configures a server with an IP address of 12.0.44.129 as backup FTP server 1. The first command configures the gateway to automatically back up files at 2:00 AM every day. The second command changes the server configuration to back up files every 8 hours instead of daily at 2:00. Finally, the third command enables automatic backup on that server.

```
CES(config)# exception backup 1 12.0.44.129 time 2:00
username BackupLogon password BackupPassword
CES(config)# exception backup 1 12.0.44.129 interval 8
username BackupLogon password BackupPassword
CES(config)# exception backup 1 enable
```

The following examples configure the redundant internal disk of a Nortel VPN Router 4600 gateway as a backup server. The first example configures backups for 2:00 PM every day; the second example configures backups to take place every 12 hours.

```
CES(config)# exception backup redundant time 14:00
CES(config)# exception backup redundant interval 12
```

The following example modifies backup server 2 to perform only partial backups, that is, the server will back up only system and log files.

```
CES(config)# exception backup advanced 2 partial
CES(config)# exception backup advanced 2 system log
```

The following example configures backup server 2 for a full backup. (You would use this command if you previously configured the server for partial backups.)

```
CES(config)# exception backup advanced 2 full
```

If you are not sure which partial configuration parameters are active, you can reset the backup configuration to default values (all system, configuration, and log files are backed up every day).

In the following example, the first commands clear all settings; the subsequent commands configure the gateway to back up only configuration and log files on Monday, Wednesday, and Friday.

```
CES(config)# exception backup advanced 1 full
CES(config)# exception backup advanced 1 every
CES(config)# exception backup advanced 1 config log
CES(config)# exception backup advanced 1 monday
CES(config)# exception backup advanced 1 wednesday
CES(config)# exception backup advanced 1 friday
```

ftp-coredump

This command specifies the FTP server that will store core dumps created by the Nortel VPN Router 1010, 1050, and 1100 gateways. Use the **no** form of this command to delete the FTP server specification for core dumps.

Syntax

ftp-coredump host <*ip-address*> [**path** <*path-name*>] **user-id** <*user_ID*> **password** <*password*>
no ftp-coredump

Parameters

ip-address	Specifies in dotted-decimal notation the IP address of the FTP server that will store core dumps from the gateway.
path-name	Specifies the path to the directory on the FTP server where you want to store the core files. (If this directory does not exist, it is created.) If you do not specify a path, the core file is placed in the root directory of the FTP server.
user-ID	Specifies the user name used to log in to the FTP server host system.
password	Specifies the password for the user login name on the FTP server host system.

Default

No FTP server for core dumps is configured.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ftp-coredump enable
show ftp-coredump

Example

The following example shows how to configure an FTP server for core dumps and how to enable backups to that server.

```
CES(config)# ftp-coredump host 192.33.249.4 path ces/cores
user-id george13 password eewG32L=73
CES(config)# ftp-coredump enable
CES(config)#
```

The following example shows how to delete the FTP core dump server specification.

```
CES(config)# no ftp-coredump
CES(config)#
```

ftp-coredump enable

This command enables the FTP core dump utility for a Nortel VPN Router 1010, 1050, or 1100 gateway. Use the **no** form of this command to disable the sending of core dump files to an FTP server.

Syntax

```
ftp-coredump enable
no ftp-coredump enable
```

Parameters

None

Default

The FTP core dump utility is disabled.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
ftp-coredump
show ftp-coredump
```

Example

The following example enables the sending of core dump files to an FTP server.

```
CES(config)# ftp-coredump enable
CES(config)#
```

The following example disables the sending of core dump files to an FTP server.

```
CES(config)# no ftp-coredump enable
CES(config)#
```

hostname

This command sets the system host's name. This should be the same name that is used by the Domain Name Service (DNS) server to identify the management address of the gateway that is located on your private network.

Syntax

hostname <*string*>
no hostname <*string*>

Parameters

string	Name of the system host. You can enter up to 64 characters.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

ip domain-name

Example

```
CES(config)# hostname new_server
```

idle-timeout

The idle timeout setting is used to force an automatic logout when an administrator session is not in use. This setting controls the timeout for all administrators. The **no** form of this command disables the idle timeout for administrator sessions.

Syntax

idle-timeout {<*hh:mm:ss*> | **enable**}
no idle-timeout enable

Parameters

hh:mm:ss	Current time in hours (military format), minutes, and seconds. The range of the idle timeout is 00:01:00 to 23:59:59.
enable	Enable the idle timeout for administrator sessions. By default, the idle timeout is disabled, even if you specify a timeout value.

Default

00:15:00 (15 minutes)

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Idle time out cannot be set to less than 1 minute
```

Related commands

adminname

Example

The following example sets the idle timeout for administrator sessions to 2 minutes and enables the timeout.

```
CES(config)# idle-timeout 00:02:00
CES(config)# idle-timeout enable
```

ip address

This command specifies the management IP address for the system. To be accessible, the management IP address must map to the same network as one of the private interfaces.

Syntax

ip address <*ip_address*>

Parameters

ip_address	Management IP address.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% Modifying the System Management IP address will make your
system unreachable
```

Related commands

ip domain-name
ip name-server

Example

```
CES(config)# ip address 10.0.3.121
```

ip domain-name

This command defines the DNS domain name.

Syntax

```
ip domain-name <string>
no ip domain-name <string>
```

Parameters

string	Domain name.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

ip address
hostname

Example

```
CES(config)# ip domain-name mycompany.com
```

ip name-server

This command specifies the address of one or more Domain Name Servers to use for name and address resolution. You can specify as many as four servers. To remove the addresses specified, use the **no** form of this command.

Syntax

```
ip name-server <server-address1> [<server-address2>]
[<server-address3>] [<server-address4>]
no ip name-server <server-address1> [<server-address2>]
[<server-address3>] [<server-address4>]
```

Parameters

server-address1	Specifies the IP address of the first DNS server to use for name and address resolution.
server-address2	Specifies the IP address of the second DNS server to use for name and address resolution.
server-address3	Specifies the IP address of the third DNS server to use for name and address resolution.
server-address4	Specifies the IP address of the fourth DNS server to use for name and address resolution.

Default

No DNS servers are configured.

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

dns-proxy
show ip name-server
split-dns enable

Example

The following example configures two DNS name servers and then removes a server.

```
CES(config)# ip name-server 12.32.112.2 12.32.112.4
CES(config)# no ip name-server 12.32.112.2
CES(config)#
```

license

Use this command to enable a license key for a paid feature on a Nortel VPN Router gateway. Use the **no** form of the command to delete a license.

Syntax

license install {**ar** | **dw** | **fw**} <*license-key*>
no license {**ar** | **dw** | **fw**}

Parameters

ar	Specifies that an Advanced Routing license key is to be installed or removed.
dw	Specifies that a Data Link Switching license key is to be installed or removed.
fw	Specifies that a Nortel VPN Router Stateful Firewall license key is to be installed or removed.
license-key	String that represents a valid feature license key. The first two characters of this key represent the license key prefix.

Default

No paid licenses are installed.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Failed to remove paid feature <feature-name>.
% Invalid license key.
% Unknown paid feature <feature-name>.
```

Related commands

show license

Example

The following example installs a license key for the Nortel VPN Router Stateful Firewall.

```
CES# configure terminal
CES(config)# license install fw fw-7384034-0342859268-d4
CES(config)#
```

The following example removes a license key for the Nortel VPN Router Stateful Firewall.

```
CES(config)# no license fw
CES(config)#
```

logging

This command enables the syslog server host for the forwarding information from the system log to host machines via the system logging daemon (syslogd). You can send different levels of information to different hosts. For example, you might send only “Urgent” system information to your primary system while sending “All” messages to a system you use for backup. No form of the command deletes the syslog server host.

The last sent message prior to disabling forwarding notifies the remote host that forwarding has been disabled.

Syntax

logging <*host*> [**facility** [**kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7**] **level** [**normal** | **urgent** | **detailed** | **all**] **port** <*port_number*>]
no logging <*host*>

Parameters

host	Either the fully qualified domain name or the IP address of the remote machine to which the log information will be sent.
facility	Logging facility.
kern	Logging kernel.
local0, local1...	Logging local use.
level	Message level.
normal	Normal events are the everyday user and system interactions that allow you to review gateway activity.
urgent	Urgent events are those that you want to be aware of immediately and that could potentially pose security or access problems.
all	All events.
detailed	Detailed events are designed specifically for use by Nortel Customer Support personnel to troubleshoot problems.
port	UDP port.
port_number	Port number from 1-9999).

Default

Facility kern
Port 514
Level normal

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

show syslog-host

Example

```
CES(config)# logging 123.21.21.1 facility local0 level all
port 240
CES(config)# logging 123.21.21.1
CES(config)# no logging 123.21.21.1
```

ntp

This command disables or enables the Network Time Protocol (NTP) for the gateway.

Syntax

ntp
no ntp

Parameters

None

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

ntp server

Example

```
CES(config)# ntp
CES(config)# no ntp
```

ntp authentication-key

This command specifies a Message Digest (MD5) authentication key for the Network Time Protocol (NTP). Use the **no** form of this command to remove the authentication key for NTP.

Syntax

ntp authentication-key <*key-number*> **password** <*secret*>
no ntp authentication-key <*key-number*>

Parameters

key-number	Key number (0-65535) of the authentication key to be trusted.
password	Authentication key. Message authentication support is provided using the MD5 algorithm.
secret	Key value; the key value can be up to 30 characters in length and cannot contain spaces.

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% Trusted-key does not exist.
% Trusted-key already exists.
```

Related commands

ntp server

Example

```
CES(config)# ntp authentication-key 2506 md5 Paris
CES(config)# no ntp authentication-key 2506
```

ntp broadcast server

This command allows the system to listen for and respond to NTP broadcast messages. NTP listens for broadcast messages at the group address of the global network. To avoid disruption in broadcast mode, both the client and the servers should use authentication and the same trusted key and key identifier.

Syntax

ntp broadcast server
no ntp broadcast server

Parameters

None

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

ntp multicast server

Example

```
CES(config)# ntp broadcast server
```

ntp multicast server

This command allows the system to listen for and respond to NTP multicast messages. The IP multicast address for NTP is 224.0.1.1.

Syntax

```
ntp multicast server
no ntp multicast server
```

Parameters

None

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

ntp broadcast server

Example

```
CES(config)# ntp multicast server
```

ntp server

This command allows the system clock to be synchronized by a time server. Use the **no** form of this command to disable this capability on the gateway.

Syntax

ntp server <*ip_address*> **source** {**private** | **public**} **key** <*key_ID*> **bursting** {**enable** | **disable**} **version** <*number*>
no ntp server <*ip_address*>

Parameters

ip_address	IP address of the NTP server.
source	Identifies the interface: public or private.
private **public**	Specifies the interface from which to choose the IP source address. The private interface is the management IP address. When you add a public interface, you can choose from a list of public interfaces. If you use the Nortel VPN Router Stateful Firewall, you must configure an interface filter to add NTP.
key	Defines the authentication key.
key_ID	Authentication key to use when sending packets to this peer.
bursting	Enables or disables the sending of more than one packet.
version	NTP version number.
number	NTP version number (1, 2, 3, or 4) used on the NTP server. The default is 4.

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% NTP server does not exist
% NTP server already exists
```

Related commands

ntp authentication-key

Example

```
CES(config)# ntp server 123.21.21.11 source private key 1235
bursting disable version 3
CES(config)# no ntp server 123.21.21.11
```

reformat diskette

Use this command to format the diskette in the floppy drive. Use this command with caution; it erases all information on the diskette. The system prompts you for verification before it reformats the diskette.

Syntax

reformat diskette {**quick** | **full**}

Parameters

full	Specifies that the data sectors that make up the storage space will be created. Use this option for unformatted diskettes.
quick	Specifies that only the header files and the existing data are to be rewritten. Use this option for diskettes that have already been used.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Disk format operation failed. The disk may be
write-protected.
```

Related commands

create diskette

Example

The following example reformats a diskette (quick mode).

```
CES# reformat diskette quick
% Are you sure you want to reformat the diskette in Quick
mode?(Yes/No)yes
Diskette Reformatted.
CES#
```

The following example formats a new, unformatted diskette (full mode).

```
CES# reformat diskette full
% Are you sure you want to reformat the diskette in Full
mode?(Yes/No)yes
Diskette Reformatted.
CES#
```

retrieve backup

Use this command to restore the Nortel VPN Router 1000 gateway's previously backed-up configuration. The backed-up file system, including software image and configuration files from the latest backup copy residing on the designated server, is restored onto the hard drive of your gateway. Refer to the **exception backup** command for information about auto backup.

Alternatively, a new factory default software image and file system can be restored to the hard disk. Specify the name or address and path of the network file server onto which the software from the Nortel CD has been installed.

Note: This command restores the disk to an operable but "clean" condition (configuration values are set to factory defaults).

Syntax

retrieve backup {<*host-name*> | <*ip-address*>} [**path** <*directory*>] **uid** <*uid*> **password** <*password*>

Parameters

host-name	Specifies the host name of the remote FTP server from which you are retrieving the backup files.
ip-address	Specifies the IP address of the remote FTP server from which you are retrieving the backup files.
directory	Specifies the path on the FTP server to the location of the backup files.
uid	Specifies the user ID required to log into the remote FTP server.
password	Specifies the password required to log into the remote FTP server.

Default

None

Command mode

Privileged EXEC

Next command mode

None

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% No DNS translation for the specified host name.
% Cannot establish connection with the host.
```

Related commands

exception backup

Example

```
CES# retrieve backup 1.1.1.1 uid admin password setup
% Are you sure you want to restore backup from 1.1.1.1?
(Yes/No)yes
Backup configuration and image have been restored.
CES#
```

save current-config-file

Use this command to save the current system configuration file.

Syntax

save current-config-file [<*file-name*>]

Parameters

file-name	Specifies a file name for the system configuration file. You can enter up to eight alphanumeric characters. Nortel recommends that you include a date or a serial number in the file name, for example, CFG0715.DAT.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
create safe-mode-config
erase config-file
show config-files
show current-config-file
```

Example

The following example saves the running configuration file to disk.

```
CES(config)# save current-config-file CFG0715.DAT
CES(config)#
```

scheduler manageability

Use this command to allow better manageability under high CPU utilization (management processes at priority 50). Use the **no** form of the command to allow better performance of the Nortel VPN Router gateway (management processes at priority 200). Use this command only if expecting certain high CPU operations (boot, reconfigurations, LDAP reconfiguration, and so on).

Syntax

```
scheduler manageability enable
no scheduler manageability enable
```

Parameters

None

Default

Disabled

Configuration mode

Global Configuration

Next configuration mode

Global Configuration

Required privileges

Services Management - Manage
User Management - None

Related commands

show scheduler

Example

The following example enables manageability mode.

```
CES# configure terminal
CES(config)# scheduler manageability enable
CES(config)#
```

The following example disables manageability mode.

```
CES(config)# no scheduler manageability enable
CES(config)#
```

show admin settings

This command displays the following settings for the administrator account: primary administrator user ID and password, the administrator idle timeout for all administrators, and the default language.

Syntax

show admin settings

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - View
User Management - None

Related commands

adminname
idle-timeout
default language

Example

```
CES# show admin settings
-------------------------------------
User ID  : admin
Password : *****
Language : English
Idle Time Out  :   00:15:00
Status   : DISABLED
```

show clock

This command shows the current date, time, and day of the week for the gateway.

Syntax

show clock [**detail**]

Parameters

detail	Displays the NTP clock source and the current summer-time setting (if any).

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Prerequisites

None

Related commands

clock set

Example

```
CES> show clock
15:29:03.158 PST Mon May 6 2004

CES> show clock detail
15:29:03.158 PST Mon May 6 2004
Time source is NTP
```

show compress-files

Use this command to find out whether file compression is enabled or disabled.

Syntax

show compress-files

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

compress-files enable

Example

The following example enables and disables file compression and displays the state of compression at each stage.

```
CES# configure terminal
CES(config)# compress-files enable
CES(config)# exit
CES# show compress-files
File Compression: enabled
CES# config term
CES(config)# no compress-files enable
CES(config)# exit
CES# show compress-files
File Compression: disabled
CES#
```

show config-files

Use this command to display a list of all configuration files on the gateway.

Syntax

show config-files

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

create safe-mode-config
erase config-file
save current-config-file
show current-config-file

Example

The following example displays the names of the configuration files on the gateway.

```
CES(config)# show config-files
CFG0731.DAT
CFG0802.DAT
CFG0803.DAT
CFG0005.DAT
CFG0806.DAT
CES(config)#
```

show current-config-file

Use this command to display the name of the current system configuration file.

Syntax

show current-config-file

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

create safe-mode-config
erase config-file
save current-config-file
show config-files

Example

The following example displays the name of the running configuration file.

```
CES# show current-config-file
The current config file is :
/ide0/system/config/CFG00033.DAT
CES#
```

Show exception backup

This command displays information about the configured backup FTP servers for the gateway.

Syntax

show exception backup

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% No backup FTP servers defined.
```

Related commands

exception backup

Example

The following command shows the output when two backup FTP servers are defined. There is no backup file path defined for the second server.

```
CES(config)# show exception backup
Backup FTP Server 1
  Server Address :  12.0.44.129
  Server Enabled :  ENABLED
  Server Status  :  Configured
  Backup Filepath:  /dev1/CES/Backup
  Specific Time  :  02:00:00
  Server Username:  BackupLogon
  Backup Type    :  Full
  Backup Days    :  Su Mo Tu We Th Fr Sa
```

```
 Backup FTP Server 2
  Server Address :  zanzibar
  Server Enabled :  ENABLED
  Server Status  :  Configured
  Backup Filepath:
  Backup Interval:  24
  Server Username:  sysadmin2
  Backup Type    :  Partial (System Files, Log Files)
  Backup Days    :  Su Mo Tu We Th Fr Sa
CES(config)#
```

show ftp-coredump

This command displays information about the FTP server used to store core dump files generated by the Nortel VPN Router 1010, 1050, or 1100 gateway.

Syntax

show ftp-coredump

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

ftp-coredump
ftp-coredump enable

Example

The following example shows the type of output you see when you execute the **show ftp-coredump** command. Passwords are replaced by "x" characters.

```
CES# show ftp-coredump
FTP Coredump is enabled
   Host: 143.35.122.15
   Path: ide0/store1/
   User-ID: george13
   Password: xxxxxxxxxx
CES#
```

show hosts

This command shows the management IP address, domain identity, and DNS server address.

Syntax

show hosts

Parameters

None

Default

00:15:00 (15 minutes)

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management – View
User Management – None

Related commands

adminname

Example

```
CES# show hosts
```

show ip name-server

This command displays information about the DNS servers configured for the gateway.

Syntax

show ip name-server

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

ip name-server
split-dns enable

Example

The following example shows the information displayed by this command.

```
CES# show ip name-server
DNS Server Configuration
DNS Proxy State: DISABLED
Split DNS State: DISABLED
Primary Server: 0.0.0.0 Server not configured
Second Server: 0.0.0.0  Server not configured
Third  Server: 0.0.0.0  Server not configured
Fourth Server: 0.0.0.0  Server not configured
ISP Provided DNS Servers
   No Provided Servers
CES#
```

show license

Use this command to display the status of features that require a paid license.

Syntax

show license

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

license

Example

The following example shows the type of information displayed by the **show license** command.

```
CES(config)# show license
   Advanced Routing                     Installed
   Nortel VPN Router Stateful Firewall Not installed
CES(config)#
```

show ntp

This command displays the NTP settings for the gateway.

Syntax

show ntp

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Warning messages

```
% There are no trusted keys in the database.
% There are no servers in the database.
```

Related commands

ntp
ntp authentication-key
ntp broadcast server
ntp multicast server
ntp server
show clock

Example

```
CES>show ntp
NTP: enable
Synchronize time with Broadcast Server: enable
Synchronize time with Multicast Server: enable
Servers:
Server IP Address Interface Key ID Bursting Version
123.23.2.33       Private   None    Disabled Default
Authentication keys: 1232321
CES>
```

show scheduler

Use this command to display the status of manageability mode.

Syntax

show scheduler

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

Services Management - Manage
User Management - None

Related commands

scheduler manageability

Example

The following example displays the status of manageability mode on the gateway.

```
CES# show scheduler
Scheduler Configuration
  Manageability: enabled
CES#
```

show status statistics admin

Use this command to display administrative statistics for branch office configurations, load balancing, and sessions.

Syntax

show status statistics admin {**branch-office-config** | **load-balancing** | **session-stats**}

Parameters

branch-office-config	Displays branch office configuration statistics.
load-balancing	Displays the traffic load allocation.
session-stats	Displays session statistics.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

show status statistics hardware
show status statistics interfaces
show status statistics network
show status statistics resources
show status statistics routing
show status statistics security
show status statistics system

Example

The following example shows the statistics displayed for branch office configurations.

```
CES> show status statistics admin branch-office-config
Date:  08/16/2003  Time: 11:13:31
Number of branch offices: 0
       SNMP Traps Nailed Up enabled:0   OnDemand enabled:0
IPSEC transports:
CES>
```

The following example shows the statistics displayed for load balancing.

```
CES> show status statistics admin load-balancing
Date:  08/16/2003  Time: 11:11:46
Pong service is disabled (version 2)
Sender:   task ID = 0x00000000     file desc= 0

Receiver: task ID = 0x00000000     file desc= 0


server          intf            state ttl  idle  con0   con1 con2   con3
0.0.0.0          0.0.0.0          0x00  00     0      0      0 0      0
                         (bandwidth in 64kbps)       0      0 0      0
0.0.0.0          0.0.0.0          0x00  00     0      0      0 0      0
                         (bandwidth in 64kbps)       0      0 0      0
CES>
```

The following example shows the statistics displayed for sessions.

```
CES> show status statistics admin session-stats
Date:  08/16/2003  Time: 11:13:11

Active user sessions (CAP = Call Admission Priority):

LOCAL[admin]:27 Tunnel FLASH 192.32.161.136 FLT [permit all]
SESS [070bb1a8]  CAP 255
LOCAL[admin]:26 Tunnel FLASH 192.32.161.136 FLT [permit all]
SESS [022e1c80]  CAP 255

Active tunnel sessions:

Active gateway sessions:

CES>
```

show status statistics hardware

Use this command to display hardware statistics.

Syntax

```
show status statistics hardware {devices | hw-accel-info |
hw-accel-stats | pace-drivers}
```

Parameters

devices	Displays the device drivers associated with the gateway.
hw-accel-info	Displays hardware accelerator information.
hw-accel-stats	Displays hardware accelerator statistics.
pace-drivers	Displays metrics that are used by the Packet Content Engine, a Nortel internal system.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

show status statistics admin
show status statistics interfaces
show status statistics network
show status statistics resources
show status statistics routing
show status statistics security
show status statistics system

Example

The following example shows the first portion of the statistics displayed for the hardware device drivers.

```
CES> show status statistics hardware devices
Date:  08/16/2003  Time: 10:28:40
drv name
   0 /null
   1 /tyCo/0
   1 /tyCo/1
   1 /tyCo/2
   1 /tyCo/3
   2 /pcConsole/0
   2 /pcConsole/1
   4 /ide0/
   4 /ram/
   6 host:
   7 /pty/telnet0.S
   7 /pty/telnet0.M
.
.
.
CES>
```

The following example shows the statistics displayed for the hardware accelerator information.

```
CES> show status statistics hardware hw-accel-info
Date 01/29/2004  Time 02:00:30
Hardware Accelerater Attributes:   Nortel Networks 7854
Accelerator Rev1
    vendor 0x000013a3 device 0x00000014
        which translates to type 1 and subtype 3
     flashkey 28
 There are currently 1 found in system.
 Capabilities            :   000010c1
System identifiers:
 Unit Identifier         :   0
 PCI Slot                :   5
 DevLoc                  :  261
Hw Accelerator Unit 0 status:
 Operational Status      :  3 - ACTIVE
 Fault Reason            :  0 - None
 Administrative Status   :  Enabled
 Auto Recovery State     :  Enabled
 Unit uptime             :  03:29:34
 Boot count              :  1
 Max sessions            :  8160
CES>
```

The following example shows the statistics displayed for the hardware accelerator card.

```
CES> show status statistics hardware hw-accel-stats
Date 01/29/2004  Time 21:03:43

Bulk Accelerator0:
Hw Accelerator Unit 0 counters
 Current encode sessions :  2

 Total encode packets    :  95294
  good encode pkts       :  95294
  expanded encode pkts   :  0

 Raw encode bytes        :  12892296
 Processed encode bytes  :  12892296
  good encode bytes      :  12892296
```

```
  expanded encode bytes  :  0

 Current decode sessions :  2

 Total decode packets    :  74206
  good decode pkts       :  74206

 Raw decode bytes        :  10163466
 Processed decode bytes  :  10163466
  good decode bytes      :  10163466
  corrupt decode bytes   :  0

 Probe faults:
  security level invalid :  0
CES>
```

The following example shows the statistics displayed for the hardware PACE drivers.

```
CES> show status statistics hardware pace-drivers
Date:  08/16/2003  Time: 10:30:16
Device Mask: 0x0
Device: 0
priority: 3
txLimit: 16
txCredits: 16
txFillCounter: 0
rxLimit: 1000
Device: 1
priority: 1
txLimit: 5
txCredits: 3
txFillCounter: 0
rxLimit: 16

Device: 2
priority: 1
txLimit: 5
txCredits: 5
txFillCounter: 0
rxLimit: 16
CES>
```

show status statistics interfaces

Use this command to display interface status statistics.

Syntax

```
show status statistics interfaces {interfaces | lan-counters
| wan-status}
```

Parameters

interfaces	Displays interface characteristics, including IP and broadcast addresses, subnet masks, Ethernet address, MTU size, packets in and out, multicast packets in and out, and input and output errors.
lan-counters	Displays Ethernet and IP statistics, including transmit and receive counters, summary information, and detailed line utilization information.
wan-status	Displays the WAN state variables, configuration values, frame counters, signal values, and the following values: • Routing filter drops: Packets filtered because no access rights are permitted to the resources specified by the designated filters. • Local system filter drops: Packets destined for the management interface that are dropped due to lack of authorization access. • Local interface filter drops: Packets destined for a physical interface are dropped due to lack of authorization access. • PAT drops: Public Address Table (PAT) drops are the number of packets dropped before being authenticated. • IP header error drops: Packets with an error in the IP header.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

show status statistics admin
show status statistics hardware
show status statistics network
show status statistics resources
show status statistics routing
show status statistics security
show status statistics system

Example

The following example shows the first portion of the statistics displayed for interfaces.

```
CES> show status statistics interfaces interfaces
Date:  08/16/2003  Time: 10:20:52
lo (unit number 0):
      Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
      ifp: 0x1992308, trusted: 1, devLoc: 0x0, devType: 6,
      devSubType: 0
                     dlCtxtPtr: 0x0, circuitMapping: 0x0
      Internet address: 127.0.0.1
   .
   .
   .
CES>
```

The following example shows the first portion of the statistics displayed for the interface LAN counters.

```
CES> show status statistics interfaces lan-counters
Date:  08/16/2003  Time: 10:23:57

LAN Device fei0:

TX good frames:                              178389
TX MAXCOL errors:                                 0
TX LATECOL errors:                                0
TX underrun errors:                               0
TX lost CRS errors:                               0
TX deferred:                                      0
.
.
.
CES>
```

The following example shows the first portion of the statistics displayed for the WAN interfaces.

```
CES> show status statistics interfaces wan-status
Date:  08/16/2003  Time: 10:26:43
  HSSI Slot 2   Link: Down  State: Enabled
  Device HSSI0 PPP down
  In:         0
  Out:        0
  In Errors:  0
  Out Errors: 0
  WANic 700 System Information:
      command result 0x00010007
      HW info        0x00000102
      FW rev         0x00040300
      POST result    0x00000000
      mode           0x52554e54
.
.
.
CES>
```

show status statistics network

Use this command to display network statistics.

Syntax

show status statistics network {**icmp-stats** | **ip-addr-pool** | **ip-fwd-table** | **ip-stats** | **ipx-route-table** | **ipx-server-table** | **ipx-stats** | **sockets** | **tcp-stats** | **udp-stats**}

Parameters

icmp-stats	Displays system-wide ICMP statistics.
ip-addr-pool	Displays the IP addresses listed in the internal address pool, including the total number and the number of addresses allocated.
ip-fwd-table	Displays the contents of the IP forwarding table.
ip-stats	Displays system-wide IP statistics, including total packets, frames too short and too small, bad header lengths, inbound and outbound fragments, fragments dropped and timed out, packets forwarded, redirects, and reassembled.
ipx-route-table	Displays the IPX routing table.
ipx-server-table	Displays the IPX server table.
ipx-stats	Displays system-wide IPX statistics.
sockets	Displays socket or port numbers to which the TCP/IP and UDP protocols are bound.
tcp-stats	Displays system-wide TCP statistics.
udp-stats	Displays system-wide UDP statistics.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

show status statistics admin
show status statistics hardware
show status statistics interfaces
show status statistics resources
show status statistics routing
show status statistics security
show status statistics system

Example

The following example shows the statistics displayed for ICMP.

```
CES> show status statistics network icmp-stats
Date:  08/16/2003  Time: 11:00:40
ICMP:
  8 calls to icmp_error
  0 error not generated because old message was icmp
  Output histogram:
          echo reply: 24
          destination unreachable: 8
  0 message with bad code fields
  0 message < minimum length
  0 bad checksum
  0 message with bad length
  Input histogram:
          destination unreachable: 8
          echo: 24
          time exceeded: 3
  24 message responses generated
CES>
```

The following example shows the statistics displayed for IP address pools.

```
CES> show status statistics network ip-addr-pool
Date:  08/16/2003  Time: 11:04:25
Address Pool(s):
 10.10.2.1 - 10.10.2.8, Name: Default, Size: 8, Allocated: 0
 Available List:
   10.10.2.1 - 10.10.2.8, Range: 8
 Freed/Blackout List:
```

The following example shows the statistics displayed for the IP forwarding table.

```
CES> show status statistics network ip-fwd-table
Date:  08/16/2003  Time: 11:02:34
IP ROUTE NET TABLE
Destination/Mask    Gateway       Flags   Ref Use Intf    MTU OuterCtxt CircMap
RtEntryP
-------------------------------------------------------------------------------
0.0.0.0/0          10.0.0.10         803    4  7788 fei0  1500 72d7cc8  7450f10
6a3b4e4
6.1.0.0/16         10.0.182.12     300003    0     0 fei0  1500 72d7cc8  7450f10
7026f3c
6.2.0.0/16         10.0.182.12     300003    0     0 fei0  1500 72d7cc8  7450f10
701dd7c
6.3.0.0/16         10.0.182.12     300003    0     0 fei0  1500 72d7cc8  7450f10
6a3aee4
.
.
.
-------------------------------------------------------------------------------
IP ROUTE HOST TABLE
Destination/Mask    Gateway       Flags   Ref Use Intf    MTU  OuterCtxt CircMap
RtEntryP
-------------------------------------------------------------------------------
9.0.0.1/32         10.0.243.13     300007    0     0 fei0  1500 72d7cc8  7450f10
7025f24
.
.
127.0.0.1/32       127.0.0.1       10005    3 45395 lo0   0    0         0
6a3bbe4
-------------------------------------------------------------------------------
IP PUBLIC ADDRESS TABLE
address          refcnt  packetFilterCnt
-------------------------------------------------------------------------------
LINK LEVEL ARP TABLE
Destination        Gateway            Flags  Ref     Use  Intf  MTU OuterCtxt
CircMap  RtEntryP
-------------------------------------------------------------------------------
10.0.0.10          00:80:2d:ca:89:26    10405    1     0 fei0   1500 72d7cc8
7450f10  6a3b3e4
.
.
.
10.0.243.13        00:e0:7b:04:d9:e0    10405    0     0 fei0  1500 72d7cc8
7450f10  6a3b1e4
-------------------------------------------------------------------------------
CES>
```

The following example shows the statistics displayed for IP.

```
CES> show status statistics network ip-stats
Date:  08/16/2003  Time: 11:02:08
                      total 5702957
                     badsum    0
                   tooshort    0
                   toosmall    0
                    badhlen    0
                     badlen    0
                 infragments    0
                 fragdropped    0
                 fragtimeout    0
                     forward    0
                 cantforward    0
                redirectsent    0
             unknownprotocol   64
                   nobuffers    0
                reassembled    0
               outfragments    0
                    noroute 47138
                 badoptions    0
                 badversion    0
              zero src addr    0
               src=dst addr    0
             src addr error    0
            dest addr error    0
           mgmt filterdrops 369695
           intf filterdrops 131559
          route filterdrops    0
                   qosdrops    0
             fw filterdrops    0
              frag overflow    0
CES>
```

The following example shows the statistics displayed for the IPX routing table.

```
CES> show status statistics network ipx-route-table
  Date:  08/16/2003  Time: 11:06:10
      IPX is disabled.
CES>
```

The following example shows the statistics displayed for the IPX server table.

```
CES> show status statistics network ipx-server-table
  Date:  08/16/2003  Time: 11:06:32
      IPX is disabled.
CES>
```

The following example shows the statistics displayed for IPX.

```
CES> show status statistics network ipx-stats
  Date:  08/16/2003  Time: 11:05:22
      IPX is disabled.
CES>
```

The following example shows the statistics displayed for network sockets and TCP ports.

```
CES> show status statistics network sockets
Date:  08/16/2003  Time: 10:49:22
Active Internet connections (including servers)
PCB      Proto Recv-Q Send-Q  Local Address      Foreign Address    (state)
-------- ----- ------ ------  ------------------ ------------------ -------
6a397dc  TCP     0      0     10.0.15.93.80      192.32.161.136.133  ESTABLISHED
6a3935c  TCP     0      0     10.0.15.93.80      192.32.161.136.133  TIME_WAIT
6a39a5c  TCP     0      0     127.0.0.1.389      127.0.0.1.1024      ESTABLISHED
7170a24  TCP     0      0     127.0.0.1.1024     127.0.0.1.389       ESTABLISHED
71709a4  TCP     0      0     0.0.0.0.113        0.0.0.0.0           LISTEN
.
.
CES>
```

The following example shows the statistics displayed for TCP.

```
CES> show status statistics network tcp-stats
Date:  08/16/2003  Time: 10:50:11
TCP:
  53775 packets sent
          47856 data packets (7876816 bytes)
          12 data packets (12 bytes) retransmitted
          5587 ack-only packets (4470 delayed)
          0 URG only packet
          0 window probe packet
          3 window update packets
          317 control packets
  51708 packets received
          35178 acks (for 7877953 bytes)
          530 duplicate acks
          0 ack for unsent data
          42419 packets (5105889 bytes) received in-sequence
          0 completely duplicate packet (0 byte)
          0 packet with some dup. data (0 byte duped)
          526 out-of-order packets (0 byte)
          0 packet (0 byte) of data after window
          0 window probe
          118 window update packets
          0 packet received after close
          0 discarded for bad checksum
          0 discarded for bad header offset field
          0 discarded because packet too short
  7 connection requests
  569 connection accepts
  576 connections established (including accepts)
  570 connections closed (including 26 drops)
  0 embryonic connection dropped
  33963 segments updated rtt (of 33964 attempts)
  12 retransmit timeouts
          1 connection dropped by rexmit timeout
  0 persist timeout
  30 keepalive timeouts
          27 keepalive probes sent
          3 connections dropped by keepalive
  0 pcb cache lookup failed
  0 bad syn packet detected
CES>
```

The following example shows the statistics displayed for UDP.

```
CES> show status statistics network udp-stats
Date:  08/16/2003  Time: 10:50:59
UDP:
          1949466 total packets
          1949458 input packets
          8 output packets
          0 incomplete header
          0 bad data length field
          0 bad checksum
          2 broadcasts received with no ports
          0 full socket
          45 pcb cache lookups failed
          8 pcb hash lookups failed
CES>
```

show status statistics resources

Use this command to display statistics for system resources.

Syntax

show status statistics resources {**mbuf-stats** | **memory** | **npbuf-stats** | **slapd** | **stack** | **tasks**}

Parameters

mbuf-stats	Displays memory statistics for forwarding packets.
memory	Displays detailed information about memory allocation, including free and allocated memory; cumulative memory; and average and maximum block sizes.
npbuf-stats	Displays statistics for NP buffers.
slapd	Displays internal LDAP statistics.
stack	Displays stack characteristics and pointers to the tasks, including task name, entry, task ID, and size.
tasks	Displays statistics for jobs that are currently running on the gateway, including task name, task ID, priority, and status.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

show status statistics admin
show status statistics hardware
show status statistics interfaces
show status statistics network
show status statistics routing
show status statistics security
show status statistics system

Example

The following example shows the memory statistics displayed for forwarding packets.

```
CES> show status statistics resources mbuf-stats
Date:  08/16/2003  Time: 10:37:22
      type        number    type        number
      ---------   ------    ---------   ------
      FREE    :    1059      DATA    :     0
      HEADER  :      4       SOCKET  :    23
      PCB     :     35       RTABLE  :   311
      HTABLE  :      0       ATABLE  :     0
      SONAME  :      0       ZOMBIE  :     0
      SOOPTS  :      0       FTABLE  :     0
      RIGHTS  :      0       IFADDR  :     8
      CONTROL :      0       OOBDATA :     0
      IPMOPTS :      0       IPMADDR :     0
      IFMADDR :      0       MRTABLE :     0
      NPBUF   :      0
      TOTAL   :   1440
      number of mbufs: 1440
      number of times failed to find space: 0
      number of times waited for space: 0
      number of times drained protocols for space: 0
      _____________________
      CLUSTER POOL TABLE

_____________________________________________________________________________
      size     clusters  free      maximum    partitionId  usage

-----------------------------------------------------------------------------
      64       680       518       32000      0x0          1899684
      128      80        40        8000       0x0          1964356
      256      670       514       32000      0x0          9167
      512      59        36        8000       0x0          6268
      1024     4         4         2000       0x0          1232
      2048     14        14        1000       0x0          1430

-----------------------------------------------------------------------------
      number of npbufs in pool: 3406
      low       npbufs in pool: 3388
CES>
```

The following example shows a portion of the statistics displayed for system memory resources.

```
CES> show status statistics resources memory
Date:  08/16/2003  Time: 10:33:39
Size Free Total Peak Usage # Bkts Peak New    New     Misses
                                    FBytes   TBytes
16    0     0     0     0     0     0     0          0   0
.
.
.
   Total    64258    175204                  441
      23983704   416
    96636

    Shared Heap Statistics:
     status   bytes    blocks   ave block  max block
     ------ --------- -------- ---------- ----------
    current
       free  54594144       92     593414  45339040
      alloc  48053216      466     103118         -
    cumulative
      alloc  616018208     7493      82212         -
    Heap Statistics:
     status   bytes    blocks   avg block  max block
     ------ --------- -------- ---------- ----------
    current
       free     91680        2      45840     81696
      alloc  102843864       52    1977766         -
    cumulative
      alloc  102843864       52    1977766         -

    Total Free Bytes in Pools + Heap: 78577880
CES>
```

The following example shows the statistics displayed for NP buffers.

```
CES> show status statistics resources npbuf-stats
Date:  08/16/2003  Time: 10:38:26

NP Buffer Pool:
009a8f00=0000000c
Free: 3503
Drivers: 64

NPBUF Extension:
Count: 0  Usage: 0  OverLimit: 0  NoMem: 0  OverSize: 0
CES>
```

The following example shows the statistics displayed for internal LDAP.

```
CES> show status statistics resources slapd
Date:  08/16/2003  Time: 10:40:38
   Slapd is running
   dn: cn=monitor
   version: slapd V3.3 (November 1997)
   threads: 0
   connection: 27 : 010805135719Z : 15485 : 15485 : NULLDN :
   connection: 61 : 010816104038Z : 1 : 0 : NULLDN :
   current connections: 2
   total connections: 2
   dtable size: 8192
   write waiters: 0
   read waiters: 0
   ops initiated: 15486
   ops completed: 15485
   entries sent: 10375
   bytes sent: 3456450
   current time: 010816104038Z
   start time: 010805135709Z
   nbackends: 1
CES>
```

The following example shows a portion of the statistics displayed for stack resources.

```
CES> show status statistics resources stack
Date:  08/16/2003  Time: 10:35:52

        NAME         ENTRY         TID      SIZE   CUR  HIGH  MARGIN
      ------------ ------------ -------- ----- ----- ----- ------
      tExcTask     _excTask     7ed1180   7988   144   608   7380
      tLogTask     _logTask     7ece848   4988   148   204   4784
      tCoredump    0x0000c29200 659b754  10228    60   116  10112
      tCorestart   0x0000c292c4 659e35c  10228    60   116  10112
      tShell       _shell       63fcf0c  29216   800   948  28268
      tCoreblock   0x0000c2928c 6a4993c   4084    68   148   3936
      tWdbTask     0x00016b3c1c 6a5edc4   3976  2308  2544   1432
.
.
.
      tDC          _dcTask(void 65c7c24   7520    60  3432   4088
      tDstMonitor  _DSTMonitor( 65b377c   8084    68   800   7284
      tHwMon       _nocLm78Task 65b5be4   8184    84  1060   7124
      tDbgNew      _DebugNewTas 7efc488  16376    64   348  16028
      tPaceIdle    _PaceIdleTas 6a5397c   4084    48   428   3656
      INTERRUPT                           1000     0     0   1000

CES>
```

The following example shows a portion of the statistics displayed for tasks.

```
CES> show status statistics resources tasks
Date:  08/16/2003  Time: 10:39:12
NAME        ENTRY       TID      PRI   STATUS      PC       SP     ERRNO  DELAY
---------- ------------ -------- --- ---------- -------- -------- ------- -----
tExcTask   _excTask      7ed1180   0 PEND        16dd8a5 7ed10f0       0     0
tLogTask   _logTask      7ece848   0 PEND        16dd8a5 7ece7b4       0     0
tCoredump  c29200        659b754   1 PEND        16505f 659b718        0     0
.
.
.
tPaceIdle  _PaceIdleTas  6a5397c 254 READY        d18eaf 6a5394c       0     0
CES>
```

show status statistics routing

Use this command to display routing statistics.

Syntax

```
show status statistics routing {arp-table | ospf-stats |
rip-stats | vrrp-stats}
```

Parameters

arp-table	Displays link-level ARP information, including the IP address, destination, gateway, and interface.
ospf-stats	Displays OSPF statistics.
rip-stats	Displays RIP statistics.
vrrp-stats	Displays VRRP statistics.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

show status statistics admin
show status statistics hardware
show status statistics interfaces
show status statistics network
show status statistics resources
show status statistics security
show status statistics system

Example

The following example shows the statistics displayed for the ARP table.

```
CES> show status statistics routing arp-table
Date:  08/16/2003  Time: 11:08:20
LINK LEVEL ARP TABLE
Destination        Gateway            Flags  Ref     Use  Intf MTU OuterCtxt
CircMap  RtEntryP
-------------------------------------------------------------------------------
10.0.0.10          00:80:2d:ca:89:26    10405    1     0 fei0 1500 72d7cc8
7450f10  6a3b3e4
10.0.16.221        00:e0:7b:00:0b:c0    10405    0     0 fei0 1500 72d7cc8
7450f10  701d974
10.0.127.183       00:e0:7b:02:d6:40    10405    0     0 fei0 1500 72d7cc8
7450f10  6a3ade4
-------------------------------------------------------------------------------
```

The following example shows the statistics displayed for OSPF.

```
CES> show status statistics routing ospf-stats
  Date:  08/16/2003  Time: 11:10:40
       Ospf has not been initialized
CES>
```

The following example shows the statistics displayed for RIP.

```
CES> show status statistics routing rip-stats
Date:  08/16/2003  Time: 11:08:44

Global Rip Status: Enabled
Update interval is 30 seconds
Trusted Neighbor: Disabled, Rip Domain: 0
Triggered Update: Off, RouteChange: 5961, Query: 132

RIP Input/Output Statistic
---------------------------
Interface       Cid RxUpdates TxUpdates TxTrigUpd RxBadPkts
RxBadRoutes
---------------- --- --------- --------- --------- ---------
-----------
10.0.8.210       1    1928949   32406    931      0
0

CES>
```

The following example shows the statistics displayed for VRRP.

```
CES> show status statistics routing vrrp-stats
Date:  08/16/2003  Time: 11:11:07

Slot Port VRID MstCnt AdvSnt AdvRcv   0Snt   0Rcv Errors
---- ---- ---- ------ ------ ------ ------ ------ ------

CES>
```

show status statistics security

Use this command to display statistics for security.

Syntax

```
show status statistics security
{active-stateful-firewall-policy | flow-cache | nat-stats|
security-stats | stateful-firewall-stats }
```

Parameters

active-stateful-firewall-policy	Displays statistics for stateful firewall policies.
flow-cache	Displays flow cache statistics.
nat-stats	Displays hairpinned packet statistics.
security-stats	Displays security statistics including total and active sessions by tunnel type and quality of service level, authentication failures, dropped sessions.
stateful-firewall-stats	Displays stateful firewall statistics.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

show status statistics admin
show status statistics hardware
show status statistics interfaces
show status statistics network
show status statistics resources
show status statistics routing
show status statistics system

Example

The following example shows the statistics displayed for stateful firewall policies.

```
CES> show status statistics security
active-stateful-firewall-policy
Date:  08/16/2003  Time: 11:20:04
Nortel VPN Router Stateful Firewall not running.
CES>
```

The following example shows the statistics displayed for flow cache:

```
CES> show status statistics security flow-cache
Date:  08/16/2003  Time: 11:19:20
=============================================================
|TCP Connections  |     Conversations  |                |
|Simple Drop      |Simple Complex Drop |Flows   PrFlows |
-------------------------------------------------------------
 0      0          0      0       0     600     100

CES>
```

The following example shows a portion of the security statistics display.

```
CES> show status statistics security security-stats
Date:  08/16/2003  Time: 11:16:29
Security statistics:
                    totalLogons   25
            totalTunneledLogons    0
                   activeLogons    1
           activeTunneledLogons    0
              totalLogons LOCAL   25
             activeLogons LOCAL    1
       totalLogons LOCAL PERSON   25
      activeLogons LOCAL PERSON    1
         totalLogons LOCAL HOST    0
        activeLogons LOCAL HOST    0
.
.
.
CES>
```

The following example shows the statistics for the stateful firewall.

```
CES> show status statistics security stateful-firewall-stats
Date:  08/16/2003  Time: 11:19:46
        Firewall Currently Disabled
CES>
```

show status statistics system

Use this command to display system statistics.

Syntax

show status statistics system {**config-file** | **event-objects** | **file-system** | **flash-contents** | **ntp-stats** | **object-list** | **version**}

Parameters

config-file	Displays the ASCII contents of the configuration file that is currently running on the gateway.
event-objects	Displays the internal software objects that are active.
file-system	Displays statistics for each gateway, including sectors, bytes per sector, sectors per cluster, and reserved sectors.
flash-contents	Displays the contents of nonvolatile memory.
ntp-stats	Displays statistics for the Network Time Protocol (NTP), including the number of packets received, processed, and sent.
object-list	Writes the contents of the object tree to a debug file. This information is for Nortel engineers only.
version	Displays the software version number (for example, V01_05_01.33), the creation date, and the base level (for example, BL029).

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

show status statistics admin
show status statistics hardware
show status statistics interfaces
show status statistics network
show status statistics resources
show status statistics routing
show status statistics security

Example

The following example shows the statistics displayed for the system version.

```
CES> show status statistics system version
   Date:  08/16/2003  Time: 08:51:49
   Version: V04_50.259
      Creation date: Aug 29 2003, 20:51:31
      Base Level: BL259
      Includes debug memory information
      Includes debug packet information
CES>
```

The following example shows the statistics displayed for the file system.

```
CES> show status statistics system file-system
  Date:  08/16/2003  Time: 08:58:20
      vdptr                     0x7495138 122245432
      device name:                /ide0/
      total number of sectors:    4193217
      bytes per sector:           512
      media byte:                 0xf8
      # of sectors per cluster:  64
      # of reserved sectors:     1
      # of FAT tables:           2
      # of sectors per FAT:      256
      max # of root dir entries: 512
      # of hidden sectors:       63
      removable medium:           false
      disk change w/out warning: not enabled
      auto-sync mode:             ENABLED
      long file names:            not enabled
      exportable file system:     not enabled
      lowercase-only filenames:  not enabled
      volume mode:                O_RDWR (read/write)
      available space:            1518108672 bytes
      max avail. contig space:    1518043136 bytes

CES>
```

The following example shows the statistics displayed for the system flash contents.

```
CES> show status statistics system flash-contents
Date:  08/16/2003  Time: 09:15:10
   Flash Header - copyright: Nortel Networks,
   Copyright 1999, 2000
                tag:       NOC
                version:   1
                length:    929
                count:     20
   Flash Data -
   model number: CES2600D
   MAC address: 00-E0-7B-06-11-D0
   serial number: 22951
   feature keys:
       Maximum Ethernet ports: 5
       Maximum T-1 ports: 8
       Maximum T-3 ports: 1
       Allow PPTP tunnels: True
       Allow L2F tunnels: True
       Allow L2TP tunnels: True
       Allow IPsec tunnels: True
       Allow QoS internal: True
       Allow QoS admission: True
       Allow RSVP: True
       Allow RADIUS authentication: True
       Allow LDAP authentication: True
       Allow NT Domain authentication: True
       Allow RSA encryption: True
       Allow SSL: True
       Allow X.509 certificates: True
       Allow RADIUS accounting: True
       CPU clock rate 733 MHz
       CPU cache size 0 KB
       Number of CPUs supported: 1
       Allow IPX: True
       Allow NAT: True
       Allow FW-1: True
       Require FW-1: False
       Firewall: Disabled
       Allow External LDAP authentication: True
       Maximum Hifn 7811 Accelerators: 1
       FIPS Mode: False
```

```
        Allow Safe Mode Boot: False
        SERVER_FARM Mode: False
        Serial Driver Controlled Crash: Disabled
    Flash Revision: 1
    key length: 128
    Boot Device: /ide0/
    maximum concurrent sessions: flash: 1000 runtime: 1000
    system default gateway: 10.0.0.10
    Last shutdown OK: Yes
    system IP netmask: 255.255.0.0
    system IP address: 10.0.15.93
    Boot Mode: Normal
       primary backup host: :
       host username:
       checksum: 62411

CES>
```

The following example shows the statistics displayed for the Network Time Protocol (NTP).

```
CES> show status statistics system ntp-stats
  Date:  08/16/2003  Time: 09:19:10
  NTP is disabled

  NTP packet:

  Packet received:    0
  Packet processed:   0
  Packet sent:        0
  Packet not sent:    0
  Packet dropped:     0
  Packet ignored:     0
  Bad stratum:        0
  Bad authentication: 0
  Bad length:         0
  Old version:        0
  New version:        0
CES>
```

The following example shows a portion of the statistics displayed for the system configuration file.

```
CES> show status statistics system config-file
Date:  08/16/2003  Time: 09:00:54
    File: /ide0/system/config/CFG00077.DAT
    AddressAcquisition.AcquisitionType=Local
    AddressAcquisition.ReadType=Config
    +AttackTrap[Failed Login]
    +AttackTrap[Firewall]
    +AttackTrap[Security Intrusion]
    +CfgAddresses.Address[cn=any]
    CfgAddresses.Address[cn=any].Key=cn=any
    CfgAddresses.Address[cn=any].Wildcard=255.255.255.255
    +CfgARules.Rule[cn=deny all/in]
    CfgARules.Rule[cn=deny all/in].AckBit=FALSE CES#
.
.
.
CES>
```

The following example shows a portion of the statistics displayed for the event objects.

```
CES> show status statistics system event-objects
  Date:  08/16/2003  Time: 09:27:43
  Minimum Message Priority: 0
  Registered Modules:
    0  Sys [On]
    0  GtpCtxtCls [On]
    0  GtpTask [On]
    0  CircuitRegion [On]
    0  CircuitManager [On]
    0  GTPMsgPkt [On]
    0  Logging [On]
.
.
.
CES>
```

show syslog-host

This command shows the current syslog forwarding hosts that are defined for the gateway.

Syntax

show syslog-host

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

logging

Example

```
CES(config)# show syslog-host
Host           Facility Level    UDP   Port  Status
12.230.111.10  kern     all      514   9999  Enabled
230.111.10.234 local0   all      514   9999  Enabled
            KERN NORMAL 514 Disabled
            KERN NORMAL 514 Disabled
```

show system accelerator

Use this command to display information about the hardware encryption accelerator cards.

Syntax

show system accelerator [<*number*>] [**detail**]

Parameters

number	Specifies the number of the hardware encryption accelerator card. Enter 0 or 1.

Default

Display information about all hardware encryption accelerator cards.

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - None
User Management - None

Warning messages

```
% system accelerator not present
```

Related commands

show system accelerator statistics
system accelerator auto-recovery enable
system accelerator enable

Example

The following example displays status information about both hardware encryption accelerator cards.

```
CES# show system accelerator
System Accelerator configuration
  Device     : 0
    Description: Nortel Networks 7854 Accelerator Rev1
    Slot/port  : 3/1
    Status     : Normal operation
  Device     : 1
    Description: Nortel Networks 7811 Accelerator Rev1
    Slot/port  : 4/1
    Status     : Normal operation
CES#
```

The following example displays status information about hardware encryption accelerator card 1 only.

```
CES# show system accelerator 1
System Accelerator configuration
  Device     : 1
  Description: Nortel Networks 7811 Accelerator Rev1
  Slot/port  : 4/1
  Status     : Normal operation
CES#
```

The following example displays detailed information about both hardware encryption accelerator cards.

```
CES# show system accelerator detail
System Accelerator 0 configuration details
  Description          : Nortel Networks 7854 Accelerator
Rev1
  Slot/port            : 3/1
  Operational Status   : Normal operation
  Administrative Status: Enabled
  Protocols            : IPSEC_ESP
  Algorithms           : DES, 3DES, NULL_CRYPT, LZS, HMAC
MD5,HMAC SHA1
  Crypto Strength      : 3DES
  Boots                : 1
  Uptime               : 15:35:45
  Context Memory Size  : 512 (kbytes)
  Max Sessions         : 2000
System Accelerator 1 configuration details
  Description          : Nortel Networks 7811 Accelerator
Rev1
  Slot/port            : 4/1
  Operational Status   : Normal operation
  Administrative Status: Enabled
  Protocols            : IPSEC_ESP
  Algorithms           : DES, 3DES, NULL_CRYPT, LZS, HMAC
MD5, HMAC SHA1
  Crypto Strength      : 3DES
  Boots                : 1
  Uptime               : 15:36:33
  Context Memory Size  : 512 (kbytes)
  Max Sessions         : 2000
CES#
```

The following example displays detailed information about hardware encryption accelerator card 1.

```
CES# show system accelerator 1 detail
System Accelerator 1 configuration details
  Description          : Nortel Networks 7811 Accelerator
Rev1
  Slot/port            : 4/1
  Operational Status   : Normal operation
  Administrative Status: Enabled
  Protocols            : IPSEC_ESP
  Algorithms           : DES, 3DES, NULL_CRYPT, LZS, HMAC
MD5, HMAC SHA1
  Crypto Strength      : 3DES
  Boots                : 1
  Uptime               : 15:36:33
  Context Memory Size  : 512 (kbytes)
  Max Sessions         : 2000
CES#
```

show system accelerator statistics

Use this command to display hardware accelerator statistics.

Syntax

show system accelerator [<*number*>] **statistics**

Parameters

number	Specifies the number of the hardware encryption accelerator card. Enter 0 or 1.

Default

Display information about all cards.

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - None
User Management - None

Related commands

show system accelerator
system accelerator auto-recovery enable
system accelerator enable

Example

The following example displays statistical information about hardware encryption accelerator cards (only one card is installed).

```
CES>show system accelerator statistics
Date 01/29/2004  Time 21:03:43

Bulk Accelerator0:
Hw Accelerator Unit 0 counters
 Current encode sessions :  2

 Total encode packets    :  95294
  good encode pkts       :  95294
  expanded encode pkts   :  0

 Raw encode bytes        :  12892296
 Processed encode bytes  :  12892296
  good encode bytes      :  12892296
  expanded encode bytes  :  0

 Current decode sessions :  2

 Total decode packets    :  74206
  good decode pkts       :  74206

 Raw decode bytes        :  10163466
 Processed decode bytes  :  10163466
  good decode bytes      :  10163466
  corrupt decode bytes   :  0

 Probe faults:
  security level invalid :  0
CES>
```

split-dns enable

This command enables split DNS on the gateway. Enable split DNS when the DNS proxy on the gateway sends DNS queries to both a private and a public DNS server. Use the **no** form of this command to disable split DNS.

Syntax

```
split-dns enable
no split-dns enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

dns-proxy
ip name-server
show ip name-server

Example

The following example enables split DNS.

```
CES(config)# split-dns enable
```

The following example disables split DNS.

```
CES(config)# no split-dns enable
```

system accelerator auto-recovery enable

Use this command to enable autorecovery of a hardware encryption accelerator card. Use the **no** form of the command to disable autorecovery on a hardware encryption accelerator card.

Syntax

system accelerator <*number*> **auto-recovery enable**
no system accelerator <*number*> **auto-recovery enable**

Parameters

number	Specifies the number of the hardware encryption accelerator card. Enter 0 or 1.

Default

Enabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show system accelerator
show system accelerator statistics
system accelerator enable

Example

The following example enables autorecovery on hardware encryption accelerator card 1.

```
CES(config)# system accelerator 1 auto-recovery enable
  System accelerator auto-recovery enabled
CES(config)#
```

The following example disables autorecovery on hardware encryption accelerator card 1.

```
CES(config)# no system accelerator 1 auto-recovery enable
  System accelerator auto-recovery disabled
CES(config)#
```

system accelerator enable

Use this command to enable a hardware encryption accelerator card. Use the **no** form of the command to disable a hardware encryption accelerator card.

Syntax

system accelerator <*number*> **enable**
no system accelerator <*number*> **enable**

Parameters

number	Specifies the number of the hardware encryption accelerator card. Enter 0 or 1.

Default

0

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% system accelerator not present
```

Related commands

```
show system accelerator
show system accelerator statistics
system accelerator auto-recovery enable
```

Example

The following example enables hardware encryption accelerator card 0.

```
CES(config)# system accelerator 0 enable
CES(config)#
```

The following example disables hardware encryption accelerator card 0.

```
CES(config)# no system accelerator 0 enable
CES(config)#
```

verify system

Use this command to perform an integrity check on files of the installed software. This integrity check is performed by comparing file checksums.



Note: This command does not check LDAP database files or unsaved configuration files. For information about these files, see the event log or the system log.

Syntax

```
verify system
```

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Example

The following example shows a successful integrity check.

```
CES> verify system
Software integrity check successful.
```

The following example shows an unsuccessful integrity check.

```
CES> verify system
Software integrity check failed. See event log for details.
```

Chapter 12
Service and tunnel configuration commands

This chapter describes service and tunnel configuration commands.

Command	Page
aaa authentication administrator	666
aaa authentication fwua	668
aaa authentication ipsec	669
aaa authentication l2f	671
aaa authentication l2tp	672
aaa authentication pptp	673
cmp	675
crl retrieval	676
demand	677
fips	679
firewall user-authentication	680
ftp-server enable	682
http enable	683
https	684
identification enable	686
ip radius source-interface	687
ipsec authentication	688
ipsec encryption	689
ipsec encryption ike	691
ipsec fail-over	693
ipsec load-balance	694

Command	Page
ipsec nat-traversal	696
ipsec nat-traversal-bo	697
ipsec nat-traversal port	698
l2f authentication	699
l2f nas-uid	701
l2tp authentication	702
l2tp lac-uid	704
pptp authentication	706
radius service	707
radius-accounting private enable	709
radius-accounting public enable	710
radius-client	711
radius-client host	713
radius-client port	714
show firewall user-authentication	715
show (ipsec | l2f | l2tp | pptp)	717
telnet enable	718
tunnel protocol	719

aaa authentication administrator

Use this command to select the auth server types and order to be used when you authenticate administrators dynamically. Use the no form of this command to disable auth server types.

Syntax

aaa authentication administrator [ldap-server | radius]

no aaa authentication administrator [ldap-server | radius]

Parameters

None

Default

Command mode

CES

Next command mode

CES

Required privileges

System Management - Manage
User Management - None

Related commands

Example

The following example enables the dynamic authentication of administrators.

```
CES(config)#aaa authentication administrator
```

The following example disables the dynamic authentication of administrators

```
CES(config)# no aaa authentication administrator
```

aaa authentication fwua

Use this command to change the firewall user authentication configuration by adding or removing authentication servers, or changing their order. Use the **no** form of the command to remove an authentication server from the firewall user authentication configuration.

Syntax

```
aaa authentication fwua {ldap-server [nt | radius] |
radius [ldap-server | nt]}

no aaa authentication fwua {ldap-server | radius}
```

Parameters

ldap-server	Use an external LDAP authentication server.
nt	Use a Windows NT authentication server.
radius	Use a RADIUS authentication server.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

firewall user-authentication
show firewall user-authentication

Example

The following example specifies that the firewall user authentication service will use a RADIUS server for authentication.

```
CES(config)# aaa authentication fwua radius
CES(config)#
```

The following example reverses the order of the authentication servers. The LDAP server will now be queried first.

```
CES(config)# aaa authentication fwua ldap-server radius
CES(config)#
```

The following example removes the RADIUS server from the firewall user authentication configuration.

```
CES(config)# no aaa authentication fwua radius
CES(config)#
```

aaa authentication ipsec

This command specifies which authentication server will be used for the IPsec tunnel. The internal LDAP server is always queried first, then RADIUS and external LDAP, if applicable. The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions.

Syntax

```
aaa authentication ipsec {radius | ldap-server}
no aaa authentication ipsec {radius | ldap-server}
```

Parameters

radius	RADIUS authentication server.
ldap-server	External LDAP authentication server.

Default

Local RADIUS authentication

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ipsec authentication

Example

```
CES(config)# aaa authentication ipsec radius
CES(config)# no aaa authentication ipsec radius
```

aaa authentication l2f

This command specifies which authentication server will be used for the L2F tunnel. The internal LDAP server is always queried first, then RADIUS and external LDAP, if applicable. The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions.

Syntax

```
aaa authentication l2f {radius | ldap-server}
no aaa authentication l2f {radius | ldap-server}
```

Parameters

radius	RADIUS authentication server.
ldap-server	External LDAP authentication server.

Default

Local RADIUS authentication

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

l2f authentication

Example

```
CES(config)# aaa authentication l2f radius
CES(config)# no aaa authentication l2f radius
```

aaa authentication l2tp

This command specifies which authentication server will be used for L2TP tunnel. The internal LDAP server is always queried first, then RADIUS and external LDAP, if applicable. The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions.

Syntax

```
aaa authentication l2tp {radius | ldap-server}
no aaa authentication l2tp {radius | ldap-server}
```

Parameters

radius	RADIUS authentication server.
ldap-server	External LDAP authentication server.

Default

Local RADIUS authentication

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

l2tp authentication

Example

```
CES(config)# aaa authentication l2tp RADIUS
CES(config)# no aaa authentication l2tp RADIUS
```

aaa authentication pptp

This command specifies which authentication server will be used for the PPTP tunnel. The internal LDAP server is always queried first, then RADIUS and external LDAP, if applicable. The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions.

Syntax

```
aaa authentication pptp {radius | ldap-server}
no aaa authentication pptp {radius | ldap-server}
```

Parameters

radius	RADIUS authentication server.
ldap-server	External LDAP authentication server.

Default

Local RADIUS authentication

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

pptp authentication

Example

```
CES(config)# aaa authentication pptp radius
CES(config)# no aaa authentication pptp radius
```

cmp

This command enables or disables the Certificate Management Protocol to the system management IP address through private and public interfaces. Both interfaces can be enabled or disabled at the same time.

Syntax

```
cmp {private | public}
no cmp {private | public}
```

Parameters

private	Private interface.
public	Public interface.

Default

Enabled on the private side
Disabled on the public side

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config)# no cmp public
CES(config)# cmp private
```

crl retrieval

This command enables or disables the retrieval of Certificate Revocation Lists (CRLs) to the system management IP address through private and public interfaces. Both interfaces can be enabled or disabled at the same time.

Syntax

```
crl retrieval {private | public}
no crl retrieval {private | public}
```

Parameters

private	Private interface.
public	Public interface.

Default

crl retrieval private
no crl retrieval public

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config)# no crl retrieval public
CES(config)# crl retrieval private
```

demand

Use this to configure demand services such as as adding, editing, or disabling a demand interface.

Syntax

demand {**enable**| **add** <*demandinterface*> | <*demandinterface*> | <*demandinterface*> **enable**| **delay** <*numseconds*>}

no demand {**enable**| <*demandinterface*> | <*demandinterface*> **enable**}

Parameters

<demandinterface>	Specifies a selection of an interface
<numseconds>	Specify a number of seconds

Default

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

```
show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger
wait
no dial
remote-network
```

Example

```
CES(config)# demand enable
CES(config)# no demand enable
```

fips

This command enables or disables FIPS 140-1 Level 2. FIPS stands for Federal Information Processing Standards, which specify the security requirements that are to be satisfied by a cryptographic module used within a security system protecting unclassified information within computer and telecommunication systems (including voice systems). When you enable FIPS, FTP and Telnet are automatically disabled, and the gateway will reboot. Also, if you disable FIPS, the gateway will reboot.

Syntax

```
fips enable
no fips
```

Parameters

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

```
show health
show services
```

Example

```
CES(config)# fips enable
CES(config)# no fips
```

firewall user-authentication

Use this command to change the firewall user authentication configuration. Use the **no** form of the command to remove welcome text or an authentication server.

Syntax

```
firewall user-authentication {banner <welcome-message> |
ldap-server [radius] | max-sessions <max-sessions> | port
<port-number> | radius [ldap-server]| tg-only-enable |
tg-only-user <user name> | tg-only-password <password> |
tg-only-epassword <password> |}

no firewall user-authentication {banner | ldap-server |
max-sessions | port | radius}
```

Parameters

welcome-message	Specifies the welcome message to be displayed to users. If the string has spaces, enclose it in quotation marks.
ldap-server	Use an external LDAP authentication server.
radius	Use a RADIUS authentication server.
max-sessions	Specifies the maximum number of user authentication sessions.
port-number	Specifies the HTTPS user authentication port. Type an integer from 1024 through 65535 (but not port 1723, which is reserved for PPTP).
tg-only-enable	Enables fwua for TunnelGuard enforcement only.
tg-only-user	Specifies the name of the TunnelGuard user for the fwua for TunnelGuard enforcement only feature.

user name	Specifies the user name for the fwua for TunnelGuard only user.
tg-only-password	Specifies the password for the fwua for TunnelGuard only user.
password	Specifies the password for the fwua for TunnelGuard only user.
tg-only-epassword	Specifies the password for the fwua for TunnelGuard enforcement only user.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Port <port-number> has been reserved for another service.
```

Related commands

aaa authentication fwua
show firewall user-authentication

Example

The following example sets the HTTPS port for firewall user authentication to 8000.

```
CES(config)# firewall user-authentication port 8000
CES(config)#
```

The following example creates a message for client users.

```
CES(config)# firewall user-authentication banner “Please
enter your HTTPS user ID and password.”
CES(config)#
```

The following example deletes the message for client users.

```
CES(config)# no firewall user-authentication banner
CES(config)#
```

ftp-server enable

This command enables or disables FTP to the system management IP address through any private interface that allows you to transfer files between systems over a network.

Syntax

```
ftp-server enable
no ftp-server enable
```

Parameters

None

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ip http server

Example

```
CES(config)# ftp-server enable
CES(config)# no ftp-server enable
```

http enable

Use this command to enable HTTP on the private side of the gateway. Use the **no** form of the command to disable HTTP.

Syntax

```
http enable
no http enable
```

Parameters

None

Default

Enabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

snmp server management

Example

The following example disables HTTP on the gateway and then reenables it.

```
CES(config)# no http enable
CES(config)# http enable
```

https

Use this command to enable secure HTTP (HTTPS) on the private or public interfaces of the gateway. Use the **no** form of the command to disable HTTPS on the private or public interface.

Syntax

```
https {private | public}
no https {private | public}
```

Parameters

private	Enable or disable HTTPS on private interfaces.
public	Enable or disable HTTPS on public interfaces.

Default

Enabled on the private side
Disabled on the public side

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

The following example enables HTTPS on the public interface and disables it on the private interface.

```
CES(config)# https public
CES(config)# no https private
CES(config)#
```

identification enable

Use this command to enable the identification protocol (RFC 1413) on the private side of the gateway. Use the **no** form of the command to disable the identification protocol.

Syntax

```
identification enable
no identification enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

dns-proxy

Example

The following example enables RFC 1413 on the gateway.

```
CES(config)# identification enable
CES(config)#
```

ip radius source-interface

This command enables or disables access that allows RADIUS requests on the public and private interfaces of the gateway.

Syntax

```
ip radius source-interface {public | private}
no ip radius source-interface {public | private}
```

Parameters

public	Public interface.
private	Private interface.

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config)# ip radius source-interface public
```

ipsec authentication

This command specifies authentication methods for the IPsec tunnel. If the methods are disabled, you cannot configure these in the group mode.

Syntax

```
ipsec authentication {local {rsa-sig | username-password} |
radius {username-password}}

no ipsec authentication {local {rsa-sig | username-password}
| radius { dynamic-securid | username-password}}
```

Parameters

rsa-sig	Rivest-Shamir-Adleman Signature.
dynamic-securid	RADIUS Security Dynamic SecurID token.
username-password	User name and password.
local	LDAP authentication.
radius	RADIUS authentication.

Default

Enabled all

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

pptp authentication
l2f authentication
l2tp authentication

Example

```
CES(config)# ipsec authentication local rsa-sig
CES(config)# no ipsec authentication local pre-share
CES(config)# ipsec authentication radius username-password
```

ipsec encryption

This command enables or disables encryption algorithms for IPsec tunneling.

Syntax

```
ipsec encryption {3des-md5 | 3des-sha1 | aes128-sha1 |
aes256-sha1 | des40-md5 | des40-sha1 | des56-md5 |
des56-sha1 | hmac-md5 | hmac-sha1 | md5 | sha1}

no ipsec encryption {3des-md5 | 3des-sha1 | aes128-sha1 |
aes256-sha1 | des40-md5 | des40-sha1 | des56-md5 |
des56-sha1 | hmac-md5 | hmac-sha1 | md5 | sha1}
```

Parameters

3des-md5	Triple DES with MD5 integrity.
3des-sha1	Triple DES with SHA1 integrity.
aes128-sha1	ESP-AES 128-bit with SHA1 integrity.
aes256-sha1	ESP-AES 256-bit with SHA1 integrity.
des40-md5	40-bit DES with MD5 integrity.
des40-sha1	40-bit DES with SHA1 integrity.
des56-md5	56-bit DES with MD5 integrity.
des56-sha1	56-bit DES with SHA1 integrity.
hmac-md5	Hashing Message Authentication Code Message Digest 5.
hmac-sha1	Hashing Message Authentication Code Secure Hash Algorithm.
md5	Authentication only with MD5 integrity.
sha1	Authentication only with SHA1 integrity.

Default

Enabled - ipsec encryption 3des-md5
Enabled - ipsec encryption des56-md5
Enabled - ipsec encryption hmac-md5
Enabled - ipsec encryption hmac-sha1
Disabled - no ipsec encryption 3des-sha1
Disabled - no ipsec encryption aes128-sha1
Disabled - no ipsec encryption aes256-sha1
Disabled - no ipsec encryption des40-md5

Disabled - no ipsec encryption des40-sha1
Disabled - no ipsec encryption des56-sha1
Disabled - no ipsec encryption md5
Disabled - no ipsec encryption sha1

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ipsec encryption ike

Example

```
CES(config)# ipsec encryption aes128-sha1
```

ipsec encryption ike

This command specifies IKE encryption and Diffie-Hellman group for IPsec tunneling.

Syntax

```
ipsec encryption ike {128aes-group2 | 128aes-group5 |
128aes-group8 | 256aes-group5 | 256aes-group8 | 3des-group2
| 3des-group7 | des56-group1}

no ipsec encryption ike {128aes-group2 | 128aes-group5 |
128aes-group8 | 256aes-group5 | 256aes-group8 | 3des-group2
| 3des-group7 | des56-group1}
```

Parameters

128aes-group2	AES 128 with Group 2 (1024-bit prime).
128aes-group5	AES 128 with Group 5 (1536-bit prime).
128aes-group8	AES 128 with Group 8 (ECC 283-bit field).
256aes-group5	AES 256 with Group 5 (1536-bit prime).
256aes-group8	AES 256 with Group 8 (ECC 283-bit field).
3des-group2	Triple DES with Group 2 (1024-bit prime).
3des-group7	Triple DES with Group 7 (ECC 163-bit field).
des56-group1	56-bit DES with Group 1 (768-bit prime).

Default

All are enabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ipsec encryption

Example

```
CES(config)# ipsec encryption ike 128aes-group5
```

ipsec fail-over

This command specifies fail-over of the selected gateway. A fail-over condition will be detected in approximately two minutes. If a connection is somehow terminated or lost, the client then attempts to connect to the first-listed fail-over gateway. It will try each gateway in succession and if no connection is established, it stops. The no option of the command disables fail-over of the gateway. This command is only available for the gateway.

Syntax

```
ipsec fail-over {<host1> | <host2> | <host3>} <ip-address>
[disable | enabled]
no ipsec fail-over {<host1> | <host2> | <host3>}
```

Parameters

host1, host2, host3	Fail-over gateway.
ip-address	Public IP address of the gateway.
enabled	Enable IPsec fail-over.
disabled	Disabled IPsec fail-over.

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ipsec load-balance

Example

```
CES(config)# ipsec fail-over host1 132.21.21.1
CES(config)# no ipsec fail-over host1
```

ipsec load-balance

This command enables the load balancing of one gateway with an alternate gateway. Load balancing is a protocol between two gateways that exchanges information about the number of sessions of each connection priority and the CPU utilization. The no option of the command disables the load balancing mechanism.

Syntax

```
ipsec load-balance <ip-address> [enabled | disabled]
no ipsec load-balance
```

Parameters

ip-address	Private management IP address of the gateway that you want to serve as the alternate gateway for load balancing.
enabled	Enable load-balance.
disabled	Disable load-balance.

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The gateway and the alternate gateway must be in the same location (that is, they must be in communication via the private interface).

Related commands

ipsec fail-over

Example

```
CES(config)# ipsec load-balance 132.21.21.1
CES(config)# no ipsec load-balance
```

ipsec nat-traversal

This command enables/disables the NAT traversal feature for IPsec tunnel.

Syntax

ipsec nat-traversal
no ipsec nat-traversal

Parameters

None

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

You cannot enable IPsec NAT traversal if you do not specify the port.

Related commands

ipsec nat-traversal port

Example

```
CES(config)# ipsec nat-traversal port 1078
CES(config)# ipsec nat-traversal
```

ipsec nat-traversal-bo

This command enables or disables IPsec NAT Traversal for branch office tunnels. Use the no form of the command to disable NAT traversal.

Syntax

```
ipsec nat-traversal-bo
no ipsec nat-traversal-bo
```

Parameters

None

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage

User Management – None

Prerequisites

None

Example

```
CES(config)#ipsec nat-traversal-bo
```

ipsec nat-traversal port

This command specifies the port number for UDP encapsulation.

Syntax

ipsec nat-traversal port <*port-number*>

Parameters

port-number	UDP port (range 1025-49151).

Default

0

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ipsec nat-traversal

Example

```
CES(config)# ipsec nat-traversal port 10457
CES(config)# ipsec nat-traversal
```

l2f authentication

This command specifies authentication methods for the L2F tunnel. This command is specific to the Nortel VPN Router.

Syntax

```
l2f authentication {pap | chap}
no l2f authentication l2f {pap | chap}
```

Parameters

pap	Password Authentication Protocol.
chap	Challenge Handshake Authentication Protocol.

Default

Enabled all

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

l2tp authentication
pptp authentication
ipsec authentication

Example

```
CES(config)# l2f authentication chap
CES(config)# l2f authentication pap
CES(config)# no l2f authentication pap
```

l2f nas-uid

Use this command to specify the L2F network access server (NAS) user ID and password that allow you to authenticate to the NAS. Use the **no** form of the command to delete the L2F NAS user ID.

Syntax

l2f nas-uid [**add**] <*user-id*> **password** <*password*> **switch-uid** <*switch-id*> **password** <*password*>

no l2f nas-uid <*user-id*>

Parameters

add	Create the NAS user ID. If you do not use this parameter, the NAS user ID must already exist.
user-id	Specifies the NAS user ID (this ID must be coordinated between you and the NAS provider).
password	Specify a password.
password	Specifies a password for the L2F user ID. This password must be coordinated between you and the NAS provider.
switch-uid	Specify the gateway ID.
switch-id	Specifies the gateway ID (this ID must be coordinated between you and the NAS provider).

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

l2tp lac-uid

Example

```
CES(config)# l2f nas-uid add home password my_home switch-id
123433 password my_home
CES(config)# no l2f nas-uid home
```

l2tp authentication

This command specifies authentication methods for the L2TP tunnel. This command is specific for the gateway.

Syntax

l2tp authentication {**pap** | **chap** | **ms-chap** {**version** {**1** | **2**} | **encryption** {**none** | **rc4-40** | **rc4-128**}}
no l2tp authentication {**pap** | **chap** | **ms-chap** {**version** {**1** | **2**} | **encryption** {**none** | **rc4-40** | **rc4-128**}

Parameters

version	Version keyword.
1	Version 1 of MS-CHAP.
2	Version 2 of MS-CHAP.
encryption	Encryption keyword.
none	Tunnels requesting no data encryption.
rc4-40	Tunnels requesting 40-bit RC4 encryption are accepted.
rc4-128	Tunnels requesting 128-bit RC4 encryption are accepted.
pap	Password Authentication Protocol.
chap	Challenge Handshake Authentication Protocol.
ms-chap	MS Challenge Handshake Authentication Protocol.

Default

Enabled all

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ipsec authentication
pptp authentication
l2f authentication

Example

```
CES(config)# l2tp authentication ms-chap version 1
CES(config)# l2tp authentication chap
CES(config)# no l2tp authentication pap
CES(config)# no l2tp authentication ms-chap encryption
rc4-40
CES(config)# l2tp authentication ms-chap version 2
```

l2tp lac-uid

Use this command to specify the L2TP access concentrator (LAC) that allows you to configure the authentication between the gateway and the LAC. Use the **no** form of the command to delete the L2TP LAC.

Syntax

l2tp lac-uid [**add**] <*user-id*> **switch-uid** <*switch-id*> **password** <*password*>

no l2tp lac-uid <*user-id*>

Parameters

add	Create the LAC user ID. If you do not use this parameter, the LAC user ID must already exist.
user-id	Specifies the LAC user ID (this ID must be coordinated between you and the LAC provider).
switch-uid	Specify the gateway ID.
switch-id	Specifies the gateway ID (this ID must be coordinated between you and the LAC provider).
password	Specify a password for the gateway.
password	Specifies a password for the gateway user ID. This password must be coordinated between you and the LAC provider.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

`l2f nas-uid`

Example

```
CES(config)# l2tp lac-uid home switch-uid 123433 password
my_home
CES(config)# no l2tp lac-uid home
```

pptp authentication

This command specifies authentication methods for the PPTP tunnel.

Syntax

```
pptp authentication {pap | chap | ms-chap {version {1 | 2} |
encryption {none | rc4-40 | rc4-128}}
no pptp authentication {pap | chap | ms-chap {version {1 | 2}
| encryption {none | rc4-40 | rc4-128}}
```

Parameters

version	Version keyword.
1	Version 1 of MS-CHAP.
2	Version 2 of MS-CHAP.
encryption	Encryption keyword.
none	Tunnels requesting no data encryption.
rc4-40	Tunnels requesting 40-bit RC4 encryption are accepted.
rc4-128	Tunnels requesting 128-bit RC4 encryption are accepted.
pap	Password Authentication Protocol.
chap	Challenge Handshake Authentication Protocol.
ms-chap	MS Challenge Handshake Authentication Protocol.

Default

Enabled all

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

l2tp authentication
l2f authentication
ipsec authentication

Example

```
CES(config)# pptp authentication ms-chap version 1
CES(config)# pptp authentication chap
CES(config)# no pptp authentication pap
CES(config)# no pptp authentication ms-chap encryption
rc4-40
```

radius service

Use this command to enable the gateway to function as a simple RADIUS server. When you enable this service, the gateway listens on the configured port for authentication requests from remote RADIUS clients. Use the **no** form of the command to disable this feature.

Syntax

```
radius service
no radius service
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

```
ip radius source-interface
radius-client port
```

Example

The following example configures the gateway to act as a simple RADIUS server.

```
CES(config)# radius service
CES(config)#
```

radius-accounting private enable

Use this command to enable RADIUS accounting services on a private interface. Use the **no** form of this command to disable RADIUS accounting services on a private interface.

Syntax

```
radius-accounting private enable
no radius-accounting private enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
radius-accounting public enable
```

Example

The following example enables RADIUS accounting services on private interfaces.

```
CES# configure terminal
CES(config)# radius-accounting private enable
CES(config)#
```

The following example disables RADIUS accounting services on private interfaces.

```
CES(config)# no radius-accounting private enable
CES(config)#
```

radius-accounting public enable

Use this command to enable RADIUS accounting services on a public interface. Use the **no** form of this command to disable RADIUS accounting services on a public interface.

Syntax

```
radius-accounting public enable
no radius-accounting public enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

radius-accounting private enable

Example

The following example enables RADIUS accounting services on public interfaces.

```
CES# configure terminal
CES(config)# radius-accounting public enable
CES(config)#
```

The following example disables RADIUS accounting services on public interfaces.

```
CES(config)# no radius-accounting public enable
CES(config)#
```

radius-client

This command allows the gateway to receive authentication requests from the specified RADIUS client.

Syntax

radius-client {<*hostname*> | <*ip-address*>} {**enabled** | **disabled**}

Parameters

hostname	Name of the RADIUS client.
ip-address	IP address of the RADIUS client.
enabled	Enable RADIUS client.
disabled	Disable RADIUS client.

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-client host

Example

```
CES(config)# radius-client 192.250.2.113 enabled
```

radius-client host

This command specifies a RADIUS client host. These clients are network access devices or RADIUS servers (usually belonging to an ISP), which can initiate or forward (proxy) authentication requests to the gateway.

Syntax

radius-client host {<*hostname*> | <*ip-address*>} **password** <*password*> **no radius-client host** {<*hostname*> | <*ip-address*>}

Parameters

hostname	DNS name of the host.
ip-address	IP address of the host.
password	Specifies that a password is to be used.
password	Password word.

Default

Default client. This is a time-saving feature that enables a Nortel VPN Router administrator to allow all public authentication devices that know the specified secret to send or forward authentication requests to the gateway. Using this feature, the Nortel VPN Router administrator does not have to enter a host name or IP address for each remote device that will be a client for the RADIUS service.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-client

Example

```
CES(config)# radius-client host 192.250.2.113 password
“Hello”
```

radius-client port

This specifies the port number on which the gateway will listen for authentication requests from remote RADIUS clients.

Syntax

radius-client port <*port-number*>

Parameters

port-number	Port number. The range is 0 through 65535.

Default

Port 1645 is the default port number, which is commonly used. However, port 1812 is the port number specified by the RADIUS RFC.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-client

Example

```
CES(config)# radius-client port 1812
```

show firewall user-authentication

Use this command to display information about the configuration of firewall user authentication. This information includes the firewall port, the maximum number of sessions, the authentication order, and so on.

Syntax

show firewall user-authentication

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

aaa authentication fwua
firewall user-authentication

Example

The following example displays the firewall user authentication configuration.

```
CES(config)# show firewall user-authentication
Firewall UA Port:              8000
Firewall UA Max Sessions:      3000
Firewall UA Welcome Banner:

Authentication Order:
 Authentication Server:       Local LDAP
 Authentication Server:       External LDAP
CES(config)#
```

show (ipsec | l2f | l2tp | pptp)

This command displays the tunnel protocol (IPsec, PPTP, L2F, L2TP) configuration for the gateway.

Syntax

```
show {ipsec | l2f | l2tp | pptp}
```

Parameters

ipsec	Show IPsec settings.
l2f	Show L2F settings.
l2tp	Show L2TP settings.
pptp	Show PPTP settings.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – View
User Management – None

Example

```
CES(config)# show l2f
L2F Tunnel Configuration:
   Authentication PAP   : Enabled
   Authentication CHAP  : Enabled
   Authentication Order:
   Authentication Server: Local LDAP
   Authentication Server: Authentication LDAP
   Authentication Server: Radius
   Network Access Servers:
```

telnet enable

This command enables or disables Telnet to the system management IP address through any private interface that allows users on one device to access and manage a remote device. This differs from the de facto standard. Telnet has direct access to the gateway system services and therefore should normally be disabled for security reasons.

Syntax

```
telnet enable
no telnet enable
```

Parameters

None

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config)# telnet enable
CES(config)# no telnet enable
```

tunnel protocol

This command enables or disables the tunneling protocols on private and public interfaces. By default, all tunneling protocols are enabled on the public and private networks. Because data in tunnels is encrypted, this default setting guarantees that all interactions with the gateway are private.

To prevent tunnel connections of a particular type (for all users, including administrators), you can disable the tunnel type using the **no** form of the command. By leaving IPsec, PPTP, L2TP, and L2F enabled on the private side, you can establish tunneled connections to the gateway using any of the tunnel types from within your corporation (private).

Syntax

tunnel protocol {**ipsec** | **pptp** | **l2tp-l2f**} {**private** | **public**}
no tunnel protocol {**ipsec** | **pptp** | **l2tp-l2f**} {**private** | **public**}

Parameters

private	Private interface.
public	Public interface.
ipsec	IPsec tunneling protocol.
pptp	PPTP tunneling protocol.
l2f-l2tp	L2F and L2TP tunneling protocols.

Default

Enable all protocols.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config)# no tunnel protocol pptp public
CES(config)# no tunnel protocol ipsec public
CES(config)# no tunnel protocol l2tp-l2f public
```

Chapter 13
SSL configuration commands

This chapter describes Secure Socket Layer (SSL)/Transport Layer Security (TLS) configuration commands.

Command	Page
reset ssl-vpn	721
restart ssl-vpn	723
show ssl cipher	724
show ssl server-cert	726
show ssl option des-cbc-padding	727
show ssl-vpn	728
ssl cipher	729
ssl https-port	731
ssl option des-cbc-padding enable	733
ssl server-cert	735
ssl-vpn enable	736
ssl-vpn init	737
ssl-vpn csfw-implied-rule enable	739
ssl-vpn paste-config	740
ssl-vpn-cli	742

reset ssl-vpn

This command causes the Nortel VPN Router gateway to perform a reset (AKA resetting to factory defaults) of the Nortel SSL VPN 1000 card.

Syntax

reset ssl-vpn

Parameters

None

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management – Manage
User Management – None

Error Messages

The following error message may be returned:

```
% SSL VPN card not installed
```

Example

Example of resetting SSL VPN card:

```
CES# reset ssl-vpn
%Proceed with SSL-VPN resetting factory defaults? (y/n)yes
%Proceeding with restart...
```

restart ssl-vpn

This command causes the CES to perform a restart (aka reboot) of the SSL VPN card.

Syntax

```
restart ssl-vpn
```

Parameters

None

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management – Manage
User Management – None

Error Messages

The following error message may be returned:

```
% SSL VPN card not installed
```

Example

Example of restarting SSL VPN card:

```
CES#restart ssl-vpn
%Proceed with SSL-VPN restart? (y/n)y
%Proceeding with restart...
```

show ssl cipher

Use this command to display information about the state of the SSL ciphers (enabled or disabled).

Syntax

```
show ssl cipher
```

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ssl cipher

Example

The following example displays the ciphers that are enabled and disabled for SSL.

```
CES(config)# show ssl cipher
  Cipher 1 (DHE_RSA_WITH_3DES_EDE_CBC_SHA, 0x16)      : Enabled
  Cipher 2 (RSA_WITH_3DES_EDE_CBC_SHA, 0x0a)          : Enabled
  Cipher 3 (RSA_WITH_RC4_128_SHA, 0x05)               : Enabled
  Cipher 4 (RSA_WITH_RC4_128_MD5, 0x04)               : Enabled
  Cipher 5 (RSA_EXPORT1024_WITH_RC4_56_SHA, 0x64)     : Enabled
  Cipher 6 (RSA_EXPORT1024_WITH_DES_CBC_SHA, 0x62)    : Enabled
  Cipher 7 (RSA_EXPORT1024_WITH_RC4_56_MD5, 0x60)     : Enabled
  Cipher 8 (DHE_RSA_WITH_DES_CBC_SHA, 0x15)           : Enabled
  Cipher 9 (RSA_WITH_DES_CBC_SHA, 0x09)               : Enabled
  Cipher 10 (DHE_RSA_EXPORT_WITH_DES40_CBC_SHA, 0x14) : Enabled
  Cipher 11 (RSA_EXPORT_WITH_DES40_CBC_SHA, 0x08)     : Enabled
CES(config)#
```

show ssl server-cert

Use this command to display information about the SSL server certificate.

Syntax

show ssl server-cert

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ssl server-cert

Example

```
CES(config)# show ssl server-cert
  Server Certificate                  : None
```

show ssl option des-cbc-padding

Use this command to display the status of SSL DES CBC padding on the gateway, that is, whether SSL DES CBC padding is enabled or disabled.

Syntax

show ssl option des-cbc-padding

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ssl option des-cbc-padding enable

Example

```
CES(config)# show ssl option des-cbc-padding
  DES-CBC padding               : Enabled
```

show ssl-vpn

This command displays the current status and setting of SSL VPN accelerator.

Syntax

show ssl-vpn [detail]

Parameters

detail	This optional parameter causes the display of additional SSL VPN configuration information that may be of help in troubleshooting or checking the health of the setup.

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management – Manage
User Management – None

Error Messages

The following error message may be returned:

```
% SSL VPN card not installed
```

Example

Example of show command.

```
CES#show ssl-vpn
Nortel Networks SSL-VPN Accelerator in slot 1
  Administrative State: Enabled
  Status              : Operational
  CSFW Implied Rules  : Enabled
  One Time Password   : Enabled
  Management Address  : 10.10.10.13
  Interface Address   : 10.10.10.14
  SSL-VPN VIP Ports   : 443
                      : 444
                      : 7777
```

ssl cipher

Use this command to enable a set of cryptographic algorithms (the *cipher*). Each cipher specifies a key exchange mechanism, an authentication method, an encryption algorithm, and a message authority code (hash). Use the **no** form of the command to disallow all or any specific cipher algorithm from SSL TLS usage on the gateway.

Syntax

```
ssl cipher <value>
no ssl cipher <value>
```

Parameters

Specify the SSL TLS cipher algorithm as follows:

all	All SSL TLS ciphers
1	EDH-RSA-DES-CBC3-SHA
10	EXP-EDH-RSA-DES-CBC-SHA
11	EXP-EDH-DSS-DES-CBC-SHA
12	EXP-DES-CBC-SHA
2	DES-CBC3-SHA
3	RC4-SHA
4	RC4-MD5
5	EXP1024-RC4-SHA
6	EXP1024-DES-CBC-SHA
7	EXP1024-RC4-MD5
8	EDH-RSA-DES-CBC-SHA
9	DES-CBC-SHA

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

Services Management - Manage
User Management - None

Related commands

show ssl cipher
ssl option des-cbc-padding enable

Example

The following example configures the gateway to allow all cipher algorithms for SSL TLS.

```
CES(config)# ssl cipher all
CES(config)#
```

The following example configures the gateway not to allow any cipher algorithms for SSL TLS.

```
CES(config)# no ssl cipher all
CES(config)#
```

ssl https-port

Use this command to set the SSL port on a Nortel VPN Router. Use the **no** form of this command to return to the default, 443.

Syntax

ssl htpps-port <*value*>
no ssl htpps-port <*value*>

Parameters

port number

Default

443

Command mode

Global configuration

Next command mode

Global configuration

Required privileges

Services Management – Manage
User Management – None

Related commands

None

Example

```
CES(config)# ssl https-port 1234
```

To reset port to the default:

```
CES(config)# no ssl https-port
```

ssl option des-cbc-padding enable

Use this command to enable SSL DES CBC padding on the gateway. Use the **no** form of the command to disable this option.

Syntax

```
ssl option des-cbc-padding enable
no ssl option des-cbc-padding enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

Services Management - Manage
User Management - None

Related commands

```
show ssl cipher
show ssl option des-cbc-padding enable
ssl cipher
```

Example

The following example enables DES-CBC padding for SSL.

```
CES(config)# ssl option des-cbc-padding enable
CES(config)#
```

The following example disables DES-CBC padding for SSL.

```
CES(config)# no ssl option des-cbc-padding enable
CES(config)#
```

ssl server-cert

Use this command to configure the server certificate. The **no** form of the command disables the server certificate.

Syntax

```
ssl server-cert <certificate>
no ssl server-cert
```

Parameters

certificate	Specifies the server certificate for a gateway acting as an SSL server.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Server certificate does not exist.
```

Related commands

ssl cipher

Example

The following example specifies the SSL server certificate for the gateway.

```
CES# configure terminal
CES(config)# ssl server-cert "CN=kb ces2, OU=Entrust-CA,
O=engeast.nortelnetworks.com"
CES(config)#
```

The following example removes the SSL server certificate.

```
CES(config)# no ssl server-cert
CES(config)#
```

ssl-vpn enable

This command enables the use of the optional SSL VPN accelerator card; the **no** form of the command disables it.

Syntax

[no] ssl-vpn enable

Parameters

None

Default

None

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management – Manage
User Management – None

Error Messages

The following error message may be returned:

```
% SSL VPN card not installed
```

Example

Example of enabling and disabling the use of the optional SSL VPN PCI card.

```
CES(config)# ssl-vpn enable
CES(config)# no ssl-vpn enable
```

ssl-vpn init

This command initializes the SSL VPN Accelerator card to make it manageable.

Syntax

ssl-vpn init management-ip *address* **interface-ip** *address*
{**admin-pwd** | **eadmin-pwd**} *password*

Parameters

management-ip	Specifies the management IP address to be configured on SSL VPN accelerator card
interface-ip	Specifies the interface address to be configured on the SSL VPN accelerator card
admin-pwd	Specifies the administrator password to be configured on the SSL VPN accelerator card
eadmin-pwd	Specifies the encrypted admin password. This is a hidden parameter. It is generated by the **show running-config** command.

Default

None

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management – Manage
User Management – None

Error Messages

The following error message may be returned:

```
% SSL VPN card not installed
```

Example

Example of initializing the optional SSL VPN PCI card:

```
CES(config)# ssl-vpn init management-ip 10.10.10.10
interface-ip 10.10.10.1 admin-pwd setup
```

ssl-vpn csfw-implied-rule enable

This command allows SSL VPN traffic through the Nortel VPN Router Stateful Firewall using an implied rule. The **no** form of the command disables it. Disabling this feature will require the administrator to create override rules in the Nortel VPN Router Stateful Firewall to allow Nortel SSL VPN 1000 traffic.

Syntax

```
[no] ssl-vpn csfw-implied-rule enable
```

Parameters

None

Default

Enabled

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management – Manage
User Management – None

Error Messages

The following error message may be returned:

```
% SSL VPN card not installed
```

Example

Example of enabling the cfsw-implied-rule:

```
CES(config)# ssl-vpn csfw-implied-rule enable
```

ssl-vpn paste-config

This is a hidden command for use with show running-config. The lines following this command must be Nortel SSL VPN 1000 Accelerator commands. All input following this command up to a line with the Nortel SSL VPN 1000 Accelerator command ‘exit’ will be sent to the Nortel SSL VPN 1000 Accelerator. Note that an ‘apply’ command should immediately precede the exit. If the Nortel SSL VPN 1000 Accelerator is not present, all input up to the exit command will be consumed before this command returns.

Syntax

ssl-vpn paste-config

Parameters

None

Default

None

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management – Manage
User Management – None

Error Messages

The following error message may be returned:

```
% SSL VPN card not installed
```

Example

Example of output from show running config:

```
! [Configure SSL VPN accelerator]
    ssl-vpn enable
    ssl-vpn init management 10.10.10.43 interface
10.10.10.44 eadmin 6850175F71
    ssl-vpn paste-config
    /.
    /info/.
    /info/events/.
    /stats/.
```

…additional SSL VPN Accelerator commands…

```
/cfg/sys/adm/https/.
            port 443
            ena false
    /cfg/sys/user/.
            expire 0
    /boot/.
    /boot/software/.
    /maint/.

    apply
    exit
! [Configure SSL VPN accelerator (END)]
!
```

ssl-vpn-cli

This command enters the cli of the Nortel SSL VPN 1000.

Syntax

ssl-vpn-cli [**login** | **reinstall** <*ipaddr*>]

Parameters

login	No automatic admin login is performed. The user is presented with a login prompt and can login to any account on the Nortel SSL VPN 1000 Accelerator.
reinstall <*ipaddr***>**	This parameter is used only if the Nortel SSL VPN 1000 accelerator software is malfunctioning to the point where a reinstall of the card software is necessary. Refer to the Nortel SSL VPN 1000 Accelerator User's Guide for more information. The <ipaddr> parameter is the address to be used by the Nortel SSL VPN 1000 accelerator during the software reinstall process.

Default

Performs an admin login to the Nortel SSL VPN 1000 Accelerator.

Command Mode

Privileged Exec

Next Command Mode

Nortel SSL VPN 1000 Accelerator Card CLI

Required Privileges

System Management – Manage
User Management – None

Error Messages

The following error message may be returned:

```
% SSL VPN card not installed
```

Example

Example of the SSL-VPN-CLI:

```
CES# ssl-vpn-cli

Alteon iSD SSL
Software Version 4.1.1.1

[Main Menu]
      info       - Information menu
      stats      - Statistics menu
      cfg        - Configuration menu
      boot       - Boot menu
      maint      - Maintenance menu
      diff       - Show pending config changes
      apply      - Apply pending config changes
      revert     - Revert pending config changes
      paste      - Restore saved config with key
      help       - Show command help
      exit       - Exit
>>Main# exit
CES#
```

Chapter 14
RADIUS server configuration commands

This chapter describes RADIUS server configuration commands.

Command	Page
aaa accounting network radius	746
aaa accounting session update	747
aaa accounting timeout	748
aaa accounting timeout enable	750
aaa accounting update	751
aaa authorization network radius	752
accounting radius-server	753
accounting radius-server host	754
clear accounting	756
radius-server	757
radius-server authentication	758
radius-server default-group	760
radius-server domain-delimiter	761
radius-server group	762
radius-server group enable	764
radius-server group domain-delimiter	766
radius-server group group-level enable	767
radius-server group maximum-transmit-attempts	769
radius-server group response-timeout-interval	770
radius-server group suffix-remove enable	772
radius-server host	773

Command	Page
radius-server interface	775
radius-server key	776
radius-server retransmit	778
radius-server suffix-remove	779
radius-server suppress-service-type enable	780
radius-server timeout	782
show accounting radius-server	783
show authentication radius-server	784
show radius-server group	786

aaa accounting network radius

Use this command to enable or disable the internal RADIUS accounting server.

Syntax

```
aaa accounting network radius
no aaa accounting network radius
```

Parameters

None

Default

Local RADIUS Accounting Server is enabled.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config)# aaa accounting network radius
CES(config)# no aaa accounting network radius
```

aaa accounting session update

Use this command to specify an interval when a snapshot of the current active tunnel sessions is recorded in a journal file. The journal file stores the session information until the user logs out of the tunnel session, after which the session stop record is saved on the local disk. In the event of a system crash, upon reinitialization the gateway translates the journal file into a series of stop records on a per-session basis. This minimizes accounting data loss. Note that a low interval creates system overhead and requires additional processing.

Syntax

```
aaa accounting session update <interval>
no aaa accounting session update
```

Parameters

interval	Interval in *hh:mm:ss*.

Default

00:30:00 (30 minutes)

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

clear accounting

Example

```
CES(config)# aaa accounting session update 00:30:00
CES(config)# no aaa accounting session update
```

aaa accounting timeout

Use this command to specify the timeout interval for requests to an external RADIUS accounting server.

Syntax

aaa accounting timeout <*seconds*>

Parameters

seconds	Specifies the number of seconds that can elapse before the RADIUS accounting session times out. Enter an integer from 1 through 10.

Default

3 seconds

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

aaa accounting timeout enable

Example

The following example enables the RADIUS accounting timeout and sets the timeout interval to 10 seconds.

```
CES(config)# aaa accounting timeout enable
CES(config)# aaa accounting timeout 10
CES(config)#
```

aaa accounting timeout enable

Use this command to enable the timing out of requests to an external RADIUS accounting server. Use the **no** form of the command to disable the timing out of requests to an external RADIUS accounting server.

Syntax

```
aaa accounting timeout enable
no aaa accounting timeout enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

aaa accounting timeout

Example

The following example enables the timing out of requests to the external RADIUS server, sets the timeout interval to 10 seconds, and then disables the timing out of requests to the external RADIUS server.

```
CES(config)# aaa accounting timeout enable
CES(config)# aaa accounting timeout 10
CES(config)# no aaa accounting timeout enable
CES(config)#
```

aaa accounting update

Use this command to enable periodic interim accounting records at which time interim RADIUS records will be sent to the specified external RADIUS server.

Syntax

aaa accounting update [<*interval*>]
no aaa accounting update

Parameters

interval	Interval in *hh:mm:ss*.

Default

00:30:00 (30 minutes)

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config)# aaa accounting update 00:30:00
CES(config)# no aaa accounting update
```

aaa authorization network radius

Use this command to enable or disable the access to RADIUS authentication server. This command sets parameters that restrict a user's network access.

Syntax

```
aaa authorization network radius
no aaa authorization network radius
```

Parameters

None

Default

Enable

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config)# no aaa authorization network radius
```

accounting radius-server

Use this command to enable or disable an external RADIUS accounting server.

Syntax

```
accounting radius-server {enabled | disabled}
```

Parameters

enabled	Enables the external RADIUS accounting server.
disabled	Disable the external RADIUS accounting server.

Default

Disable

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

accounting radius-server host
radius-server

Example

```
CES(config)# accounting radius-server enabled

CES(config)# accounting radius-server disabled
```

accounting radius-server host

This specifies an external RADIUS accounting server.

Syntax

accounting radius-server host {<*hostname*> | <*ip-address*>}
acct-port <*port-number*> **key** <*secret-word*>

Parameters

hostname	Specifies the DNS name of the RADIUS server host.
ip-address	Specifies the IP address of the RADIUS server host.
acct-port	Specifies the UDP destination port for the accounting requests.
port-number	Specifies the port number for accounting requests.
key	Specifies the key used to set authentication and encryption.
secret-word	Specifies the password for accounting requests.

Default

The default port is 1646.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

`accounting radius-server`

Example

```
CES(config)# accounting radius-server host 192.250.2.113
acct-port 1647 key New
```

clear accounting

Use this command to specify the number of days after which journal files will be removed from the internal RADIUS server.

Syntax

clear accounting <*days*>

Parameters

days	Number of days.

Default

60

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

aaa accounting network radius
aaa accounting session update

Example

```
CES(config)# clear accounting 45
```

radius-server

Use this command to enable or disable a RADIUS server host.

Syntax

radius-server {**primary** | **alternate1** | **alternate2**} {**enabled** | **disabled}**

Parameters

primary	Primary RADIUS server.
alternate1	Alternate1 RADIUS server. This server will process incoming authentication requests if the Primary RADIUS server is unavailable.
alternate2	Alternate2 RADIUS server. This server will process incoming authentication requests if the Primary and Alternate1 RADIUS servers are unavailable.
enabled	Enable server.
disabled	Disable server.

Default

Disable all

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-server host

Example

```
CES(config)# radius-server primary enabled

CES(config)# radius-server primary disabled
```

radius-server authentication

Use this command to enable the authentication types that the RADIUS server supports and uses.

Syntax

```
radius-server authentication {response | pap | chap |
ms-chap version {1 [rfc-2548] | 2}}

no radius-server authentication {challenge | response | pap
| chap | ms-chap version {1 [rfc-2548] | 2}}
```

Parameters

challenge	Challenge/response authentication, for example, PassGo OmniGuard/Defender.
response	Response only authentication, for example Security Dynamics SecurID.
pap	Password Authentication Protocol.
chap	Challenge Handshake Authentication Protocol.
ms-chap version	Microsoft Challenge Handshake Authentication Protocol encrypted authentication Version 1 or Version 2.
rfc-2548	If you enable MS-CHAP Version 1, you can enable RFC 2548 for interoperation with a Microsoft RADIUS server.

Default

Challenge	Disabled
Response	Disabled
MS-CHAP	Disabled
CHAP	Enabled
PAP	Enabled
RFC-2548	Enabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

accounting radius-server timeout

Example

```
CES(config)# radius-server authentication challenge
CES(config)# no radius-server authentication pap
CES(config)# no radius-server authentication ms-chap version
1 rfc-2548
```

radius-server default-group

Use this command to specify the default group from which authorization and operational settings are taken. Any user authorized against a RADIUS server acquires the attributes of this group by default. If the RADIUS server returns a valid group identifier, the gateway will then use this group for the user profile. Otherwise, the gateway will use the default group.

Syntax

radius-server default-group *<group-name>*

Parameters

group-name	Group name.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

% Invalid Group Name.

Example

```
CES(config)# radius-server default-group /Base/SQA
```

radius-server domain-delimiter

Use this command to specify the character that separates the suffix from the UID.

Syntax

radius-server domain-delimiter <*character*>

Parameters

character	Character, for example @.

Default

@

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-server suffix-remove

Example

```
CES(config)# radius-server domain-delimiter #
```

radius-server group

Use this command to specify the IP address, interface, port, and password for a RADIUS server that will communicate with the gateway. Use the **no** form of this command to delete the RADIUS server definition.

Syntax

```
radius-server group <group> {primary | alt1 | alt2}
ip-addr <server-address> interface {private | public
<interface-address>} port <port-number> secret <password>
no radius-server group <group> {primary | alt1 | alt2}
```

Parameters

group	Specifies the group name, for example, /Base/RADIUS/RADIUS11. If the group name includes a space, enclose it in quotation marks, for example, “/Base/New York/Sales”.
server-address	Specifies the IP address of the RADIUS server in dotted-decimal notation.
private	Specifies that the RADIUS server will be reached over the private interface, that is, the Nortel VPN Router management IP address is used.
public	Specifies that the RADIUS server will be reached over a public interface on the gateway.
interface-address	Specifies the IP address of the gateway’s public interface that will communicate with the RADIUS server. Enter the address in dotted-decimal notation.
port-number	Specifies the RADIUS port number. Type a value from 0 through 65535.
password	Specifies the password for the RADIUS server.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

radius-server group enable
radius-server group group-level enable
show radius-server group

Example

The following example configures the primary RADIUS server for the group /Base/New York:

```
CES(config)# radius-server group "/Base/New York" primary
ip-addr 10.10.10.4 interface public 47.17.248.44 port 1812
secret a8z2qlm
CES(config)#
```

The following example deletes the primary RADIUS server from the group:

```
CES(config)# no radius-server group /Base/IT primary
CES(config)#
```

radius-server group enable

Use this command to enable a RADIUS server at group level. Use the **no** form of this command to disable a RADIUS server at group level.

Syntax

radius-server group <*group*> {**primary** | **alt1** | **alt2**} **enable**
no radius-server group <*group*> {**primary** | **alt1** | **alt2**} **enable**

Parameters

group	Specifies the group name, for example, /Base/RADIUS/RADIUS11. If the group name includes a space, enclose it in quotation marks, for example, “/Base/New York/Sales”.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

radius-server group
radius-server group group-level enable
show radius-server group

Example

The following example enables the primary RADIUS server for the group /Base/IT:

```
CES(config)# radius-server group /Base/IT primary enable
```

The following example disables the primary RADIUS server for the group:

```
CES(config)# no radius-server group /Base/IT primary enable
CES(config)#
```

radius-server group domain-delimiter

Use this command to specify the character that will separate the user name portion of a fully qualified user ID from the domain suffix. For example, in the fully qualified UID okcole@acme.com, the “at” character (@) is the domain delimiter. Use the **no** form of this command to remove the domain delimiter.

Syntax

radius-server group <*group*> **domain-delimiter** <*character*>
no radius-server group <*group*> **domain-delimiter**

Parameters

group	Specifies the group name, for example, /Base/RADIUS/RADIUS11. If the group name includes a space, enclose it in quotation marks, for example, “/Base/New York/Sales”.
character	Specifies the delimiter character, for example, @.

Default

The default domain delimiter is the @ character.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

radius-server group
radius-server group suffix-remove
show radius-server group

Example

The following example changes the domain delimiter to the exclamation point (!) for the group /Base/IT:

```
CES(config)# radius-server group /Base/IT domain-delimiter !
CES(config)#
```

radius-server group group-level enable

Use this command to enable a RADIUS server configuration at group level. Use the **no** form of this command to disable the RADIUS server configuration at group level.

Syntax

radius-server group <*group*> **group-level enable**
no radius-server group <*group*> **group-level enable**

Parameters

group	Specifies the group name, for example, /Base/RADIUS/RADIUS11. If the group name includes a space, enclose it in quotation marks, for example, “/Base/New York/Sales”.

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

radius-server group
radius-server group enable
show radius-server group

Example

The following example enables the RADIUS server group-level configuration:

```
CES(config)# radius-server group /Base/IT group-level enable
CES(config)#
```

The following example disables the RADIUS server group-level configuration:

```
CES(config)# no radius-server group /Base/IT group-level
enable
CES(config)#
```

radius-server group maximum-transmit-attempts

Use this command to specify the maximum number of times that the gateway will try to connect to the RADIUS servers. Use the **no** form of this command to revert to the default number of attempts, 3.

Syntax

radius-server group <*group*> **maximum-transmit-attempts** <*attempts*>
no radius-server group <*group*> **maximum-transmit-attempts**

Parameters

group	Specifies the group name, for example, /Base/RADIUS/RADIUS11. If the group name includes a space, enclose it in quotation marks, for example, “/Base/New York/Sales”.
attempts	Specifies the number of attempts that the gateway will make to connect to the RADIUS servers.

Default

3 attempts

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

radius-server group
radius-server group response-timeout-interval
show radius-server group

Example

The following example changes the maximum number of connection attempts for the group /Base/IT to 12.

```
CES(config)# radius-server group /Base/IT
maximum-transmit-attempts 12
CES(config)#
```

radius-server group response-timeout-interval

Use this command to specify the frequency, in seconds, that you want the gateway to wait before trying again to connect to the RADIUS servers. By default, the gateway waits 3 seconds between attempts. The minimum setting is 1 second. Use the **no** form of this command to revert to the default number of seconds, 3.

Syntax

radius-server group <*group*> **response-timeout-interval** <*seconds*>
no radius-server group <*group*> **response-timeout-interval**

Parameters

group	Specifies the group name, for example, /Base/RADIUS/RADIUS11. If the group name includes a space, enclose it in quotation marks, for example, “/Base/New York/Sales”.
seconds	Specifies the number of seconds that the gateway waits between attempts to connect to the RADIUS servers. Type an integer from 1 through 999.

Default

3 seconds

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

radius-server group
radius-server group maximum-transmit-attempts
show radius-server group

Example

The following example changes the number of seconds between attempts to connect to the RADIUS servers to 8.

```
CES(config)# radius-server group /Base/IT
response-timeout-interval 8
CES(config)#
```

radius-server group suffix-remove enable

Use this command to remove the domain delimiter and suffix from the fully qualified user ID before sending it to the RADIUS server. For example, in the fully qualified UID okcole@acme.com, “acme.com” is the suffix. Use the **no** form of this command to restore the suffix in each RADIUS user ID.



Caution: If you use MS-CHAP Version 2 for authentication, do not remove the suffix from the user ID (authentication will fail).

Syntax

```
radius-server group <group> suffix-remove enable
no radius-server group <group> suffix-remove enable
```

Parameters

group	Specifies the group name, for example, /Base/RADIUS/RADIUS11. If the group name includes a space, enclose it in quotation marks, for example, “/Base/New York/Sales”.

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-server group
radius-server group domain-delimiter
show radius-server group

Example

The following example configures the gateway to remove the domain delimiter and suffix from the fully qualified user ID before sending it to the RADIUS server.

```
CES(config)# radius-server group /Base/IT suffix-remove
enable
CES(config)#
```

radius-server host

Use this command to configure a RADIUS server host.

Syntax

radius-server {**primary** | **alternate1** | **alternate2**} **host** {<*hostname*> | <*ip-address*>} **auth-port** <*port-number*>
no radius-server {**primary** | **alternate1** | **alternate2**} **host** {<*hostname*> | <*ip-address*>}

Parameters

primary	Primary RADIUS server.
alternate1	First alternate RADIUS server. This server will process incoming authentication requests if the Primary RADIUS server is unavailable.
alternate2	Second alternate RADIUS server. This server will process incoming authentication requests if the primary and first alternate RADIUS servers are unavailable.
hostname	DNS name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
auth-port	The UDP destination port for the authentication requests.
port-number	Port number for authentication requests.

Default

Default port is 1645.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

aaa authorization network radius

Example

```
CES(config)# radius-server primary host 192.250.2.113
auth-port 1645
```

radius-server interface

Use this command to specify how the gateway's interface (public or private) via RADIUS server will be accessed.

Syntax

radius-server {**primary** | **alternate1** | **alternate2**} **interface** {**private** | **public**}

Parameters

primary	Primary RADIUS server.
alternate1	Alternate1 RADIUS server. This server will process incoming authentication requests if the Primary RADIUS server is unavailable.
alternate2	Alternate2 RADIUS server. This server will process incoming authentication requests if the Primary and Alternate1 RADIUS servers are unavailable.
private	Private interface (management IP address).
public	Public interface.

Default

Private

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-server host

Example

```
CES(config)# radius-server primary interface private
```

radius-server key

Use this command to specify the authentication and encryption key for all RADIUS communications between the gateway and the server when the tunnel connection uses PAP or SecurID. Use the **no** form of this command to remove a RADIUS server key.

Syntax

radius-server {**primary** | **alternate1** | **alternate2**} **key** <*string*>
no radius-server {**primary** | **alternate1** | **alternate2**} **key** <*string*>

Parameters

primary	Primary RADIUS server.
alternate1	Alternate1 RADIUS server. This server will process incoming authentication requests if the Primary RADIUS server is unavailable.
alternate2	Alternate2 RADIUS server. This server will process incoming authentication requests if the Primary and Alternate1 RADIUS servers are unavailable.
key	Sets authentication and encryption.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-server host

Example

```
CES(config)# radius-server primary key Freedom
```

radius-server retransmit

Use this command to specify the number of times that you want the gateway to attempt to connect to the RADIUS servers before failing. Use the **no** form of the command to reset the number of retries to the default value, 3.

Syntax

radius-server retransmit <*retries*>
no radius-server retransmit

Parameters

retries	Specifies the maximum number of retransmission attempts. Type a value from 0 - 5.

Default

3

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-server timeout

Example

The following example resets the number of retries to 5 and then restores the default number of retries (3).

```
CES(config)# radius-server retransmit 5
CES(config)# no radius-server retransmit
```

radius-server suffix-remove

Use this command to remove the domain delimiter and suffix from the fully qualified user ID before sending it to the RADIUS server. You do not need the fully qualified user ID if the DNS server has been properly configured on the gateway. A sample user ID and suffix, where okcole is the UID and acme.com is the suffix, is okcole@acme.com.



Caution: If you use MS-CHAP Version 2 for authentication, do not remove the suffix from the user ID (authentication will fail).

Syntax

```
radius-server suffix-remove
no radius-server suffix-remove
```

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-server domain-delimiter

Example

```
CES(config)# radius-server suffix-remove
```

radius-server suppress-service-type enable

Use this command to remove the service type 8 attribute from the RADIUS access message and allow attributes to be returned to the gateway. (Execute this command to maintain backward compatibility with older versions of Steel-Belted Radius*.) Use the **no** form of this command to disable service type suppression.

Syntax

```
radius-server {primary | alternate1 | alternate2}
suppress-service-type enable
no radius-server {primary | alternate1 | alternate2}
suppress-service-type enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-server host
show authentication radius-server

Example

The following example configures the gateway to remove the service type 8 attribute from the RADIUS access message to allow attributes to be returned to the gateway.

```
CES(config)# radius-server primary suppress-service-type
enable
CES(config)#
```

radius-server timeout

Use this command to specify the number of seconds to wait before trying again to connect to the RADIUS servers. By default, the gateway tries once every 3 seconds. The minimum setting is 1 second. Use the **no** form of the command to revert to the default setting (3 seconds).

Syntax

```
radius-server timeout <seconds>
no radius-server timeout
```

Parameters

seconds	Specifies the number of seconds to wait before retrying to reconnect. You can enter an integer from 1 through 10.

Default

3

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

radius-server retransmit

Example

The following example resets the timeout to 5 seconds and then restores the default number of seconds (3).

```
CES(config)# radius-server timeout 5
CES(config)# no radius-server timeout
```

show accounting radius-server

Use this command to display configuration information about the RADIUS accounting server.

Syntax

show accounting radius server

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

accounting radius-server timeout

Example

```
CES(config)# show accounting radius-server
Radius Accounting Server Properties
  Internal Radius Accounting        : Enabled
  Session Update Interval           : 12:13:12
  Remove Accounting Files in        : 60 Days
  Interim Radius Accounting Record  : Enabled
  Interim Update Interval           : 11:11:11
  External Radius Accounting Server : Enabled
  Host Name                         : 1.1.1.1 Port : 123
  Radius Server Response Timeout    : Enabled
  Response Timeout Interval         : 01:01:01
```

show authentication radius-server

Use this command to display the configuration for the external RADIUS authentication server.

Syntax

show authentication radius-server

Parameters

None

Default

None

Command mode

Global Configuration

Required privileges

System Management – View
User Management – None

Example

```
CES(config)# show authentication radius-server
Radius Authentication Server Properties
  RADIUS Auth. Server access     : Enabled
  Delimiter Value                : @
  Remove Suffix from User ID     : Disabled
  Default Group                  : /Base
  Challenge                      : Disabled
  Response                       : Disabled
  MS-CHAP                        : Enabled
  CHAP                           : Enabled
  PAP                            : Enabled
  RFC_2548                       : Enabled
  Primary host:  Port: 1645 Status: Disabled
  Alternate1  :  Port: 1645 Status: Disabled
  Alternate2  :  Port: 1645 Status: Disabled
  Timeout in sec                 : 3
  Max Attempts                   : 3
CES(config)#
```

show radius-server group

Use this command to display a list of RADIUS servers and their configured attributes.

Syntax

show radius-server group <*group*> {**all** | **primary** | **alt1** | **alt2**}

Parameters

group	Specifies the group name, for example, /Base/RADIUS/RADIUS11. If the group name includes a space, enclose it in quotation marks, for example, “/Base/New York/Sales”.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

radius-server group
radius-server group enable
radius-server group group-level enable

Example

The following example displays all RADIUS server configurations for group /Base/Radius1/Radius11:

```
CES# show radius-server group /Base/Radius1/Radius11 all
  RADIUS Server: Disabled
  Server: Primary
  Hostname or IP address: 47.17.249.176
  Interface: Private
  Interface: 47.17.249.164
  Status: Not configured
  Port: 1812

  RADIUS Server: Enabled
  Server: Alternate 1
  Hostname or IP address: 1.2.3.4
  Interface: Private
  Interface: 47.17.249.164
  Status: Error
  Port: 1646

  RADIUS Server: Disabled
  Server: Alternate 2
  Hostname or IP address: 47.17.249.176
  Interface: Private
  Interface: 47.17.249.164
  Status: Not configured
  Port: 1645
```

The following example displays only the primary RADIUS server configuration for group /Base/Radius1/Radius11:

```
CES# show radius-server group /Base/Radius1/Radius11 primary
  RADIUS Server: Disabled
  Server: Primary
  Hostname or IP address: 47.17.249.176
  Interface: Private
  Interface: 47.17.249.164
  Status: Not configured
  Port: 1812
```

Chapter 15
LDAP server configuration commands

This chapter describes Nortel VPN Router LDAP server and external LDAP server configuration commands.

Command	Page
aaa authentication ldap-server	790
authentication ldap-server base-dn	791
authentication ldap-server contivity-group	793
authentication ldap-server default-group	794
authentication ldap-server digital-certificate	795
authentication ldap-server domain-delimiter	797
authentication ldap-server filter	798
authentication ldap-server host	799
authentication ldap-server ip-address	802
authentication ldap-server ldap-filter	803
authentication ldap-server net-mask	805
authentication ldap-server password	806
authentication ldap-server remove-suffix	808
authentication ldap-server subject-dn	809
authentication ldap-server timeout	811
authentication ldap-server uid	812
authentication ldap-server username-password	814
ldap-server encryptionkey-hex	815
ldap-server encryptionkey-text	817
ldap-server external	818
ldap-server external host	820

Command	Page
ldap-server internal	823
ldap-server source	826
proxy ldap-server server-type	826
proxy ldap-server pwd-timestamp-attr	826
proxy ldap-server pwd-lifetime	826
show authentication ldap-server	832
show ldap-server	834
ssl encryption	836

aaa authentication ldap-server

Use this command to enable the external LDAP authentication server. Use the **no** form of this command to disable the external LDAP authentication server.

Syntax

```
aaa authentication ldap-server
no aaa authentication ldap-server
```

Parameters

None

Default

LDAP authentication server is enabled.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

authentication ldap-server host
show authentication ldap-server

Example

The following example enables and then disables the external LDAP authentication server.

```
CES(config)# aaa authentication ldap-server
CES(config)# no aaa authentication ldap-server
CES(config)#
```

authentication ldap-server base-dn

Use this command to specify the base distinguished name (DN) for the external LDAP server. A base DN is usually in this form:

ou=*organizational unit*, **o=***organization*, **c=***country*

Syntax

authentication ldap-server base-dn <*base-dn-value*>

Parameters

base-dn-value	Specifies the base DN for the external LDAP server. If the value of this parameter contains embedded spaces, enclose the entire string in double quotation marks.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

authentication ldap-server host
show authentication ldap-server

Example

The following example specifies the base DN for the external LDAP server.

```
CES(config)# authentication ldap-server base-dn “o=My
Company, cn=France”
CES(config)#
```

authentication ldap-server contivity-group

Use this command to specify the assigned Nortel VPN Router group for the external LDAP authentication server. Use the **no** form of this command to remove the assigned Nortel VPN Router group.

Syntax

authentication ldap-server contivity-group *<group-name>*
no authentication ldap-server contivity-group

Parameters

group-name	Specifies the Nortel VPN Router group name. Along with the static IP address, IP network mask, and personal filter name, this field can be used as an LDAP search filter.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

authentication ldap-server filter
authentication ldap-server ip-address
authentication ldap-server net-mask
show authentication ldap-server

Example

The following example configures the Nortel VPN Router group for the external LDAP server.

```
CES(config)# authentication ldap-server contivity-group
Paris
CES(config)#
```

authentication ldap-server default-group

Use this command to specify the default group to which users are assigned.

Syntax

authentication ldap-server default-group *<group-name>*

Parameters

group-name	Specifies the group name to which users are assigned.

Default

/Base

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

authentication ldap-server base-dn
show authentication ldap-server

Example

The following example specifies the default group to which users are assigned on the external LDAP server.

```
CES(config)# authentication ldap-server default-group /Base/
Paris
CES(config)#
```

authentication ldap-server digital-certificate

Use this command to enable digital certificate authentication using an external LDAP authentication server. Use the **no** form of this command to disable digital certificate authentication.

Syntax

authentication ldap-server digital-certificate
no authentication ldap-server digital-certificate

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

authentication ldap-server subject-dn
show authentication ldap-server

Example

The following example enables digital certificate authentication on the external LDAP authentication server.

```
CES(config)# authentication ldap-server digital-certificate
CES(config)#
```

authentication ldap-server domain-delimiter

Use this command to specify the character that separates the suffix from the UID in a fully qualified user ID. By default, the domain delimiter is the @ character.

Syntax

authentication ldap-server domain-delimiter <*character*>

Parameters

character	Specifies the delimiter character, for example, @.

Default

@

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

authentication ldap-server remove-suffix
show authentication ldap-server

Example

The following example sets the domain delimiter character for the external LDAP authentication server to the exclamation point (!).

```
CES(config)# authentication ldap-server domain-delimiter !
```

authentication ldap-server filter

Use this command to specify the personal filter for an external LDAP authentication server. Use the **no** form of this command to remove the personal filter.

Syntax

authentication ldap-server filter *<filter-name>*
no authentication ldap-server filter

Parameters

filter-name	Specifies the personal filter name. Along with the Nortel VPN Router group name, IP address, and IP network mask, this field can be used as an LDAP search filter.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

authentication ldap-server contivity-group
authentication ldap-server ip-address
authentication ldap-server net-mask
show authentication ldap-server

Example

The following example specifies the personal filter for the external LDAP authentication server.

```
CES(config)# authentication ldap-server filter myfilter
CES(config)#
```

authentication ldap-server host

Use this command to configure an external LDAP server that can be shared by one or more gateways. Use the **no** form of this command to remove the bind DN from an LDAP server configuration or to remove an entire LDAP server configuration.

Syntax

authentication ldap-server host {<*address*> | <*host_name*>} {**master** | **slave1** | **slave2**} [**bind-dn** <*bind_dn_value*> **bind-password** <*password*>] [{**port** | **ssl-port**} <*port_number*>]
no authentication ldap-server host {**master** | **slave1** | **slave2**} [**bind-dn**]

Parameters

address	Specifies the IP address of the LDAP server.
host_name	Specifies the host name of the LDAP server.
master	Configures this LDAP server as the master LDAP server, that is, the primary server to process queries.
slave1	Configures this LDAP server as the slave 1 LDAP server; this read-only server responds to queries if the master LDAP server is unavailable.
slave2	Configures this LDAP server as the slave 2 LDAP server; this read-only server responds to queries if both the master LDAP server and the slave 1 LDAP server are unavailable.
bind-dn	Specifies the bind distinguished name (DN) that is required to access the base DN and its subentries. (The bind DN is the LDAP equivalent of a user ID.) Do not enter this parameter if your LDAP server allows anonymous access.
bind_dn_value	Specifies the bind DN value.
bind-password	Specifies the password that allows the gateway to prove its identity (the bind DN) to the LDAP server.
password	Specifies the password. You can type up to 32 characters.
port	Sets the port that your LDAP server listens to queries on. Port 389 is the default LDAP port number.
ssl-port	Sets the Secure Socket Layer (SSL) port number that your LDAP server listens to queries on. Port 636 is the default SSL LDAP port number.
port-number	Specifies the port number or SSL port number.

Default

SSL port 636
Port 389

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% External LDAP server not configured.
% Cannot reach external LDAP server.
```

Related commands

authentication ldap-server base-dn
show authentication ldap-server

Example

The following example configures an external LDAP server as the master server and specifies its bind DN and password.

```
CES(config)# authentication ldap-server host 122.33.102.44
master bind-dn cn=Management bind-password myPas4wd
CES(config)#
```

authentication ldap-server ip-address

Use this command to specify the assigned IP address for the external LDAP authentication server. Use the **no** form of this command to remove the IP address.

Syntax

```
authentication ldap-server ip-address <IP_address>
no authentication ldap-server ip-address
```

Parameters

IP_address	Specifies the IP address. Along with the Nortel VPN Router group name, IP network mask, and user filter, this field can be used as an LDAP search filter.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

authentication ldap-server contivity-group
authentication ldap-server filter
authentication ldap-server net-mask
show authentication ldap-server

Example

The following example specifies the assigned IP address and the network mask for the external LDAP authentication server.

```
CES(config)# authentication ldap-server ip-address
123.1.1.45
CES(config)# authentication ldap-server net-mask 255.255.0.0
CES(config)#
```

authentication ldap-server ldap-filter

Use this command to specify the LDAP search filter for username/password authentication. Use the **no** form of this command to remove the LDAP search filter.

Syntax

authentication ldap-server ldap-filter <*filter*>
no authentication ldap-server ldap-filter

Parameters

filter	Specifies the LDAP search filter to be used for username/password authentication.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

authentication ldap-server password
authentication ldap-server uid
authentication ldap-server username-password
show authentication ldap-server

Example

The following example configures user name/password authentication for an external LDAP server and specifies the user name, password, and LDAP filter.

```
CES(config)# authentication ldap-server username-password
CES(config)# authentication ldap-server uid Paris
CES(config)# authentication ldap-server password France
CES(config)# authentication ldap-server ldap-filter
(&(VPNuser=1)(nlogins<30))
CES(config)#
```

authentication ldap-server net-mask

Use this command to specify the assigned IP network mask for the external LDAP authentication server. Use the **no** form of this command to remove the network mask.

Syntax

authentication ldap-server net-mask *<mask>*
no authentication ldap-server net-mask

Parameters

mask	Specifies the network mask. Along with the Nortel VPN Router group name, static IP address, and user filter, this field can be used as an LDAP search filter.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

```
authentication ldap-server contivity-group
authentication ldap-server filter
authentication ldap-server ip-address
show authentication ldap-server
```

Example

The following example specifies the assigned IP address and the network mask for the external LDAP authentication server.

```
CES(config)# authentication ldap-server ip-address
123.1.1.45
CES(config)# authentication ldap-server net-mask 255.255.0.0
CES(config)#
```

authentication ldap-server password

Use this command to set the password for user name/password authentication on the external LDAP authentication server. Use the **no** form of this command to remove the password.

Syntax

```
authentication ldap-server password <password>
no authentication ldap-server password
```

Parameters

password	Specifies the password for user name/password authentication. The password string is not case sensitive.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

authentication ldap-server ldap-filter
authentication ldap-server uid
authentication ldap-server username-password
show authentication ldap-server

Example

The following example configures user name/password authentication for an external LDAP server and specifies the user name, password, and LDAP filter.

```
CES(config)# authentication ldap-server username-password
CES(config)# authentication ldap-server uid Paris
CES(config)# authentication ldap-server password France
CES(config)# authentication ldap-server ldap-filter
(&(VPNuser=1)(nlogins<30))
CES(config)#
```

authentication ldap-server remove-suffix

Use this command to remove the domain delimiter and suffix from the fully qualified user ID before sending it to the LDAP server. For example, in the fully qualified UID okcole@acme.com, “acme.com” is the suffix. Use the **no** form of this command to restore the suffix in each LDAP user ID.



Caution: If you use MS-CHAP Version 2 for authentication, do not remove the suffix from the user ID (authentication will fail).

Syntax

```
authentication ldap-server remove-suffix
no authentication ldap-server remove-suffix
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

authentication ldap-server domain-delimeter
show authentication ldap-server

Example

The following example configures the gateway to remove the domain delimiter and suffix from the fully qualified user ID before sending it to the LDAP server.

```
CES(config)# authentication ldap-server remove-suffix
CES(config)#
```

authentication ldap-server subject-dn

Use this command to specify the subject distinguished name, subject alternative name, and certificate authority for digital certificate authentication.

Syntax

authentication ldap-server subject-dn <*dn-name*>
subject-alt-name <*alt-name*> **ca** <*ca-name*>
[**ldap-filter** <*ldap-filter*>]

Parameters

dn-name	Specifies the subject DN attribute, a case-insensitive character string.
alt-name	Specifies the subject alternative name, a case-insensitive character string.
ca-name	Specifies the certificate authority name.
ldap-filter	Specifies the LDAP search filter used for policy checking.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

authentication ldap-server digital-certificate
show authentication ldap-server

Example

The following example enables digital certificate authentication and sets the appropriate attributes.

```
CES(config)# authentication ldap-server digital-certificate
CES(config)# authentication ldap-server subject-dn Paris
subject-alt-name Versailles ca Entrust ldap-filter
(&(VPNuser=1)(nlogins<30))
CES(config)#
```

authentication ldap-server timeout

Use this command to specify the timeout value in seconds for the external LDAP server. By default, the timeout is set to 4 seconds.

Syntax

authentication ldap-server timeout <*seconds*>

Parameters

seconds	Specifies the number of seconds after which the connection to the external LDAP server times out.

Default

4 seconds

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

show authentication ldap-server

Example

The following example specifies a timeout value of 8 seconds for the external LDAP server.

```
CES(config)# authentication ldap-server timeout 8
CES(config)#
```

authentication ldap-server uid

Use this command to specify the user ID and password for user name/password authentication using the external LDAP authentication server. Use the **no** form of the command to remove the user name.

Syntax

authentication ldap-server uid <*username*> [**password** <*password*>] [**ldap-filter** <*filter*>]
no authentication ldap-server uid

Parameters

username	Specifies the user ID for user name/password authentication. This string is not case sensitive.
password	Specifies a password for the user name.
filter	Specifies the LDAP search filter to be used for username/password authentication.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

authentication ldap-server ldap-filter
authentication ldap-server password
authentication ldap-server username-password
show authentication ldap-server

Example

The following example configures user name/password authentication for an external LDAP server and specifies the user name, password, and LDAP filter.

```
CES(config)# authentication ldap-server username-password
CES(config)# authentication ldap-server uid Paris
CES(config)# authentication ldap-server password France
CES(config)# authentication ldap-server ldap-filter
(&(VPNuser=1)(nlogins<30))
CES(config)#
```

authentication ldap-server username-password

Use this command to enable user name/password authentication using the external LDAP authentication server. Use the **no** form of this command to disable user name/password authentication.

Syntax

```
authentication ldap-server username-password
no authentication ldap-server username-password
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

authentication ldap-server ldap-filter
authentication ldap-server password
authentication ldap-server uid
show authentication ldap-server

Example

The following example configures user name/password authentication for an external LDAP server and specifies the user name, password, and LDAP filter.

```
CES(config)# authentication ldap-server username-password
CES(config)# authentication ldap-server uid Paris
CES(config)# authentication ldap-server password France
CES(config)# authentication ldap-server ldap-filter
(&(VPNuser=1)(nlogins<30))
CES(config)#
```

ldap-server encryptionkey-hex

Use this command to set your own user-defined encryption key instead of the default encryption key that is present on the VPN Router. If you use a user-defined encryption key with an external server, all the VPN Routers that use that external LDAP sever must have the same configured encryption key.

Syntax

ldap-server encryptionkey-hex *<password>*

Parameters

encryptionkey-hex	Configures the LDAP user to a configurable text hash key where the password is an 16-byte hexa decimal value.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ldap-server source encryptionkey-text

Example

The following example sets the LDAP user configurable hex hash key.

```
CES(config)# ldap-server source encryptionkey-hex mypassword
```

ldap-server encryptionkey-text

Use this command to set your own user-defined encryption key instead of the default encryption key that is present on the VPN Router. If you use a user-defined encryption key with an external server, all the VPN Routers that use that external LDAP sever must have the same configured encryption key.

Syntax

ldap-server encryptionkey-text <password**>**

Parameters

encryptionkey-text	Configures the LDAP user to a configurable text hash key where the password is an eight-byte character string.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ldap-server source encryptionkey-hex

Example

The following example sets the LDAP user configurable text hash key.

```
CES(config)# ldap-server source encryptionkey-text
mypassword
```

ldap-server external

Use this command to configure the base DN for an external LDAP server and to change the domain delimiter character (the default is @). You can also use this command to remove the domain delimiter and the suffix from the fully qualified user ID before sending it to the LDAP server. Use the **no** form of the **ldap-server external remove-suffix** command to restore the suffix in the LDAP user ID.



Caution: If you use MS-CHAP Version 2 for authentication, do not remove the suffix from the user ID (authentication will fail).

Syntax

ldap-server external {**base-dn** <*base-dn-value*> | **domain-delimiter** <*character*> | **remove-suffix**}
no ldap-server external remove-suffix

Parameters

base-dn	Specifies the base distinguished name (DN) for the external LDAP server. A base DN usually takes this form: ou=organizational unit, o=organization, c=country. If the base DN string contains embedded spaces, enclose the entire string in double quotation marks.
domain-delimiter	Specifies the character that will separate the user name portion of a fully qualified user ID from the domain suffix. For example, in the fully qualified UID okcole@acme.com, “okcole” is the UID, “acme.com” is the suffix, and the “at” character (@) is the domain delimiter.
remove-suffix	Removes the suffix from the user’s fully qualified user ID before sending it to the LDAP server. For example, in the fully qualified UID okcole@acme.com, “acme.com” is the suffix. **Note**: If you use MS-CHAP V2 for authentication, do not use this parameter; authentication will fail.

Default

The default domain delimiter is the @ character.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ldap-server external host
ldap-server source
show ldap-server

Example

The following example sets the base DN for an external LDAP server.

```
CES(config)# ldap-server external base-dn cn=France
CES(config)#
```

The following example sets the domain delimiter for an external LDAP server to the character "#."

```
CES(config)# ldap-server external domain-delimiter #
CES(config)#
```

ldap-server external host

Use this command to configure an external LDAP server that can be shared by one or more gateways. Use the **no** form of the command to remove an external LDAP server configuration.

Syntax

ldap-server external host {*<address>* | *<host_name>*} {**master** | **slave1** | **slave2**} [**bind-dn** *<bind_dn_value>* **bind-password** *<password>*] [{**port** | **ssl-port**} *<port_number>*]
no ldap-server external host {**master** | **slave1** | **slave2**}

Parameters

address	Specifies the IP address of the external LDAP server.
host_name	Specifies the host name of the external LDAP server.
master	Configures this external LDAP server as the master LDAP server, that is, the primary server to process queries.
slave1	Configures this external LDAP server as the slave 1 LDAP server; this read-only server responds to queries if the master LDAP server is unavailable.
slave2	Configures this external LDAP server as the slave 2 LDAP server; this read-only server responds to queries if both the master LDAP server and the slave 1 LDAP server are unavailable.
bind-dn	Specifies the bind distinguished name (DN) that is required to access the base DN and its subentries. (The bind DN is the LDAP equivalent of a user ID.)
bind_dn_value	Specifies the bind DN value; leave this field blank if your LDAP server allows anonymous access.
bind-password	Specifies the password that allows the gateway to prove its identity (the bind DN) to the LDAP server.
password	Specifies the password. You can type up to 32 characters.
port	Sets the port that your LDAP server listens to queries on. Port 389 is the default LDAP port number.
ssl-port	Sets the Secure Socket Layer (SSL) port number that your LDAP server listens to queries on. Port 636 is the default SSL LDAP port number.
port-number	Specifies the port number or SSL port number.

Default

SSL port 636
Port 389

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% External LDAP server not configured.
% Cannot reach external LDAP server.
```

Related commands

ldap-server external
ldap-server source
show ldap-server

Example

The following example configures an external LDAP server as the master server and specifies its bind DN and password.

```
CES(config)# ldap-server external host 122.33.102.44 master
bind-dn cn=Management bind-password myPas4wd
CES(config)#
```

ldap-server internal

Use this command to start or stop the internal LDAP server, back up the LDAP database, and restore the LDAP database. Backup files are created in the directory /ide0/system/slapd/ldif. To restore the LDAP database, the gateway looks for the appropriate backup file in the same directory.

You can also use this command to change the domain delimiter character (the default is @) or to remove the domain delimiter and suffix from the fully qualified user ID before sending it to the LDAP server. Use the **no** form of the **ldap-server internal remove-suffix** command to restore the suffix in each LDAP user ID.



Caution: If you use MS-CHAP Version 2 for authentication, do not remove the suffix from the user ID (authentication will fail).

Syntax

```
ldap-server internal {domain-delimiter <character> | export
<filename> | import <filename> [autorestart] | remove-suffix
| start | stop}| optimize specific-time {<days of
week>|enable|everday{ time <hh:mm>}
no ldap-server internal remove-suffix
no ldap-server internal optimize specific-time everyday
```

Parameters

domain-delimiter	Specifies the character that will separate the user name portion of a fully qualified user ID from the domain suffix. For example, in the fully qualified UID okcole@acme.com, the “at” character (@) is the domain delimiter.
export	Backs up the contents of the LDAP database to the specified file. The file name can have up to 8 characters. The backup file is created in the directory /ide0/system/slapd/ldif. The LDAP server must be stopped before an export operation can be performed.

import	Restores the contents of the LDAP database from the specified backup file. The backup file must be located in the directory /ide0/system/slapd/ldif. The current LDAP database contents are replaced. The LDAP server must be stopped before an import operation can be performed.
autorestart	Configures the internal LDAP server to restart automatically after the database is backed up or restored.
remove-suffix	Removes the suffix from the user's fully qualified user ID before sending it to the LDAP server. For example, in the fully qualified UID okcole@acme.com, "acme.com" is the suffix. **Note**: If you use MS-CHAP Version 2 for authentication, do not remove the suffix from the user ID.
start	Starts the LDAP server. You can execute this command only when the LDAP server is stopped. You cannot execute this command while the LDAP server is performing an export or import operation.
stop	Stops the LDAP server. You can only execute this command while the LDAP server is running.
stop	Stops the LDAP server. You can only execute this command while the LDAP server is running.
optimize specific-time	Sets the LDAP Optimization Scheduling on specific days of the week.
enable	Enables LDAP Optimization Scheduling everyday at a specific time,
everday	Sets LDAP Optimization Scheduling everyday at a specific time, where *hh:mm* is the hour (00–24) and the minutes of the specific time.
time	Enables LDAP Optimization Scheduling everyday at a specific time, where *hh:mm* is the hour (00–24) and the minutes of the specific time.

Default

The default domain delimiter is the @ character.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% LDAP server is currently running.
% LDAP server is already running.
% LDAP server is already stopped.
% Invalid LDIF file name.
% LDIF file does not exist.
```

Related commands

ldap-server source
show ldap-server

Example

The following example stops the internal LDAP server and backs up the LDAP database to the file “ldap_data_11_11.”

```
CES(config)# ldap-server internal stop
CES(config)# ldap-server internal export ldap_data_11_11
CES(config)#
```

The following example stops the internal LDAP server and restores the LDAP database from the backup file “ldap_data_11_11.” The LDAP database will restart automatically after the import operation is finished.

```
CES(config)# ldap-server internal stop
CES(config)# ldap-server internal import ldap_data_11_11
autorestart
CES(config)#
```

ldap-server source

Use this command to set the source of the LDAP server used by the gateway. The source can be either the internal LDAP server on the gateway itself or an external LDAP server that can be shared by more than one gateway.

Syntax

```
ldap-server source {internal | external}
```

Parameters

internal	Use the internal LDAP server for Nortel VPN Router configuration data.
external	Use an external LDAP server for Nortel VPN Router configuration data.

Default

When initially configured, the gateway uses an internal LDAP server.

Command mode

Global Configuration

Next command mode

Global Configuration

Prerequisites

If you set the source of the LDAP server to external, the LDAP server must already have been configured for use by the gateway.

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% External LDAP server not configured.
% Cannot reach external LDAP server.
```

Related commands

ldap-server external host
ldap-server internal
show ldap-server

Example

The following example sets the source of the LDAP server to external.

```
CES(config)# ldap-server source external
```

ldap-server triple-des enable

Use this command to enable LDAP server triple des.

Syntax

ldap-server triple-des enable

Parameters

None

Default

None

Command mode

Global Configuration/CES

Next command mode

Global Configuration/CES

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

show proxy ldap-server

Example

```
CES(config)# ldap-server server triple-des enable
```

proxy ldap-server server-type

Use this command to authenticate the user through the LDAP proxy.

Syntax

proxy ldap-server server-type

Parameters

None

Default

None

Command mode

Global Configuration/CES

Next command mode

Global Configuration/CES

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

show proxy ldap-server

Example

```
CES(config)# proxy ldap-server server-type server_type
```

proxy ldap-server pwd-timestamp-attr

Use this command to manage password abilities through the CVC Client.

Syntax

proxy ldap-server pwd-timestamp-attr
no proxy ldap-server pwd-timestamp-attr

Parameters

None

Default

None

Command mode

Global Configuration/CES

Next command mode

Global Configuration/CES

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

show proxy ldap-server

Example

```
CES(config)# proxy ldap-server pwd-timestamp-attr attr
CES(config)# no proxy ldap-server pwd-timestamp-attr attr
```

proxy ldap-server pwd-lifetime

Use this command to set the password lifetime in days.

Syntax

proxy ldap-server pwd-lifetime

Parameters

None

Default

None

Command mode

Global Configuration/CES

Next command mode

Global Configuration/CES

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

show proxy ldap-server

Example

```
CES(config)# proxy ldap-server pwd-lifetime life_time
```

show authentication ldap-server

Use this command to display the external authentication LDAP server configuration.

Syntax

show authentication ldap-server

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – View
User Management – None

Related commands

`show ldap-server`

Example

The following example shows the output generated by the command.

```
CES(config)#show authentication ldap-server
LDAP Authentication Server Properties:
  LDAP Authentication Server     : Enabled
  LDAP Digital Certificate       : Disabled
  Delimiter Value                : @
  Remove Suffix from User ID     : Disabled
  Master host:  Port: 389 Bind-dn:  Password: None Status: Not Configured
  Slave1 host:  Port: 389 Bind-dn:  Password: None Status: Not Configured
  Slave2 host:  Port: 389 Bind-dn:  Password: None Status: Not Configured
  Base DN                        :
  Default Group                  : /Base
  Subject DN                     :
  Subject Alternate Name         :
  LDAP Certificate Authority     :
  LDAP Search Filter             :
  Username/Password Access       : Enabled
  Username                       :
  Password                       :
  LDAP Filter                    :
  Contivity Group                : /Base
  Personal Filter               : cn=asdf, ou=Filters, o=My Company, c=US
  IP Address                     : 192.32.25.123
  Netmask                        : 255.255.255.254
  Timeout                        : 4
CES(config)#
```

show ldap-server

Use this command to display the LDAP server configuration.

Syntax

show ldap-server

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – View
User Management – None

Related commands

`show authentication ldap-server`

Example

The following example shows the output generated by the **show ldap-server** command.

```
CES(config)# show ldap-server

General Configuration:
   Delimiter Value: @
   Remove Suffix from User ID: Disabled
   Internal server is running

CES(config)# ldap-server source external

CES(config)# show ldap-server

General Configuration:
   Delimiter Value: None
   Remove Suffix from User ID: Disabled
   External server is running
   External LDAP Servers:
   Base DN: u=My Company
   Master host:  Port: 389 Bind-dn:  Bind Password
   Slave1 host:  Port: 389 Bind-dn:  Bind Password
   Slave2 host:  Port: 389 Bind-dn:  Bind Password
```

ssl encryption

Use this command to set an encryption mode that the gateway will use during negotiation with an external LDAP server. If the external LDAP server does not support one of the selected encryption types, the connection is not established. The encryption type must be set if the connection to an external LDAP server is via SSL. Use the **no** form of the command to remove an SSL encryption mode.

Syntax

```
ssl encryption {des56-sha | rc4-128 | rc4-40}
no ssl encryption {rc4-128 | des56-sha | rc4-40}
```

Parameters

des56-sha	Specifies DES 56-bit encryption with SHA integrity.
rc4-128	Specifies RC4 128-bit encryption with MD5.
rc4-40	Specifies RC4 40-bit encryption with MD5.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Prerequisites

Must have an SSL connection to an external LDAP server.

Required privileges

System Management – Manage
User Management – None

Related commands

ldap-server external host
show ldap-server

Example

The following example specifies that RC4 128-bit and DES 56-bit encryption be used during negotiation with the external LDAP server.

```
CES(config)# ssl encryption rc4-128
CES(config)# ssl encryption des56-sha
CES(config)#
```

Chapter 16
DHCP server configuration commands

This chapter describes DHCP server configuration commands and includes an extended configuration example.

Command	Page
bootfile	840
debug dhcp	841
description	843
excluded-address	844
hardware-address	847
host	848
included-address	850
ip dhcp server pool	851
lease	853
next-server	856
option	857
option client-identifier	860
option default-router	861
option dns-server	863
option domain-name	864
option netbios-name-server	865
option netbios-node-type	867
server-name	868
service dhcp enable	870
service dhcp restart	871

Command	Page
show ip dhcp server	872
DHCP server configuration example	875

bootfile

Use this command to specify the name of the default boot image for the DHCP server. A DHCP server can store the boot files on another host. Use the **no** form of this command to delete the boot image name.

Syntax

```
bootfile <file-name>
no bootfile
```

Parameters

file-name	Specifies the name of the file to be used as a boot image.

Default

None

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip dhcp server pool
next-server

Example

The following example specifies the name of the file to be used as a boot image for the DHCP server on the gateway. To execute the **bootfile** command, you must enter DHCP Pool Configuration mode with a host definition.

```
CES(config)# ip dhcp server pool network 192.33.12.4 host
moloko
CES(config-dhcp)# bootfile dhcpmainbootfile
CES(config-dhcp)#
```

debug dhcp

Use this command to start debug-level logging for DHCP. Use the **no** form of the command to stop the logging of debug messages.

Syntax

debug dhcp
no debug dhcp

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

debug interface

Example

The following example starts debug logging for DHCP.

```
CES# debug dhcp
CES#
```

The following example stops debug logging for DHCP.

```
CES# no debug dhcp
CES#
```

description

Use this command to specify a text description for the interface that you are configuring as a DHCP client. Use the **no** form of this command to delete the description.

The interface text description appears in the result of the ifName MIB.

Syntax

description <*text*>
no description

Parameters

text	Specifies atext description for the DHCP client

Default

None

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip dhcp server pool
option client-identifier

Example

The following example specifies a string to describe a DHCP client. To execute the **description** command, you must enter DHCP Pool Configuration mode with a network definition.

```
CES(config)# ip dhcp server pool network 42.33.12.4 mask /24
CES(config-dhcp)# description “DHCP client interface”
CES(config-dhcp)#
```

excluded-address

Use this command to specify IP addresses that the DHCP server on the gateway should not assign to DHCP clients. Use the **no** form of this command to remove the address or range of addresses from the list of excluded IP addresses.

By default, the DHCP server can assign any address in an address pool to a client. Use this command to exclude a single IP address or a range of IP addresses from the pool of available IP addresses to be assigned to clients.

Syntax

excluded-address <*low-address*> [<*high-address*>]
no excluded-address <*low-address*>

Parameters

low-address	Specifies a single IP address or the first address in a range of IP addresses to be excluded from the pool of available addresses.
high-address	Specifies the last address in the range of excluded IP addresses.

Default

All IP pool addresses are assignable.

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

included-address
ip dhcp server pool

Example

The following example adds IP addresses 47.26.11.100 through 47.26.11.199 to the list of addresses available for assignment to DHCP clients and then excludes addresses 47.26.11.140 through 47.26.11.150 from the DHCP address pool. To execute this command, you must enter DHCP Pool Configuration mode with a network definition.

```
CES(config)# ip dhcp server pool network 47.26.11.0 mask /16
CES(config-dhcp)# included-address 47.26.11.100 47.26.11.199
CES(config-dhcp)# excluded-address 47.26.11.140 47.26.11.150
CES(config-dhcp)#
```

hardware-address

Use this command to specify the hardware address of a DHCP client. This address is valid for manual bindings only. Use the **no** form of this command to remove the hardware address.

Syntax

hardware-address <*mac-address*>
no hardware-address

Parameters

mac-address	Specifies the MAC address of the DHCP client. Enter the MAC address in this format: 00:04:34:D3:40:CC

Default

No hardware address is defined.

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

host
ip dhcp server pool
option client-identifier

Example

The following example specifies the MAC address of the DHCP client santiago. To execute this command, you must enter DHCP Pool Configuration mode with a host definition.

```
CES(config)# ip dhcp server pool network 147.26.246.63 host
santiago
CES(config-dhcp)# hardware-address 02:c7:f8:00:04:22
```

host

Use this command to specify the IP address for a manual binding to a DHCP client. Use the **no** form of this command to remove the client IP address.

Syntax

host <*address*>
no host

Parameters

address	Specifies the IP address assigned to the client.

Default

None

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

hardware-address
ip dhcp server pool
option client-identifier

Example

The following example specifies 10.21.11.14 as the DHCP client's IP address to be used in a manual binding. To execute the **host** command, you must enter DHCP Pool Configuration mode with a host definition.

```
CES(config)# ip dhcp server pool network 147.26.246.63 host
santiago
CES(config-dhcp)# host 10.21.11.14
CES(config-dhcp)#
```

included-address

Use this command to specify IP addresses that the DHCP server on the gateway should include in the pool of addresses to assign to DHCP clients. Use the **no** form of this command to remove IP addresses from the pool of addresses that can be assigned to DHCP clients.

By default, the DHCP server can assign any address in an address pool to a client. To exclude IP addresses from the pool of available IP addresses to be assigned to clients, use the **excluded-address** command.

Syntax

included-address <*low-address*> [<*high-address*>]
no included-address <*low-address*>

Parameters

low-address	Specifies a single IP address or the first address in a range of IP addresses to be included in the pool of available addresses.
high-address	Specifies the last address in the range of included IP addresses.

Default

No address pools are configured.

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

excluded-address
ip dhcp server pool

Example

The following example adds IP addresses 47.26.11.100 through 47.26.11.199 to the list of addresses available for assignment to DHCP clients. To execute this command, you must enter DHCP Pool Configuration mode with a network definition.

```
CES(config)# ip dhcp server pool network 47.26.11.0 mask /16
CES(config-dhcp)# included-address 47.26.11.100 47.26.11.199
CES(config-dhcp)#
```

ip dhcp server pool

Use this command to configure an address pool for the DHCP server on the gateway. You can define address ranges for the entire gateway, for a network address, or for an individual host. Use the **no** form of this command to remove the address pool.

When you execute this command, you enter DHCP Pool Configuration mode (identified by the `CES(config-dhcp)#` prompt). In this mode, you can configure pool parameters, such as the default router list.

Syntax

ip dhcp server pool [**network** *<network-address>* {**mask** *<subnet-mask>* | **host** *<host-name>*}]

no ip dhcp server pool [**network** <*network-address*> [**host** <*host-name*>]]

Parameters

network-address	Specifies the IP address of the network for which you are creating an address pool.
subnet-mask	Specifies the subnet mask of the network for which you are creating an address pool. Enter the mask in dotted-decimal notation or as a bit mask (for example, **mask /24**).
host-name	Specifies the name of a host for which you are creating an address pool.

Default

DHCP address pools are not configured.

Command mode

Global Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

excluded-address
included-address
lease

Example

The following example configures a global DHCP address pool.

```
CES(config)# ip dhcp server pool
CES(config-dhcp)#
```

The following example configures a DHCP address pool for network 192.10.0.0.

```
CES(config)# ip dhcp server pool network 192.10.0.0 mask /16
CES(config-dhcp)#
```

The following example configures a DHCP address pool for host 192.10.10.1.

```
CES(config)# ip dhcp server pool network 192.10.0.0 host
printer
CES(config-dhcp)#
```

lease

Use this command to configure the default and maximum duration of a lease for an IP address that is assigned by the DHCP server to a DHCP client. Use the **no** form of this command to restore the default values: 12 hours for the default lease period and 1 day for the maximum lease period.

Syntax

lease {**default** | **maximum**} {**infinite** | <*days*> [<*hours*> [<*minutes*> [<*seconds*>]]]}
no lease {**default** | **maximum**}

Parameters

default	Specifies the default duration of a lease period if no other lease period is specified.
maximum	Specifies the maximum duration of a lease period if no other lease period is specified.
infinite	Specifies the duration of the lease period as unlimited.
days	Specifies the duration of the lease period in days. Enter a value from 0-999.
hours	Specifies the duration of the lease period in hours. Enter a value from 0-23. To specify the lease period as a number of hours only, set the value for *days* to 0, for example, **lease default 0 12**.
minutes	Specifies the duration of the lease period in minutes. Enter a value from 0-59. To specify the lease period as a number of minutes only, set the value for *days* and *hours* to 0, for example, **lease maximum 0 0 45**.
seconds	Specifies the duration of the lease period in seconds. Enter a value from 0-59. To specify the lease period as a number of seconds only, set the value for *days*, *hours*, and *minutes* to 0, for example, **lease default 0 0 0 45**.

Default

The default lease period is 12 hours; the maximum lease period is 1 day.

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip dhcp server pool

Example

The following example specifies a default lease of 50 minutes and a maximum lease of 12 hours for host maxwell.

```
CES(config)# ip dhcp server pool network 192.168.0.0 host
maxwell
CES(config-dhcp)# lease default 0 0 50
CES(config-dhcp)# lease maximum 0 12
```

The following example specifies an infinite (unlimited) lease for a host printer.

```
CES(config)# ip dhcp server pool network 192.168.0.0 host
printer
CES(config-dhcp)# host 192.168.0.111
CES(config-dhcp)# lease default infinite
```

The following example specifies a maximum lease of 3 days and 12 hours for network 192.168.0.0/16.

```
CES(config)# ip dhcp server pool network 192.168.0.0 mask /16
CES(config-dhcp)# lease maximum 3 12
```

The following example specifies a maximum lease of 2 days and a default lease of 8 hours and 30 minutes for the entire gateway.

```
CES(config)# ip dhcp server pool
CES(config-dhcp)# lease maximum 2
CES(config-dhcp)# lease default 0 8 30
```

next-server

Use this command to configure the next server in a DHCP client's boot process. You can specify up to eight servers. Servers are listed in order of preference: the first address is the most preferred server, the second address is the next most preferred server, and so on. Use the **no** form of this command to remove the boot server list.

If you do not configure a boot server list, the DHCP server uses the boot servers configured for DHCP relay using the **ip-helper-address** command.

Syntax

next-server <*address1*> [<*address2*> ... <*address8*>]
no next-server

Parameters

address	Specifies the IP address of the next server in the boot process, usually an FTP server. You can configure as many as eight servers.

Default

DHCP server uses the boot servers configured for DHCP relay using the **ip-helper-address** command.

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

bootfile
ip dhcp server pool
ip-helper-address
option

Example

The following example specifies 10.21.11.67 as the IP address of the next server in the boot process. To execute the **next-server** command, you must enter DHCP Pool Configuration mode with a host definition.

```
CES(config)# ip dhcp server pool network 147.26.246.63 host
santiago
CES(config-dhcp)# next-server 10.21.11.67
CES(config-dhcp)#
```

option

Use this command to configure DHCP server options on the gateway. Use the **no** form of this command to remove the options.

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are called options. The current set of DHCP options is documented in RFC 2131, “Dynamic Host Configuration Protocol,” and in RFC 2132, “DHCP Options and BOOTP Vendor Extensions.”

Syntax

```
option <code> {ascii <ascii_string> | hex <hex_string> |
integer <integers> | ip <ip_address>}
no option <code>
```

A number of DHCP options are binary: that is, they take a value of 0 or 1. To configure these options on the gateway, enter the ASCII text “true” or “false” instead of the integers 0 and 1. For example, to configure option 30 (mask supplier option), enter **`option 30 ascii false`**. The binary options include options 19, 20, 27, 29, 30, 31, 34, 36, and 39.

Parameters

code	Specifies the DHCP option code. Enter an integer from 1-254 (see RFC 2132 for descriptions of the option codes).
ascii_string	Specifies an ASCII character string. Enclose ASCII strings with embedded spaces in quotation marks.
hex_string	Specifies dotted-hexadecimal data. Each byte in the hex character string is two hexadecimal digits. You can separate bytes using a period, a colon, or a space.
integer	Specifies one or more integers. If you enter more than one integer, use a comma to separate them.
ip_address	Specifies one or more IP addresses in dotted-decimal notation. If you enter more than one address, use a space to separate them.

Default

None

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip dhcp server pool

Example

The following example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. A value of false (0) disables IP forwarding; a value of true (1) enables IP forwarding. IP forwarding is enabled and then disabled in the following example.

```
CES(config-dhcp)# option 19 ascii true
CES(config-dhcp)# option 19 ascii false
```

The following example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 192.134.37.22 and 192.134.37.23 are configured in the following example.

```
CES(config-dhcp)# option 72 ip 192.134.37.22 192.134.37.23
CES(config-dhcp)#
```

option client-identifier

Use this command to specify a unique identifier for a Microsoft DHCP client in dotted-hexadecimal notation. The client identifier is valid for manual bindings only. Use the **no** form of this command to delete the client identifier.

Microsoft DHCP clients require client identifiers instead of hardware addresses. The client identifier is formed by concatenating the code for the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address b3.0436.5678.23 is 01b3.0436.5678.23, where 01 represents the Ethernet media type.

For a list of media type codes, refer to the "Address Resolution Protocol Parameters" section of RFC 1700, "Assigned Numbers."

Syntax

```
option client-identifier <unique-identifier>
no option client-identifier
```

Parameters

unique-identifier	Specifies the unique identifier of the client in dotted-hexadecimal notation. Prefix the hardware address with the two-character code for the media type, for example, 01b3.0436.5678.23; the prefix 01 represents Ethernet.

Default

None

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

hardware-address
host
ip dhcp server pool

Example

The following example configures a host that will always be assigned the same IP address (147.128.0.111) and specifies the Microsoft DHCP client identifier. The MAC address for the host is b3.0436.5678.23; 01 is the code for the Ethernet media type.

```
CES(config)# ip dhcp server pool network 147.128.0.0 host
officepc
CES(config-dhcp)# host 147.128.0.111
CES(config-dhcp)# option client-identifier 01b3.0436.5678.23
```

option default-router

Use this command to specify the default router list for a DHCP client. You can specify up to eight routers. Use the **no** form of this command to remove the default router list.

Enter the IP addresses of the default routers in order of preference: the first address is the most preferred router, the second address is the next most preferred router, and so on. The IP address of a router on the list should be on the same subnet as the client.

Syntax

option default-router <*address1*> [<*address2*> ... <*address8*>]
no option default-router

Parameters

address	Specifies the IP address of a router. You can configure as many as eight routers.

Default

None

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip dhcp server pool

Example

The following example configures a default router list with one router address.

```
CES(config-dhcp)# option default-router 10.21.11.67
```

option dns-server

Use this command to specify the Domain Name System (DNS) servers available to a DHCP client. You can specify up to eight servers. Use the **no** form of this command to remove the server list.

Enter the IP addresses of the servers in order of preference: the first address is the most preferred server, the second address is the next most preferred server, and so on. If you do not configure a list of DNS servers for a DHCP client, the client cannot correlate host names to IP addresses.

Syntax

```
option dns-server <address1> [<address2> ... <address8>]
no option dns-server
```

Parameters

address	Specifies the IP address of a DNS server. You can configure as many as eight servers.

Default

No DNS servers are configured.

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip dhcp server pool
option domain-name

Example

The following example specifies 10.21.11.67 as a DNS server for the DHCP client.

```
CES(config-dhcp)# option dns-server 10.21.11.67
```

option domain-name

Use this command to specify the domain name for a DHCP client. Use the **no** form of this command to remove the domain name.

Syntax

option domain-name <*domain*>
no option domain-name

Parameters

domain	Specifies the client's domain name.

Default

None

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip dhcp server pool
option dns-server

Example

The following example specifies the string “acme.com” as the domain name of the client.

```
CES(config-dhcp)# option domain-name acme.com
```

option netbios-name-server

Use this command to configure a list of NetBIOS Windows* Internet Naming Service (WINS) name servers that are available to Microsoft DHCP clients. You can specify up to eight servers. Enter the IP addresses of the servers in order of preference: the first address is the most preferred server, the second address is the next most preferred server, and so on. Use the **no** form of this command to remove the NetBIOS name server list.

Syntax

option netbios-name-server <*address1*> [<*address2*> ... <*address8*>]
no option netbios-name-server

Parameters

address	Specifies the IP address of a NetBIOS WINS name server. You can configure as many as eight servers.

Default

No WINS servers are configured.

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip dhcp server pool
option dns-server
option domain-name
option netbios-node-type

Example

The following example configures a list of NetBIOS name servers available to the client.

```
CES(config-dhcp)# option netbios-name-server 10.21.11.66
10.21.11.67 10.21.11.68
```

option netbios-node-type

Use this command to configure the NetBIOS node type for Microsoft DHCP clients. The recommended type is **h-node** (hybrid). Use the **no** form of this command to remove the NetBIOS node type.

Syntax

option netbios-node-type <*type*>
no option netbios-node-type

Parameters

type	Specifies the NetBIOS node type. Enter one of the following values: **b-node** (broadcast), **h-node** (hybrid), **m-node** (mixed), or **p-node** (peer-to-peer). The recommended value is hybrid (**h-node**).

Default

None

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip dhcp server pool
option netbios-name-server

Example

The following example specifies the client's NetBIOS type as hybrid.

```
CES(config-dhcp)# option netbios-node-type h-node
```

server-name

Use this command to specify the DHCP server name for the gateway. Use the **no** form of this command to remove the server name.

Syntax

server-name <*name*>
no server-name

Parameters

name	Specifies the DHCP server name.

Default

None

Command mode

DHCP Pool Configuration

Next command mode

DHCP Pool Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

bootfile
ip dhcp server pool
next-server
option

Example

The following example specifies “dakar” as the DHCP server name. To execute the **server-name** command, you must enter DHCP Pool Configuration mode with a host definition.

```
CES(config)# ip dhcp server pool network 147.26.246.63 host
santiago
CES(config-dhcp)# server-name dakar
CES(config-dhcp)#
```

service dhcp enable

Use this command to enable the DHCP server on the gateway. If the DHCP server is currently enabled and configuration changes have been made, you must disable the server and reenable it for the changes to take effect.

Use the **no** form of this command to disable the DHCP server on the gateway.



Note: To disable and reenable the DHCP server, you can also execute the **`service dhcp restart`** command.

Syntax

```
service dhcp enable
no service dhcp enable
```

Parameters

None

Default

Enabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

service dhcp restart

Example

The following example disables and reenables the DHCP server on the gateway to force updates to the configuration to take effect.

```
CES(config)# no service dhcp enable
CES(config)# service dhcp enable
```

service dhcp restart

Use this command to restart the DHCP server on the gateway. All changes to the configuration take effect after you execute this command. You can use this command instead of the commands **no service dhcp enable** and **service dhcp enable** to restart the server.

Syntax

service dhcp restart

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

`service dhcp enable`

Example

The following example restarts DHCP services on the DHCP server.

```
CES(config)# service dhcp restart
```

show ip dhcp server

Use this command to display current DHCP server settings for the gateway.

Syntax

`show ip dhcp server`

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

ip dhcp server pool

Example

The following example displays the current DHCP settings for the whole gateway.

```
CES# show ip dhcp server
!
dhcp global values
service: enabled
default lease time: 0 day(s) 12 hour(s) 0 minute(s) 0 second(s)
maximum lease time: 1 day(s) 0 hour(s) 0 minute(s) 0 second(s)
  subnet: 3.3.3.3
  network mask: 255.255.0.0
  default lease time: 0 day(s) 12 hour(s) 0 minute(s) 0 second(s)
  maximum lease time: 1 day(s) 0 hour(s) 0 minute(s) 0 second(s)
    host: shazam
    default lease time: 0 day(s) 12 hour(s) 0 minute(s) 0 second(s)
    maximum lease time: 1 day(s) 0 hour(s) 0 minute(s) 0 second(s)
    bootfile: dhcp-backup-bootfile
    host address: 3.3.3.4
    hardware address: 0:0:c0:5d:bd:95
  subnet: 47.26.11.0
  network mask: 255.255.0.0
  included addresses: 47.26.11.100 - 47.26.11.255
  excluded addresses: 47.26.11.140 - 47.26.11.150
  default lease time: 0 day(s) 12 hour(s) 0 minute(s) 0 second(s)
  maximum lease time: 1 day(s) 0 hour(s) 0 minute(s) 0 second(s)
  subnet: 192.168.0.0
  network mask: 255.255.255.0
  description: printer pool
  included addresses: 192.168.0.10 - 192.168.0.110
  default lease time: 0 day(s) 12 hour(s) 0 minute(s) 0 second(s)
  maximum lease time: 1 day(s) 0 hour(s) 0 minute(s) 0 second(s)
  option default router: 192.168.0.1
  option dns server: 192.168.0.1
  option netbios name server: 192.168.0.1
    host: printer
    default lease time: 0 day(s) 12 hour(s) 0 minute(s) 0 second(s)
    maximum lease time: 1 day(s) 0 hour(s) 0 minute(s) 0 second(s)
    host address: 192.168.0.111
    hardware address: 00:50:04:AD:28:03
CES#
```

DHCP server configuration example

The following commands configure a DHCP address pool (192.168.0.0/24) and one host (printer) that will always be assigned the same IP address (192.168.0.111). The last command enables the DHCP server on the gateway.

```
CES(config)# ip dhcp server pool network 192.168.0.0 mask /24
CES(config-dhcp)# description “printer address pool”
CES(config-dhcp)# included-address 192.168.0.10 192.168.0.110
CES(config-dhcp)# option default-router 192.168.0.1
CES(config-dhcp)# option dns-server 192.168.0.1
CES(config-dhcp)# option netbios-name-server 192.168.0.1
CES(config-dhcp)# exit
CES(config)# ip dhcp server pool network 192.168.0.0 host
printer
CES(config-dhcp)# host 192.168.0.111
CES(config-dhcp)# hardware-address 00:50:04:AD:28:03
CES(config-dhcp)# exit
CES(config)# service dhcp enable
CES(config)#
```

Chapter 17
SNMP commands

This chapter describes SNMP and SNMP trap configuration commands.

Command	Page
show snmp get-host	878
show snmp host	879
show snmp identity	880
show snmp mib	881
show snmp-traps trap-groups	883
show snmp-traps trap-hosts	886
snmp-ifspeed	886
snmp-server contact	889
snmp-server enable traps attack	890
snmp-server enable traps hardware	891
snmp-server enable traps ietf	896
snmp-server enable traps server	898
snmp-server enable traps service	900
snmp-server get-host	901
snmp-server host	903
snmp-server location	904
snmp-server management	905
snmp-server mib	906
snmp-server name	908

show snmp get-host

Use this command to display the SNMP get-host settings: state, host name or IP address, community name, and status.

Syntax

```
show snmp get-host
```

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

```
snmp-server location
snmp-server name
```

Example

```
CES# show snmp get-host
Host: 191.32.250.226
Enable: Enabled
Community: Public
Status: Error

Host: mycompany.com
Enable: Disabled
Community: My Company
Status: Configured

CES#
```

show snmp host

Use this command to display the SNMP trap host settings: state, host name or IP address, community name, and status.

Syntax

show snmp host

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

snmp-server location
snmp-server name

Example

```
CES# show snmp host
Host: 192.32.250.226
Enable: Enabled
Community: Public
Status: Error

Host: 10.0.10.111
Enable: Disabled
Community: test1
Status: Configured

CES#
```

show snmp identity

Use this command to display the SNMP identity settings: administratively assigned name, physical location, system description, ID, and contact information.

Syntax

show snmp identity

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

snmp-server location
snmp-server name

Example

```
CES# show snmp identity
SNMP IDENTITY:
SysDescr: V3.0
SysObjectID: 01.03.06.01.04.01.2505.05
SysName: Joe Smith
SysContact: Joe Smith
SysLocation: Boxboro, MA

CES#
```

show snmp mib

Use this command to display the SNMP MIB settings.

Syntax

show snmp mib

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

snmp-server location
snmp-server name

Example

```
CES# show snmp mib
IP Tunnel: ENABLED
RIPV2: DISABLED
OSPF: ENABLED
BGP: ENABLED
VRRP: DISABLED
IPX: ENABLED
RIPSAP: DISABLED
DSU/CSU: ENABLED

CES#
```

show snmp-traps trap-groups

Use this command to display the configuration of SNMP traps for various groups of MIBs, for example, hardware or services.

Syntax

```
show snmp-traps trap-groups {attack | hardware | ietf |
server | service}
```

Parameters

attack	Display the configuration of attack traps.
hardware	Display the configuration of hardware traps.
ietf	Display the configuration of IETF traps.
server	Display the configuration of server traps.
service	Display the configuration of service traps.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

show snmp-traps trap-hosts
snmp-server enable traps attack
snmp-server enable traps hardware
snmp-server enable traps ietf
snmp-server enable traps server
snmp-server enable traps service

Example

The following example displays hardware traps.

```
CES# show snmp-traps trap-groups hardware
SNMP Hardware Traps
  Name                          Enabled    Interval    Send One
  ---------------------------    -------    --------    ------
  Bulk Accelerator in slot 3     Yes         01:00:00    No
  WAN Slot 4 Interface 1         No          00:30:00    No
  LAN on Slot 1 Interface 1      Yes         00:30:00    No
  LAN on System Board            No          00:30:00    No
  ISDN BRI Card on slot 2        No          00:30:00    No
  Memory Usage                   Yes         00:15:00    No
  Hard Disk 0                    No          00:30:00    No
  Intrusion                      No          00:30:00    No
  Normal Temperature             No          00:30:00    No
  Voltage 12 V Plus              No          00:30:00    No
  Voltage 2.5 VA                 No          00:30:00    No
  Voltage 3.3 V Plus             No          00:30:00    No
  Voltage 5 V Plus               No          00:30:00    No
  Chassis Fan                    No          00:30:00    No
  CPU One Fan                    No          00:30:00    No
  Heart Beat                     No          00:30:00    No

CES#
```

The following example displays standard IETF traps.

```
CES# show snmp-traps trap-groups ietf
SNMP Standard IETF Traps
  Name                              Enabled
  ------------------------------    -------
  SNMP Authentication               Yes
  VRRP                              No
  BGP                               No
  OSPF                              Yes
  DSU/CSU                           Yes

Link Up/Down
  Name                              Enabled
  ------------------------------    -------
  Physical Interfaces               Yes
  BranchOffice Nailed-Up Tunnel     Yes
  BranchOffice OnDemand Tunnel      No

CES#
```

```
CES# show snmp-traps trap-groups ietf BGP
```

The following example displays server traps.

```
CES# show snmp-traps trap-groups server
SNMP Server Traps
  Name                          Enabled    Interval    Send One
  ------------------------      -------    --------    -------
  DHCP Server                       Yes        01:00:00    No
  CMP                               No         00:30:00    No
  Certificates Validity             Yes        00:30:00    No
  Auto Backup Servers               No         00:30:00    No
  Load Balancing Service            No         00:30:00    No
  Internal LDAP Server              No         00:30:00    No
  RADIUS Authentication Servers     No         00:30:00    No
  RADIUS Accounting Server          Yes        00:10:00    No
  External LDAP Servers             No         00:30:00    No
  SNMP Servers                      No         00:30:00    No
  IP Address Pool                   Yes        02:00:00    No
  LDAP Proxy Servers                No         00:30:00    No
  DNS Servers                       No         00:30:00    No

CES#
```

The following example displays service traps.

```
CES# show snmp-traps trap-groups service
SNMP Service Traps
  Name                          Enabled    Interval    Send One
  --------------------------    -------    --------    -------
  FIPS                           Yes        00:10:00    No
  NAT                            No         00:20:00    No
  Firewall                       Yes        00:30:00    No
  Temporary Licenses             No         24:00:00    No
  Buffer Usage                   Yes        00:30:00    No

CES#
```

The following example displays attack traps.

```
CES# show snmp-traps trap-groups attack
SNMP Attack Traps
  Name                          Enabled
  --------------------------    -------
  Failed Login                  Yes
  Firewall                      Yes
  Security Intrusion            Yes

CES#
```

show snmp-traps trap-hosts

Use this command to display the configuration of SNMP trap hosts for the Nortel VPN Router gateway.

Syntax

show snmp-traps trap-hosts

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

snmp-server host

Example

The following example displays trap hosts for the Nortel VPN Router gateway.

```
CES# show snmp-traps trap-hosts
SNMP Trap Hosts
  Host Name or IP Address       Community Name    Enabled
  --------------------------    --------------    --------
  47.11.22.33                   130               Yes
  Boston                        130               No
  New_York                      130               Yes

CES#
```

snmp-ifspeed

Syntax

```
snmp-ifspeed
no snmp-ifspeed
```

Parameters

Default

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

Example

```
CES(config-if)# snmp-ifspeed
CES(config-if)# no snmp-ifspeed
```

snmp-server contact

Use this command to set the system contact (sysContact) string. Use the **no** form of the command to remove the system contact information.

Syntax

snmp-server contact *<text>*
no snmp-server contact

Parameters

text	String that describes the system contact information. You must use double quotation marks if you use blank spaces.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

snmp-server location
snmp-server name

Example

```
CES(config)# snmp-server contact “System Admin x3333”
```

snmp-server enable traps attack

Use this command to enable SNMP traps for attacks on the Nortel VPN Router gateway. Use the **no** form of the command to disable traps.

Syntax

snmp-server enable traps attack [**failed-login** | **firewall** | **intrusion**]
no snmp-server enable traps attack [**failed-login** | **firewall** | **intrusion**]

Parameters

failed-login	Specifies that failed-login attacks will generate SNMP traps.
firewall	Specifies that firewall attacks will generate SNMP traps.
intrusion	Specifies that intrusion attacks will generate SNMP traps.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show snmp-traps trap-groups attack

Example

The following example enables traps on intrusion attacks and on failed logins.

```
CES# configure terminal
CES(config)# snmp-server enable traps attack intrusion
CES(config)# snmp-server enable traps attack failed-login
CES(config)#
```

The following example disables all traps on security attacks.

```
CES(config)# no snmp-server enable traps attack
CES(config)#
```

snmp-server enable traps hardware

Use this command to enable SNMP traps on hardware components. Use the **no** form of the command to disable traps on hardware. The hardware components that you can configure traps on depend on the type of Nortel VPN Router gateway and the hardware included in that gateway. To display a list of hardware components, enter the **snmp-server enable traps hardware ?** command.

Syntax

snmp-server enable traps hardware [<*type*> [**interval** <*time*>] [**send-one**]]
no snmp-server enable traps hardware [<*type*>]

Parameters

type	Specifies the hardware component. To see the hardware that you can set an SNMP trap on, enter the command **snmp-server enable traps hardware ?**.
interval	Specify that the condition for this trap be checked at the configured interval.
time	Specifies how often the condition for this trap is checked. Type the time in this format: *hh:mm:ss*.
send-one	Specifies that the software send only one SNMP trap.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show snmp-traps trap-groups hardware

Example

The following example shows a sample display of hardware when you use the question mark command.

```
CES(config)# snmp-server enable traps hardware ?
  accelerator-1     System Accelerator on Slot 1
  accelerator-2     System Accelerator on Slot 2
  accelerator-3     System Accelerator on Slot 3
  accelerator-4     System Accelerator on Slot 4
  accelerator-5     System Accelerator on Slot 5
  accelerator-6     System Accelerator on Slot 6
  chassis-fan       Chassis Fan
  chassis-fan2      Chassis Fan 2
  cpu2              CPU 2
  disk0             Hard Disk 0
  disk1             Hard Disk 1
  dual-power        Dual Power Supply
  fan1              CPU One Fan
  fan2              CPU Two Fan
  heart-beat        Heart Beat
  hssi0             High Speed Serial Interface 0
  hssi1             High Speed Serial Interface 1
  interval          Polling Interval
  intrusion         Intrusion
  lan-1/1           LAN on Slot 1 Interface 1
  lan-2/1           LAN on Slot 2 Interface 2
  lan-3/1           LAN on Slot 3 Interface 3
  lan-4/1           LAN on Slot 4 Interface 4
  lan-5/1           LAN on Slot 5 Interface 5
  lan-6/1           LAN on Slot 6 Interface 6
  lan-system        LAN on System Board
  memory            Memory Usage
  send-one          Trap sent once
  temp-critical     Critical Temperature
  temp-normal       Normal Temperature
  voltage-12minus   Voltage 12 V Minus
  voltage-12plus    Voltage 12 V Plus
  voltage-2.5a      Voltage 2.5 VA
  voltage-2.5b      Voltage 2.5 VB
  voltage-3.3minus  Voltage 3.3 V Minus
  voltage-3.3plus   Voltage 3.3 V Plus
  voltage-5minus    Voltage 5 V Minus
```

```
  voltage-5plus     Voltage 5 V Plus
  wan-1/1           WAN Slot 1 Interface 1
  wan-1/2           WAN Slot 1 Interface 2
  wan-2/1           WAN Slot 2 Interface 1
  wan-2/2           WAN Slot 2 Interface 2
  wan-3/1           WAN Slot 3 Interface 1
  wan-3/2           WAN Slot 3 Interface 2
  wan-4/1           WAN Slot 4 Interface 1
  wan-4/2           WAN Slot 4 Interface 2
  wan-5/1           WAN Slot 5 Interface 1
  wan-5/2           WAN Slot 5 Interface 2
  wan-6/1           WAN Slot 6 Interface 1
  wan-6/2           WAN Slot 6 Interface 2
  <cr>
```

The following example enables an SNMP trap on the hardware encryption accelerator card in slot 1.

```
CES# configure terminal
CES(config)# snmp-server enable traps hardware accelerator-1
CES(config)#
```

The following example enables an SNMP trap on the system LAN port with a polling interval of 1 hour and with the option to send only one trap.

```
CES(config)# snmp-server enable traps hardware lan-system
interval 01:00:00 send-one
CES(config)#
```

The following example disables the sending of SNMP traps for the chassis fan.

```
CES(config)# no snmp-server enable traps hardware chassis-fan
CES(config)#
```

snmp-server enable traps ietf

Use this command to enable SNMP standard IETF traps on a Nortel VPN Router gateway. Use the **no** form of the command to disable a trap.

Syntax

```
snmp-server enable traps ietf [authentication |
bo-tunnel-nailed-up | bo-tunnel-ondemand | dsu/csu | ospf |
physical | vrrp]

no snmp-server enable traps ietf [authentication |
bo-tunnel-nailed-up | bo-tunnel-ondemand | dsu/csu | ospf |
physical | vrrp]
```

Parameters

authentication	Enable standard IETF traps for SNMP authentication.
bo-tunnel-nailed-up	Enable standard IETF traps for nailed-up branch office tunnels.
bo-tunnel-ondemand	Enable standard IETF traps for on-demand branch office tunnels.
dsu/csu	Enable standard IETF traps for DSU/CSU.
ospf	Enable standard IETF traps for OSPF.
physical	Enable standard IETF traps for physical interfaces.
vrrp	Enable standard IETF traps for VRRP.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show snmp-traps trap-groups ietf

Example

The following example enables standard IETF traps on SNMP authentication, on OSPF, and on physical interfaces.

```
CES# configure terminal
CES(config)# snmp-server enable traps ietf authentication
CES(config)# snmp-server enable traps ietf ospf
CES(config)# snmp-server enable traps ietf physical
CES(config)#
```

The following example disables standard IETF traps on on-demand branch office tunnels.

```
CES(config)# no snmp-server enable traps ietf
bo-tunnel-ondemand
```

The following example disables all standard IETF traps.

```
CES(config)# no snmp-server enable traps ietf
CES(config)#
```

snmp-server enable traps server

Use this command to enable SNMP traps on servers used by the Nortel VPN Router gateway. Use the **no** form of the command to disable traps on servers. To display a list of servers, enter the **snmp-server enable traps server ?** command.

Syntax

snmp-server enable traps server [<*type*> [**interval** <*time*>] [**send-one**]]
no snmp-server enable traps server [<*type*>]

Parameters

type	Specifies the type of server. To display a list of the servers that you can set an SNMP trap on, enter the command **snmp-server enable traps server ?**.
interval	Specify that the condition for this trap be checked at the configured interval.
time	Specifies how often the condition for this trap is checked. Type the time in this format: *hh:mm:ss*.
send-one	Specifies that the software send only one SNMP trap.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show snmp-traps trap-groups server

Example

The following example enables traps on the auto-backup servers and sets the polling interval to 45 minutes.

```
CES# configure terminal
CES(config)# snmp-server enable traps server backup interval
00:45:00
```

The following example enables traps on the IP address pool servers and configures the gateway check the servers every 30 minutes and to send only one trap.

```
CES(config)# snmp-server enable traps server ipaddr-pool
interval 00:30:00 send-one
CES(config)#
```

The following example disables traps on the SNMP and DNS servers.

```
CES(config)# no snmp-server enable traps server dns
CES(config)# no snmp-server enable traps server snmp
CES(config)#
```

snmp-server enable traps service

Use this command to enable SNMP traps on services for a Nortel VPN Router gateway. Use the **no** form of the command to disable a trap. To display a list of services, enter the **`snmp-server enable traps services ?`** command.

Syntax

`snmp-server enable traps service` [<*`type`*> [**`interval`** <*`time`*>] [**`send-one`**]]
`no snmp-server enable traps service` [<*`type`*>]

Parameters

type	Specifies the type of service. Type one of the following services: **anti-spoofing**, **buffer**, **fips**, **firewall**, **nat**, or **temp-license**.
interval	Specify that the condition for this trap be checked at the configured interval.
time	Specifies how often the condition for this trap is checked. Type the time in this format: *hh:mm:ss*.
send-one	Specifies that the software send only one SNMP trap.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show snmp-traps trap-groups services

Example

The following example enables SNMP traps on the firewall and NAT services. The services will be checked every hour.

```
CES# configure terminal
CES(config)# snmp-server enable traps service firewall
interval 01:00:00
CES(config)# snmp-server enable traps service nat interval
01:00:00
CES(config)#
```

The following example disables SNMP traps on the buffer usage and anti-spoofing services.

```
CES(config)# no snmp-server enable traps service buffer
CES(config)# no snmp-server enable traps service
anti-spoofing
CES(config)#
```

snmp-server get-host

This command defines an SNMP management station that is authorized to send SNMP get requests to the gateway. Use the **no** form of the command to remove the specified host.

Syntax

snmp-server get-host <*host*> [<*community-string*>] {**enabled** | **disabled**}
no snmp-server get-host <*host*>

Parameters

host	Name or IP address of the host.
community-string	Password-like community string sent with the notification operation.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

snmp-server host

Example

```
CES(config)# snmp-server get-host myhost.mycompany.com
public disabled
CES(config)# snmp-server get-host myhost.mycompany.com
enabled
CES(config)# no snmp-server ‘get-host myhost.mycompany.com
```

snmp-server host

This command set defines a host recipient of an SNMP notification operation. Use the **no** form of the command to remove the specified host.

Syntax

snmp-server host <*host*> [<*community-string*>] {**enabled** | **disabled**}
no snmp-server host <*host*>

Parameters

host	Name or IP address of the host.
community-string	Password-like community string sent with the notification operation.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

snmp-server enable traps

Example

```
CES(config)# snmp-server host myhost.mycompany.com public
CES(config)# no snmp-server host myhost.mycompany.com
```

snmp-server location

This command sets the system location (sysLocation) string. Use the **no** form of the command to remove the system location string.

Syntax

snmp-server location <*text*>
no snmp-server location

Parameters

text	String that describes the system location information. If you include spaces, you must use double quotation marks.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

snmp-server name
snmp-server contact

Example

```
CES(config)# snmp-server location “Building 4/Room 333”
```

snmp-server management

Use this command to enable SNMP on the private interfaces of the gateway. Use the **no** form of the command to disable SNMP. For greater security, the gateway supports SNMP MIB II **get** commands only.

Syntax

snmp-server management
no snmp-server management

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

show services management
snmp-server name
snmp-server contact

Example

The following example enables SNMP on the gateway.

```
CES# configure terminal
CES(config)# snmp-server management
CES(config)#
```

The following example disables SNMP on the gateway.

```
CES(config)# no snmp-server management
CES(config)#
```

snmp-server mib

This command enables the SNMP MIBs. Use the **no** form of the command to disable the SNMP MIBs.

Syntax

snmp-server mib {**iptunnel** | **rip2** | **ospf** | **vrrp** | **ipx** | **ripsap** | **dsu/csu**}
no snmp-server mib

Parameters

iptunnel	IP Tunnel
ripv2	RIP Version 2
ospf	OSPF
vrrp	VRRP

ipx	IPX
ripsap	RIP SAP
dsu/csu	DSU/CSU

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Prerequisites

Nortel proprietary MIBs included on the Nortel CD-ROM.

Related commands

show snmp mib

Example

```
CES(config)# snmp-server mib ospf
```

snmp-server name

This command sets the system name (sysName) string. Use the **no** form of the command to remove the system name string.

Syntax

snmp-server name <*text*>
no snmp-server name

Parameters

text	String that describes the system location information. If you include spaces, you must use double quotation marks.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

snmp-server contact
snmp-server location

Example

```
CES(config)# snmp-server name “Contivity32”
```

Chapter 18
Certificate commands

Using the CLI, you can configure certificates using the Certificate Management Protocol and store a file containing a certificate from Entrust Server. This file can be transferred to the Nortel VPN Router using FTP and then imported via the PKCS #7 Base-64 certificate from a CA into the gateway's database.

This chapter describes the certificate configuration commands.

Command	Page
ca-allow-all enable	911
ca-import enable	912
ca-trusted enable	914
country	915
create	914
crl	918
crl http	919
crl optimize	921
crl optional	922
crl search-base host port attribute	923
crl search-base host port bind-dn	925
crl search-base host port enable	928
crl search-base host port object-class	930
crl search-base host port password	932
crl search-base host port ssl-enable	934
crl update	936
crypto ca allow	937

Command	Page
crypto ca configure	939
crypto ca identity	940
crypto import	941
crypto password	942
crypto server configure	943
crypto server request	945
crypto trusted	946
default-group	947
enrollment url	948
key	950
locality	951
name	952
no crypto ca enroll	953
no crypto server certificate renew	954
openSSL enable	955
organization	958
org-unit	957
ocsp	960
recover reference-number	961
renew	962
revoke now	963
set authorization-code	964
set ca-default-group	965
set issuer	966
set issuer-dn	967
set key-size	968
set port	969
set reference-number	971
set subject-dn	972
show crypto ca certificates	973

Command	Page
show crypto certificates	976
show crypto enrollment	977
show crypto password	978
show crypto server certificates renew	980
state	981
subject-dn	982

ca-allow-all enable

This command specifies that anyone with a valid certificate from the specified CA can establish a tunnel connection. The **no** form of the command disables this behavior.

Syntax

```
ca-allow-all enable
no ca-allow-all enable
```

Parameters

None

Default

Disabled

Command mode

CA Identity Configuration

Next command mode

CA Identity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ca-import enable
ca-trusted enable
enrollment url

Example

The following example specifies that any user with a valid certificate from the CA can establish a tunnel connection.

```
CES(config)# crypto ca identity 12312343 ASD-ASD_ASD
CES(config-ca-identity)# ca-allow-all enable
CES(config-ca-identity)# exit
CES(config)#
```

ca-import enable

This command specifies that the issuer CA certificate can be imported. The **no** form of the command specifies that the CA certificate not be imported.

Syntax

ca-import enable
no ca-import enable

Parameters

None

Default

Disabled

Command mode

CA Identity Configuration

Next command mode

CA Identity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ca-allow-all enable
ca-trusted enable
enrollment url

Example

The following example specifies that a certificate from the CA can be imported.

```
CES(config)# crypto ca identity 12312343 ASD-ASD_ASD
CES(config-ca-identity)# ca-import enable
CES(config-ca-identity)# exit
CES(config)#
```

ca-trusted enable

This command specifies that this issuer CA certificate is trusted. The **no** form of the command specifies that the CA certificate is not trusted.

Syntax

```
ca-trusted enable
no ca-trusted enable
```

Parameters

None

Default

Disabled

Command mode

CA Identity Configuration

Next command mode

CA Identity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
ca-allow-all enable
ca-import enable
enrollment url
```

Example

The following example specifies that the certificate from the CA can be assumed to be trusted.

```
CES(config)# crypto ca identity 12312343 ASD-ASD_ASD
CES(config-ca-identity)# ca-trusted enable
CES(config-ca-identity)# exit
CES(config)#
```

country

Use this command to enter the country for the PKCS#10 certificate request.

Syntax

country <*text*>

Parameters

text	Specifies the country of the associated gateway.

Default

None

Command mode

Certificate Request Configuration

Next command mode

Certificate Request Configuration

Related commands

crypto server request
openSSL enable

Example

The following example navigates to Certificate Request Configuration mode and specifies the country for the PKCS#10 certificate request.

```
CES(config)# crypto server request
CES(config-request)# country Brasil
CES(config-request)#
```

create

Use this command to create a PKCS#10 encoded certificate request.

Syntax

create

Parameters

None

Default

None

Command mode

Certificate Request Configuration

Next command mode

Certificate Request Configuration

Related commands

crypto server request
openSSL enable

Example

The following example creates a PKCS#10 certificate request. (Copy and paste the encoded certificate request—including the “BEGIN” and “END” lines—to a file to submit to the certificate authority.)

```
CES(config)# crypto server request
CES(config-request)# name www.circularsystems.com
CES(config-request)# org-unit Marketing
CES(config-request)# organization “Circular Systems, Inc.”
CES(config-request)# locality Barlow
CES(config-request)# state AK
CES(config-request)# country US
CES(config-request)# create
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBnAIBADAXMRUwEwYDVQQDFAxibGFoYmxhaGJsYWgwfDANBgkqhkiG9w0BAQ
EFAANrADBoAmEA3tqIjU7G9Iznf4LPtLAHxdXktsuPt8R9V0AsoqUSQnaqJT2iPE9S
g/8uTDRmIr8Ue7venKyHz13lSXzwGA/ePBWXalu5gRJOWb0/s8Nv8qjiaBjERqJtKa
KJs0+yVjoNAgMBAAGgADANBgkqhkiG9w0BAQQFAANhAI40SufRelrewJjkN/KQ+uU
o/bpQVmWYSDPyWsI5LuxLaEwo3njNr7zSrhDpAgFGYCWS4cvz8oacuRnXhs BQKfS+
4pyPIvbw5LwzorLffFYBIIWQgj4vQr7cCSqpF9wShw==
-----END CERTIFICATE REQUEST-----
CES(config-request)#
```

crl

This command enables and disables the global certificate revocation list (CRL) to support multiple CRL servers.

Syntax

```
crl
no crl
```

Parameters

None

Default

Enabled on the private side of the gateway.

Command mode

CA Configuration

Related commands

```
crl optimize
crl optional
crl update
```

Example

```
CES(config)# crypto ca configure “OU=Entrust-CA,
O=engeast.mycompany.com”
CES(config-ca)# no crl
CES(config-ca)# exit
```

crl http

This command configures the HTTP CRL server.

Syntax

crl http *<path-name> <host-name> <port-number> [ssl-enable] [enable]*

Parameters

path-name	specifies the HTTP CRL server path name
host_name	specifies the HTTP CRL server IP address
port-number	specifies the HTTP CRL server port number

Default

No CA configuration exists by default.

Command mode

Crypto CA configuration mode

Next command mode

Certificate Configuration

Related commands

ocsp

Example

```
CES(config)#
CES(config-ca)# crl http <path-name> <host-name>
<port-number> [ssl-enable] [enable]
```

crl optimize

Use this command to enable CRL performance improvements (for LDAP import only). Use the **no** form of the command to disable CRL performance improvements.

Syntax

```
crl optimize
no crl optimize
```

Parameters

None

Default

Not optimized

Command mode

CA Configuration

Next command mode

CA Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

crl
crl optional
crl update
show crypto ca certificates

Example

The following example enables CRL performance optimization.

```
CES(config)# crypto ca configure “OU=Entrust-CA,
O=engeast.nortelnetworks.com”
CES(config-ca)# crl optimize
CES(config-ca)#
```

The following example disables CRL performance optimization.

```
CES(config-ca)# no crl optimize
CES(config-ca)#
```

crl optional

This command allows certificates to be accepted by your gateway even if the appropriate CRL is not acceptable to your gateway.

Syntax

crl optional
no crl optional

Parameters

None

Default

None

Command mode

CA Configuration

Related commands

crl
crl optimize
crl update

Example

```
CES(config)# crypto ca configure ”OU=Entrust-CA,
O=engeast.mycompany.com”
CES(config-ca)# crl optional
CES(config-ca)# exit
```

crl search-base host port attribute

Use this command to configure the attribute that the CRL is stored under on the directory server for the certificate revocation list (CRL) for the particular CA. Use the **no** form of the command to delete the attribute.

Syntax

crl search-base <*search-base*> **host** <*host*> **port** <*port*> **attribute** <*attribute*>
no crl search-base <*search-base*> **host** <*host*> **port** <*port*> **attribute**

Parameters

search-base	Specifies the portion of the X.500 directory where the CA stores certificate revocation lists.
host	Specifies the host name or IP address of the LDAP-accessible directory server that is storing the published CRLs. If you specify a host name, then one or more DNS servers must be configured on the gateway's System Identity screen.
port	Specifies the port number on the gateway.
attribute	Specifies the attribute that the CRL is stored under in the directory server. Enter up to 500 characters. If the string contains spaces, enclose the string in quotation marks.

Default

None

Command mode

CA Configuration

Next command mode

CA Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

crl search-base host port bind-dn
crl search-base host port enable
crl search-base host port object-class
crl search-base host port password
crl search-base host port ssl-enable
show crypto ca certificates

Example

The following example configures an attribute for a search base, host, and port set.

```
CES(config)# crypto ca configure “OU=Entrust-CA,
O=engeast.nortelnetworks.com”
CES(config-ca)# crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 999 attribute
“certificateRevocationlist;binary”
CES(config-ca)#
```

The following example deletes the attribute for a search base, host, and port set.

```
CES(config-ca)# no crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 999 attribute
CES(config-ca)#
```

crl search-base host port bind-dn

Use this command to configure the DN (distinguished name) that the Nortel VPN Router gateway will use to bind to the directory server for a particular CA. Use the **no** form of the command to delete the distinguished name.

Syntax

crl search-base <*search-base*> **host** <*host*> **port** <*port*>
bind-dn <*string*>
no crl search-base <*search-base*> **host** <*host*> **port** <*port*>
bind-dn

Parameters

search-base	Specifies the portion of the X.500 directory where the CA stores certificate revocation lists.
host	Specifies the host name or IP address of the LDAP-accessible directory server that is storing the published CRLs. If you specify a host name, then one or more DNS servers must be configured on the gateway's System Identity screen.
port	Specifies the port number on the gateway.
bind-dn-string	Specifies the distinguished name that the gateway will use to bind to the directory server. Enter up to 500 characters. If the string contains spaces, enclose the string in quotation marks.

Default

None

Command mode

CA Configuration

Next command mode

CA Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

crl search-base host port attribute
crl search-base host port enable
crl search-base host port object-class
crl search-base host port password
crl search-base host port ssl-enable
show crypto ca certificates

Example

The following example configures a bind DN and a password for a search base, host, and port set. (You must set a password to use a bind DN.)

```
CES(config)# crypto ca configure “OU=Entrust-CA,
O=engeast.baynetworks.com”
CES(config-ca)# crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 414 bind-dn “uid=admin,
ou=Administrators, ou=TopologyManagement, o=NetscapeRoot”
CES(config-ca)# crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 414 password 1e2y3t4b5tRF8
CES(config-ca)#
```

The following example deletes the DN for a search base, host, and port set.

```
CES(config-ca)# no crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 414 bind-dn
CES(config-ca)#
```

crl search-base host port enable

Use this command to enable a specific certificate revocation list (CRL) server. Use the **no** form of the command to disable the CRL server. The search base, host, connection, and update frequency values must be set for proper access to the CRL LDAP directory store.

Syntax

crl search-base <*search-base*> **host** <*host*> **port** <*port*> **enable**
no crl search-base <*search-base*> **host** <*host*> **port** <*port*> **enable**

Parameters

search-base	Specifies the portion of the X.500 directory where the CA stores certificate revocation lists.
host	Specifies the host name or IP address of the LDAP-accessible directory server that is storing the published CRLs. If you specify a host name, then one or more DNS servers must be configured on the gateway's System Identity screen.
port	Specifies the port number on the gateway.

Default

None

Command mode

CA Configuration

Next command mode

CA Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

crl search-base host port attribute
crl search-base host port bind-dn
crl search-base host port object-class
crl search-base host port password
crl search-base host port ssl-enable
show crypto ca certificates

Example

The following example enables the CRL search base for a search base, host, and port set.

```
CES(config)# crypto ca configure “OU=Entrust-CA,
O=engeast.baynetworks.com”
CES(config-ca)# crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 333 enable
CES(config-ca)#
```

The following example disables the CRL search base for a search base, host, and port set.

```
CES(config-ca)# no crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 333 enable
CES(config-ca)#
```

crl search-base host port object-class

Use this command to specify an object class that the CRL is stored under on the directory server. Use the **no** form of the command to delete the object class.

Syntax

```
crl search-base <search-base> host <host> port <port>
object-class <object-class>
no crl search-base <search-base> host <host> port <port>
object-class
```

Parameters

search-base	Specifies the portion of the X.500 directory where the CA stores certificate revocation lists.
host	Specifies the host name or IP address of the LDAP-accessible directory server that is storing the published CRLs. If you specify a host name, then one or more DNS servers must be configured on the gateway's System Identity screen.
port	Specifies the port number on the gateway.
object-class	Specifies the object class string.

Default

None

Command mode

CA Configuration

Next command mode

CA Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

crl search-base host port attribute
crl search-base host port bind-dn
crl search-base host port enable
crl search-base host port password
crl search-base host port ssl-enable
show crypto ca certificates

Example

The following example configures the object class for a search base, host, and port set.

```
CES(config)# crypto ca configure “OU=Entrust-CA,
O=engeast.baynetworks.com”
CES(config-ca)# crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 333 object-class pkiCA
CES(config-ca)#
```

The following example deletes the object class for a search base, host, and port set.

```
CES(config-ca)# no crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 333 object-class
CES(config-ca)#
```

crl search-base host port password

Use this command to configure a password that will be used along with the bind DN when the Nortel VPN Router gateway binds to the directory server. Use the **no** form of the command to delete the password.

Syntax

```
crl search-base <search-base> host <host> port <port>
password <password>
no crl search-base <search-base> host <host> port <port>
password
```

Parameters

search-base	Specifies the portion of the X.500 directory where the CA stores certificate revocation lists.
host	Specifies the host name or IP address of the LDAP-accessible directory server that is storing the published CRLs. If you specify a host name, then one or more DNS servers must be configured on the gateway's System Identity screen.
port	Specifies the port number on the gateway.
password	Specifies the password. Enter up to 64 characters.

Default

None

Command mode

CA Configuration

Next command mode

CA Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

crl search-base host port attribute
crl search-base host port bind-dn
crl search-base host port enable
crl search-base host port object-class
crl search-base host port ssl-enable
show crypto ca certificates

Example

The following example configures a bind DN and a password for a search base, host, and port set.

```
CES(config)# crypto ca configure “OU=Entrust-CA,
O=engeast.baynetworks.com”
CES(config-ca)# crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 414 bind-dn “uid=admin,
ou=Administrators, ou=TopologyManagement, o=NetscapeRoot”
CES(config-ca)# crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 414 password 1e2y3t4b5tRF8
CES(config-ca)#
```

The following example deletes the password for a search base, host, and port set.

```
CES(config-ca)# no crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 414 password
CES(config-ca)#
```

crl search-base host port ssl-enable

Use this command to enable SSL for the certificate revocation list (CRL) for a specific CA. Use the **no** form of the command to disable SSL. The search base, host, connection, and update frequency values must be set for proper access to the CRL LDAP directory store.

Syntax

```
crl search-base <search-base> host <host> port <port>
ssl-enable
no crl search-base <search-base> host <host> port <port>
ssl-enable
```

Parameters

search-base	Specifies the portion of the X.500 directory where the CA stores certificate revocation lists.
host	Specifies the host name or IP address of the LDAP-accessible directory server that is storing the published CRLs. If you specify a host name, then one or more DNS servers must be configured on the gateway's System Identity screen.
port	Specifies the port number on the gateway.

Default

port 389
SSL disabled

Command mode

CA Configuration

Next command mode

CA Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

crl search-base host port attribute
crl search-base host port bind-dn
crl search-base host port enable
crl search-base host port object-class
crl search-base host port password
show crypto ca certificates

Example

The following example enables SSL for a search base, host, and port set.

```
CES(config)# crypto ca configure “OU=Entrust-CA,
O=engeast.baynetworks.com”
CES(config-ca)# crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 1245 ssl-enable
CES(config-ca)#
```

The following example disables SSL for a search base, host, and port set.

```
CES(config-ca)# no crl search-base “ou=Engineering, o=Nortel
Networks, c=US” host 1.1.1.1 port 1245 ssl-enable
CES(config-ca)#
```

crl update

This command specifies the frequency with which the gateway should query the CA's LDAP server for a newly published CRL.

Syntax

```
crl update {specific-time time <hh:mm> {none | every |
[monday][tuesday] [wednesday][thursday] [friday] [saturday]
[sunday]}{now}
no crl update specific-time {[monday] [tuesday] [wednesday]
[thursday] [friday] [saturday] [sunday]}
```

Parameters

specific-time time	Where hh:mm is the hour (0 to 24) and minutes of the time to apply the CRL Update.
none	Specifies CRL Update as none.
every	Specifies CRL Update as everyday.
[monday] [tuesday] [wednesday] [thursday] [friday] [saturday] [sunday]	Specifies CRL Update as specific days.
now	Spontaneously applies a CRL Update.

Default

None

Command mode

CA Configuration

Related commands

crl
crl optimize
crl optional

Example

```
CES(config)# crypto ca configure ”OU=Entrust-CA,
O=engeast.mycompany.com”
CES(config-ca)# crl update specific-time time 6:30 every
CES(config-ca)# exit
```

crypto ca allow

This command permits authentication without an explicit user entry authentication for a CA certificate. This allows anyone with a valid certificate from the particular CA to establish a tunnel connection.

Syntax

crypto ca allow {<*subject-dn*> | **all**}

Parameters

subject-dn	CA’s subject DN.
all	Allow all.

Default

None

Command mode

Global Configuration

Next Command mode

Global Configuration

Example

```
CES(config)# crypto ca allow “ou=MYCA, c=US”
```

crypto ca configure

This command configures the CA.

Syntax

crypto ca configure <*subject-dn*>

Parameters

subject-dn	CA's subject DN.

Default

No CA configuration exists by default.

Command mode

Global Configuration

Next command mode

Certificate Configuration

Related commands

crypto ca identity

Example

```
CES(config)# crypto ca configure MyCA
CES(config-ca)#
```

crypto ca identity

This command allows you to create CMP-compliant certificate requests. CMP is derived from the Entrust PKI Management protocol and includes management functions for the entire certificate and key life cycle.

Syntax

crypto ca identity <*reference*> <*authorization-code*>

Parameters

reference	Reference number.
authorization-code	Authorization code value.

Default

No CA configuration exists by default.

Command mode

Global Configuration

Next command mode

CA Identity Configuration

Warning messages

```
% Enrollment request does not exist.
```

Related commands

```
set authorization-code
set port
set reference-number
```

Example

```
CES(config)# crypto ca identity 1321543 ASD-ASD-ET
CES(config-ca-identity)#
```

crypto import

This command imports (pastes) a PKCS #7 Base-64 Certificate from a CA into the gateway's database.

Syntax

crypto {**ca** | **server** | **ssl**} **import** <*filename.dat*>
no crypto {**ca** | **server** | **ssl**} **certificate subject DN**

Parameters

ca	CA certificate.
server	Server certificate.
ssl	SSL certificate.
filename	Filename with encrypted certificate from CA. All files from CA are stored in system/certificate.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

crypto ca identity

Example

If you use the **ca** or **ssl** keyword, you can use FTP to send the certificate as a file to the system/cert/import directory and then import it.

```
CES(config)# crypto ca import ca0102.dat
```

If you use the **server** keyword, you must first generate the request through the UI and then use FTP to send it to the system/cert/import directory and import it.

```
CES(config)# crypto server import s01
```

crypto password

This command enters a crypto key storage password.

Syntax

crypto password <*value*>

Parameters

value	Crypto key password used to encrypt the public key before applying for a certificate.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show crypto password

Example

```
CES(config)# crypto password abcdefgh
Key Storage Password created
```

crypto server configure

This command navigates to the server certificate configuration mode (config-servercert#).

Syntax

crypto server configure {<*word*>}

Parameters

word	Fully distinguished name in the form "CN=kb ces2, OU=Entrust-CA, O=engeast.nortelnetworks.com".

Default

None

Command mode

Global Configuration

Next command mode

Server Certificate Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Server Certificate does not exist.
```

Related commands

enrollment url
set port

Example

```
CES(config)# crypto server configure "CN=kb ces2,
OU=Entrust-CA, O=engeast.nortelnetworks.com"
CES(config-servercert)#
```

crypto server request

Use this command to enter Certificate Request Configuration mode. The commands that you execute in this mode are transient and are not captured by the **show running-config** command.

Syntax

crypto server request

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Certificate Request Configuration

Prerequisites

The private key password must be initialized.

Warning messages

```
% Private Key Password is not currently initialized. You
must initialize the Private Key Password to a non-empty
value.
```

Related commands

country
create
crypto password
exit
key
locality
name
openSSL enable
org-unit
organization
state

Example

The following example navigates to Certificate Request Configuration mode.

```
CES(config)# crypto server request
CES(config-request)#
```

crypto trusted

This command designates this certificate as trusted if it is verified that the certificate is authorized and has been validated.

Syntax

crypto {**ca** | **server** | **ssl**} **trusted** <*subject-dn*>
no crypto {**ca** | **server** | **ssl**} **trusted** <*subject-dn*>

Parameters

ca	CA certificate.
server	Server certificate.
subject-dn	Subject DN.
ssl	SSL certificate.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Example

```
CES(config)# crypto ca trusted “ou=mycompany, c=US”
CES(config)# no crypto ca trusted “ou=mycompany, c=US”
```

default-group

This command specifies the default group.

Syntax

default-group <*group-name*>

Parameters

group-name	Default group name.

Default

/Base

Command mode

CA Configuration

Warning messages

```
% Group does not exist.
```

Related commands

subject-dn

Example

```
CES(config)# crypto ca configure ”OU=Entrust-CA,
O=engeast.mycompany.com”
CES(config-ca)# default-group /Base/test
CES(config-ca)# exit
```

enrollment url

This command specifies the enrollment address of the Entrust CA server or a server where CMP requests are sent.

Syntax

enrollment url *<url>*
no enrollment url

Parameters

url	Specifies the enrollment address.

Default

None

Command mode

CA Identity Configuration
Server Certificate Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

set authorization-code
set port
set reference-number

Example

This example specifies the enrollment URL for an Entrust CA server.

```
CES(config)# crypto ca identity 12312343 ASD-ASD_ASD
CES(config-ca-identity)# enrollment url http://123.54.6.54
CES(config-ca-identity)# exit
```

This example specifies the enrollment URL for a CMP server.

```
CES(config)# crypto server configure "CN=kb ces2,
OU=Entrust-CA, O=engeast.nortelnetworks.com"
CES(config-servercert)# enrollment url 5.54.6.54
CES(config-servercert)# exit
```

key

Use this command to specify the public key size in bits for the PKCS#10 certificate request.

Syntax

key {1 | 2 | 3 | 4}

Parameters

1, **2**, **3**, **4, 5**	Specifies the public key size in bits. • 1 = 512 bits (default value) • 2 = 768 bits • 3 = 1024 bits • 4 = 2048 bits (US only) • 5 = 4096 bits

Default

1 (512 bits)

Command mode

Certificate Request Configuration

Next command mode

Certificate Request Configuration

Related commands

crypto server request
openSSL enable

Example

The following example navigates to Certificate Request Configuration mode and sets the key bit length for the PKCS#10 certificate request to 1024 bits.

```
CES(config)# crypto server request
CES(config-request)# key 3
CES(config-request)#
```

locality

Use this command to enter the locality for the PKCS#10 certificate request.

Syntax

locality <*text*>

Parameters

text	Specifies the locality of the associated gateway.

Default

None

Command mode

Certificate Request Configuration

Next command mode

Certificate Request Configuration

Related commands

crypto server request
openSSL enable

Example

The following example navigates to Certificate Request Configuration mode and specifies the locality for the PKCS#10 certificate request.

```
CES(config)# crypto server request
CES(config-request)# locality Saskatoon
CES(config-request)#
```

name

Use this command to enter the name for the PKCS#10 certificate request.

Syntax

name <*text*>

Parameters

text	Specifies the common name or the Entrust reference number.

Default

None

Command mode

Certificate Request Configuration

Next command mode

Certificate Request Configuration

Related commands

crypto server request
openSSL enable

Example

The following example navigates to Certificate Request Configuration mode and specifies the name for the PKCS#10 certificate request.

```
CES(config)# crypto server request
CES(config-request)# name “Circular Logic Corp”
CES(config-request)#
```

no crypto ca enroll

Use the **no** form of this command to delete a current enrollment request.

Syntax

no crypto ca enroll <*reference*> <*authorization-code*>

Parameters

reference	Reference number.
authorization-code	Authorization code value.

Default

No CA requests.

Command mode

Global Configuration

Warning messages

```
% Enrollment request does not exist.
```

Related commands

crypto ca identity

Example

```
CES(config)# no crypto ca enroll 879354321 ASD-ASDIO
```

no crypto server certificate renew

This command disables the renewal of the certificate.

Syntax

no crypto server certificate <*word*> **renew**

Parameters

word	Fully distinguished name.

Default

None

Command mode

Server Certificate Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

renew
revoke now

Example

```
CES(config-servercert)# no crypto server certificate "CN= kb
ces2, OU=Entrust-CA, O=engeast.baynetworks.com" renew
```

openSSL enable

Use this command to generate a PKCS#10 certificate request that is compatible with OpenSSL, a free implementation of Secure Socket Layer used by some certificate authorities. Use the **no** form of the command to disable OpenSSL compatibility.

Syntax

openSSL enable
no openSSL enable

Parameters

None

Default

Disabled

Command mode

Certificate Request Configuration

Next command mode

Certificate Request Configuration

Related commands

crypto server request

Example

The following example navigates to Certificate Request Configuration mode and enables OpenSSL compatibility for the PKCS#10 certificate request.

```
CES(config)# crypto server request
CES(config-request)# openSSL enable
CES(config-request)#
```

The following example disables OpenSSL compatibility.

```
CES(config-request)# no openSSL enable
CES(config-request)#
```

org-unit

Use this command to enter the organizational unit for the PKCS#10 certificate request.

Syntax

org-unit <*text*>

Parameters

text	Specifies the organizational unit of the associated gateway.

Default

None

Command mode

Certificate Request Configuration

Next command mode

Certificate Request Configuration

Related commands

crypto server request
openSSL enable

Example

The following example navigates to Certificate Request Configuration mode and specifies the organizational unit for the PKCS#10 certificate request.

```
CES(config)# crypto server request
CES(config-request)# org-unit “Manufacturing Ops”
CES(config-request)#
```

organization

Use this command to enter the organization for the PKCS#10 certificate request.

Syntax

organization <*text*>

Parameters

text	Specifies the organization of the associated gateway.

Default

None

Command mode

Certificate Request Configuration

Next command mode

Certificate Request Configuration

Related commands

crypto server request
openSSL enable

Example

The following example navigates to Certificate Request Configuration mode and specifies the organization for the PKCS#10 certificate request.

```
CES(config)# crypto server request
CES(config-request)# organization “Circular Systems, Inc.”
CES(config-request)#
```

ocsp

This command configures the OCSP status check feature.

Syntax

ocsp [ca_status_check_interval] [host *<hostname>***] [nonce] [send_request_in_server_status_check] [server_check_interval** *<0-14400>***] [timeout** *<0-14400>***]**

Parameters

ca_status_check_interval	Sets the time interval at which the CA certificate status is checked
host	Specifies the OCSP server IP address
nonce	Adds nonce in the OCSP request
send_request_in_server_status_check	Sends the OCSP request in server status check
server_check_interval	Configures the time interval at which to check the OCSP server status
timeout	Configures the timeout interval for each OCSP check

Default

None

Command mode

Crypto CA configuration mode

Next command mode

Certificate Configuration

Related commands

crl http

Example

```
CES(config)#
CES(config)#crypto ca configure "CN=ceslab001, DC=sqalab,
DC=com"
CES(config-ca)#ocsp ca_status_check_interval 14400
CES(config-ca)#
```

recover reference-number

Use this command to recover the certificate with the given reference number and authorization number.

Syntax

recover reference-number <*Word1*> **authorization-number** <*Word2*>

Parameters

Word1	Reference number.
Word2	Authorization number.

Default

None

Command mode

Server Certificate Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

revoke now

Example

```
CES(config-servercert)# recover reference-number 123456
authorization-number QABAGSNS
```

renew

Use this command to renew the certificate.

Syntax

renew {**now** | **when-days-left** <*integer*>}

Parameters

now	Renew the certificate now.
when-days-left *<integer>*	Renew the certificate the specified number of days before it expires.

Default

None

Command mode

Server Certificate Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

no crypto server certificate renew
recover
show crypto server certificate renew

Example

```
CES(config-servercert)# renew now
CES(config-servercert)# renew when-days-left 6
```

revoke now

This command revokes the current certificate.

Syntax

revoke now

Parameters

None

Default

None

Command mode

Server Certificate Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

exit
no crypto server certificate renew

Example

```
CES(config-servercert)# revoke now
CES(config-servercert)#
```

set authorization-code

This command sets or modifies the authorization code provided by the Entrust CA Server when the server creates the user.

Syntax

set authorization-code *<authorization-code>*

Parameters

authorization-code	Authorization code value.

Default

None

Command mode

CA Identity Configuration

Related commands

set key-size
set reference-number

Example

```
CES(config)# crypto ca identity 1321543 ASD-ASD-ET
CES(config-ca-identity)# set authorization-code 12354654
CES(config-ca-identity)# exit
```

set ca-default-group

This command associates a default group with the CA certificate imported.

Syntax

set ca-default-group <*group-name*>

Parameters

group-name	Specifies the group name that will, by default, be associated with the certificate imported.

Default

None

Command mode

CA Identity Configuration

Related commands

```
set key-size
set reference-number
```

Example

```
CES(config)# crypto ca identity 1321543 ASD-ASD-ET
CES(config-ca-identity)# set ca-default-group testgroup
CES(config-ca-identity)# exit
```

set issuer

This command specifies the common name with which the gateway is associated.

Syntax

set issuer <*name*> [**unit** <*org_unit*> **org** <*organization*>] [**locality** <*locality_name*> | **state** <*state_name*> | **country** <*country_name*>] | **org** <*organization*>]

Parameters

name	Issuer name. It may be the reference number.
org-unit	Name of the division within the organization.
organization	Organization name.
locality_name	Locality name.
state_name	State name.
country_name	Country name.

Default

None

Command mode

CA Identity Configuration

Related commands

set authorization-code
set reference-number

Example

```
CES(config)# crypto ca identity 1321543 ASD-ASD-ET
CES(config-ca-identity)# set issuer “CES NAME”
```

set issuer-dn

This command specifies the Certificate Management Protocol (CMP) common name with which the gateway is associated.

Syntax

set issuer-dn "CN = <*common_name*>**, OU =** <*org_unit*>**,**
O = <*organization*>**, L =** <*locality_name*>**, ST =** <*state_name*>**,**
CY = <*country_name*>**]"**

Parameters

common_name	Issuer name. It may be the reference number.
org_unit	Name of the division within the organization.
organization	Organization name.
locality_name	Locality name.
state_name	State name.
country_name	Country name. Enter two letters.

Default

None

Command mode

CA Identity Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Country cannot be more than 2 characters.
```

Related commands

set authorization-code
set port

Example

```
CES(config)# crypto ca identity
CES(ca-identity)# set issuer-dn "CN = MSCAE,
OU = Security, O = TrustCo, L = Santa Cruz, ST = CA, CY = US"
CES(ca-identity)#
```

set key-size

This command specifies the public key size (generally, larger keys are more secure).

Syntax

set key-size {**512** | **768** | **1024** | **2048** | **4096**}

Parameters

512, **768, 1024, 2048, 4096**	Public key sizes in bits (512, 768, 1024, 2048-US only, 4096)

Default

512

Command mode

CA Identity Configuration

Related commands

set authorization-code
set reference-number

Example

```
CES(config)# crypto ca identity 12312343 ASD-ASD_ASD
CES(config-ca-identity)# set key-size 512
CES(config-ca-identity)# exit
```

set port

Use this command to set the port number.

Syntax

set port <*number*>

Parameters

number	Port number from 1-65535.

Default

None

Command mode

CA Identity Configuration
Server Certificate Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

CA Identity Configuration mode:

set authorization-code

Server Configuration mode:

set subject-dn

Example

This example configures the gateway to listen on port 829 for traffic.

```
CES(config)# crypto ca identity 12312343 ASD-ASD_ASD
CES(ca-identity)# set port 829
```

This example configures the gateway to listen on port 123 for CMP traffic.

```
CES(config)# crypto server configure "CN=kb ces2,
OU=Entrust-CA, O=engeast.nortelnetworks.com"
CES(config-servercert)# set port 123
```

set reference-number

This command specifies the reference number provided by the Entrust CA Server upon the server's creation of the user.

Syntax

set reference-number <*reference-number*>

Parameters

reference-number	Reference number.

Default

None

Command mode

CA Identity Configuration

Related commands

set authorization-code
set key-size

Example

```
CES(config)# crypto ca identity 12312343 ASD-ASD_ASD
CES(config-ca-identity)# set reference-number 12354654
CES(config-ca-identity)# exit
```

set subject-dn

This command specifies the Certificate Management Protocol (CMP) subject distinguished common name with which the gateway is associated.

Syntax

set subject-dn "CN = <*common_name*>**, OU =** <*org_unit*>**,**
O = <*organization*>**, L =** <*locality_name*>**, ST =** <*state_name*>**,**
CY = <*country_name*>**]"**

Parameters

common_name	Issuer name. It may be the reference number.
org_unit	Name of the division within the organization.
organization	Organization name.
locality_name	Locality name.
state_name	State name.
country_name	Country name. Enter two letters.

Default

None

Command mode

CA Identity Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Country cannot be more than 2 characters.
```

Related commands

set authorization-code
set port

Example

```
CES(config)# crypto ca identity
CES(ca-identity)# set subject-dn "CN = J356,
OU = Corp Security, O = BCNT, L = Miami, ST = FL, CY = US"
```

show crypto ca certificates

Use this command to display information about certificates and CRLs for all CAs or for a specific CA.

Syntax

show crypto ca certificates [<*subject-DN*>]

Parameters

subject-DN	Specifies the subject distinguished name.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

crl
crl optimize
crl optional
crl update
crl search-base host port attribute
crl search-base host port bind-dn
crl search-base host port enable
crl search-base host port object-class
crl search-base host port password
crl search-base host port ssl-enable

Example

The following example displays CRL information for all CAs.

```
CES(config)# show crypto ca certificates
CA Certificate:
-----------------------------------------------------
  Subject DN    : CN=RootCA, CN=AIA, CN=Public Key Services, CN=Services,
CN=Configuration, DC=Certificates, DC=SQANetworks, DC=com
  Trusted       : ENABLED
  Enabled       : ENABLED
  Default Group : /Base
  Validity      : 10/29/2002 - 10/29/2037

CA Certificate:
-----------------------------------------------------
  Subject DN    : CN=SF1, OU=SQA-CA, O=MSCAE, L=BILLERICA, ST=MA, C=US,
mail=ACT@NORTELNETWORKS.COM
  Trusted       : ENABLED
  Enabled       : ENABLED
  Default Group : /Base/aaa/mscapi
  Validity      : 10/19/2001 - 10/19/2003

CA Certificate:
-----------------------------------------------------
  Subject DN    : OU=SQA-CA, O=entrust, C=ca
  Trusted       : DISABLED
  Enabled       : DISABLED
  Default Group : /Base/Engineering/SQA/1024 Key
  Validity      : 09/07/2000 - 09/08/2020
CES(config)#
```

The following example displays CRL information for a specific CA.

```
CES(config)# show crypto ca certificates “OU=sust_sqa1, U=third_floor,
OU=north_lab, O=lab, C=US”
Details for CA Certificate: OU=sust_sqa1, OU=third_floor, OU=north_lab, O=lab,
C=US
------------------------------------------------------------------------------
  Certificate belongs to   : lab
  Certificate was issued by: OU=sust_sqa1, OU=third_floor, OU=north_lab, O=lab,
C=US
  Certificate Serial Number: 3d178df7
  Certificate is valid     : from 06/24/2002 to 06/24/2022
  Certificate Fingerprint  : ba:63:b4:04:d6:98:e7:24:14:f4:b8:37:86:e0:5d:27
  Default Group            : /Base
Group Access Control:
  Subject Distinguished Name                                    Group Name
  Not Configured
Certificate Revocation List (CRL) Information:
  Global Crl Enabled         :  DISABLED
  Global CRL Required Enabled:  DISABLED
  Global update frequency    :  0
  Global Status              :  Not Configured
  CRL Query Optimization     :  Disabled
Certificate Revocation List (CRL) Servers:
  Enabled    Search Base            Host            Port  Enable SSL    Status
     Bind DN        Object Class     Attribute
  ------------------------------------------------------------------------------
CES(config)#
```

show crypto certificates

This command displays information about server and SSL certificates.

Syntax

show crypto [**server** | **ssl**] **certificates** [<*subject-dn*>]

Parameters

server	Display only server certificates.
ssl	Display only SSL certificates.
subject-dn	Displays details for the specific subject DN.

Default

None

Command mode

Global Configuration

Warning messages

```
% Certificate does not exist.
```

Example

The following example shows all certificates.

```
CES(config)# show crypto certificates
CES(config)#
```

show crypto enrollment

This command displays the enrollment requests that have been generated by CMP.

Syntax

show crypto enrollment [<*reference*> <*authorization-code*>]

Parameters

reference	Reference number.
authorization-code	Authorization code value.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Warning messages

```
% Enrollment request does not exist.
```

Example

```
CES(config)# show crypto enrollment
```

show crypto password

This command displays whether a crypto key storage password exists on a gateway.

Syntax

show crypto password

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

crypto password

Example

```
CES(config)# show crypto password
Key Storage Password created
```

show crypto server certificates renew

This command displays the number of days before a certificate expires that the certificate will be renewed. If you omit the renew option, this command provides information about the specified server certificate.

Syntax

show crypto server certificates <*word*> **renew**

Parameters

word	Fully distinguished name.

Default

None

Command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

renew
revoke now

Example

```
CES(config)# show crypto server certificate "CN= kb ces2,
OU=Entrust-CA, O=engeast.nortelnetworks.com" renew

The certificate will be renewed 3 days before expiration.
```

state

Use this command to enter the state for the PKCS#10 certificate request.

Syntax

state <*text*>

Parameters

text	Specifies the state of the associated gateway.

Default

None

Command mode

Certificate Request Configuration

Next command mode

Certificate Request Configuration

Related commands

crypto server request
openSSL enable

Example

The following example navigates to Certificate Request Configuration mode and specifies the state for the PKCS#10 certificate request.

```
CES(config)# crypto server request
CES(config-request)# state OH
CES(config-request)#
```

subject-dn

This command specifies, adds, or deletes a set of associations between certificates' subject DN and group.

Syntax

subject-dn [**add**] <*dn-name*> **group** <*group-name*>
no subject-dn <*dn-name*>

Parameters

dn-name	Full subject distinguished name.
group-name	Group name.

Default

None

Command mode

CA Configuration

Warning messages

```
% Group does not exist.
```

Related commands

default group

Example

```
CES(config)# crypto ca configure “OU=Entrust-CA,
O=engeast.mycompany.com”
CES(config-ca)# subject-dn add new group /Base/test
CES(config-ca)# exit
```

Chapter 19
Nortel VPN Router Stateful Firewall and NAT commands

This chapter describes Nortel VPN Router Stateful Firewall and NAT configuration commands. For the Nortel VPN Router Stateful Firewall to function, you must install the Firewall License Key.



Note: When you add or edit a firewall or NAT object in one CLI session—for example, a rule or network object—the **`show`** commands (for example, **`show netobjs`**) in another CLI session will not display the new or changed objects until you exit the configuration mode and reenter it in both CLI sessions.

Command	Page
clear flow-cache	987
firewall	988
firewall alg snmp enable	990
firewall alg virtual	991
firewall anti-spoof	993
firewall cone-nat	994
firewall connection number	995
firewall hairpin enable	997
firewall logging	998
firewall scan-detection	1001
firewall tunnel-filter	1003
firewall tunnel-management-filter	1004

Command	Page
nat-traversal	1006
netobj	1007
netobj-group	1010
policy nat	1012
policy nat enable	1014
policy nat interface	1015
policy object	1017
policy security	1019
rule (Firewall Policy Configuration)	1021
rule (NAT Policy Configuration)	1025
rule description (NAT Policy Configuration)	1029
rule service (NAT Policy Configuration)	1030
rule status (NAT Policy Configuration)	1032
service (Firewall Policy Configuration)	1034
service (NAT Policy Configuration)	1037
service-group	1038
show firewall	1040
show interfaces	1044
show netobjs	1046
show policy nat	1047
show policy security	1049
show rules (Firewall Policy Configuration)	1051
show rules (NAT Policy Configuration)	1053
show services	1055

clear flow-cache

Use this command to periodically delete flows and other data structures created by the Nortel VPN Router Stateful Firewall.

Syntax

clear flow-cache

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

firewall

Example

The following example clears the firewall/NAT flow cache.

```
CES# clear flow-cache
CES#
```

firewall

Use this command to enable the Nortel VPN Router Stateful Firewall, Nortel VPN Router packet filters, or both. Use the **no** form of the command to disable the Nortel VPN Router Stateful Firewall.

Syntax

```
firewall {contivity | policy | policy-contivity}
no firewall
```

Parameters

contivity	Enables Nortel VPN Router packet filters.
policy	Enables the Nortel VPN Router Stateful Firewall. (You must purchase a separate license to use the Nortel VPN Router Stateful Firewall.)
policy-contivity	Enables both the Nortel VPN Router Stateful Firewall and Nortel VPN Router interface packet filters.

Default

No firewall

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

To select the Nortel VPN Router Stateful Firewall, the required license must be installed.

Warning messages

```
% xxx firewall does not exist
% Contivity Stateful Firewall can only be disabled when both
Contivity Tunnel Filter and Contivity Tunnel Management
Filter are enabled
```

Related commands

filter
firewall tunnel-filter
firewall tunnel-management-filter
license
policy
show license

Example

The following example enables the Nortel VPN Router Stateful Firewall.

```
CES# configure terminal
CES(config)# firewall policy-contivity
CES(config)#
```

The following example enables both the Nortel VPN Router Stateful Firewall and Nortel VPN Router policy filters.

```
CES(config)# firewall policy-contivity
CES(config)#
```

The following example disables the Nortel VPN Router Stateful Firewall.

```
CES(config)# no firewall
CES(config)#
```

firewall alg snmp enable

Use this command to enable the NAT application level gateway (ALG). Use the **no** form of the command to disable NAT ALG.

Syntax

```
firewall alg {sip|snmp} enable
no firewall alg snmp enable
```

Parameters

sip	Enables the NAT ALG for sip.
snmp	Enables the NAT ALG for SNMP.

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show firewall alg

Example

The following example enables the application level gateway for SNMP.

```
CES# configure terminal
CES(config)# firewall alg
CES(config)#
```

The following example disables the ALG for SNMP.

```
CES(config)# no firewall alg
CES(config)#
```

firewall alg virtual

Use this command to configure the virtual application level gateway (ALG). Use the **no** form of the command to disable virtual ALG.

Syntax

firewall alg virtual {**enable|server**<*server name*>**|ip** <*ip address*>**|port** <*port number*>**|proto** <*tcp/udp*>**|port-media** <*port number*>**|port-signaling** <*port number*>
no firewall alg virtual enable

Parameters

enable	Enables the virtual ALG.
server	Sets the virtual server.
server name	String that describes the system location.
ip	IP address for the virtual server.
ip address	String that describes the system location.
port	Sets the port.
proto	Enables the TCP/UDP protocols.
port-media	Specifies the port media.
port-signaling	Specifies the port signaling.

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

`show firewall alg`

Example

The following example enables the virtual firewall ALG.

```
CES# configure terminal
CES(config)# firewall alg virtual enable
CES(config)#
```

firewall anti-spoof

Use this command to enable anti-spoofing for the Nortel VPN Router Stateful Firewall and for interface NAT. Use the **no** form of the command to disable anti-spoofing.

Syntax

```
firewall anti-spoof
no firewall anti-spoof
```

Parameters

anti-spoof	Enables or disables anti-spoofing on the gateway.

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show firewall anti-spoof

Example

The following example enables anti-spoofing for interface NAT and for the Nortel VPN Router Stateful Firewall.

```
CES# configure terminal
CES(config)# firewall anti-spoof
CES(config)#
```

The following example disables anti-spoofing.

```
CES(config)# no firewall anti-spoof
CES(config)#
```

firewall cone-nat

Use this command to enable cone-nat. Use the **no** form of the command to disable cone-nat.

Syntax

firewall cone-nat enable
no firewall cone-nat enable

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

show firewall cone-nat

Example

The following example enables cone-nat as the NAT mode on the CES.

```
CES# configure terminal
CES (config)# firewall cone-nat enable
CES (config)#
```

The following example disables cone-nat as the NAT mode on the CES.

```
CES (config)# no firewall cone-nat enable
CES (config)#
```

firewall connection number

Use this command to specify the number of devices that can be connected to the gateway for the Nortel VPN Router Stateful Firewall and interface NAT.

Syntax

`firewall connection-number` *<number>*}

Parameters

connection-number *number*	Specify the number of connections for this gateway. Each model of Nortel VPN Router has a minimum and maximum number of allowed connections.

Default

Dependent on the Nortel VPN Router model; each model has a minimum and maximum connection number.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Invalid connection number.
% Connection number has to be between xxx and xxx on this
switch!
% Connection number xxx is out of range. It should be at
least xxx
```

Related commands

show firewall connection-number

Example

The following example sets the number of connections allowed for interface NAT and for the Nortel VPN Router Stateful Firewall to 5000.

```
CES# configure terminal
CES(config)# firewall connection-number 5000
CES(config)#
```

firewall hairpin enable

Use this command to enable firewall hairpinning.Use the **no** form of the command to disable firewall hairpinning.

Syntax

firewall hairpin enable
no firewall hairpin enable

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

show status statistics security nat-stats

Example

The following example enables firewall hairpin

```
CES# configure terminal
CES(config)# firewall hairpin enable
```

firewall logging

Use this command to enable one or more types of firewall-related log entries; these entries are captured in the event log only. Use the **no** form of the command to disable the saving of specific firewall log entries.

Syntax

```
firewall logging {all | debug | firewall | nat | polmgr |
traffic | log-level {brief | detail | none | trap}}
no firewall logging {all | debug | firewall | nat | polmgr |
traffic}
```

Parameters

all	Specifies that all firewall, traffic, policy manager, and NAT entries be logged in the event log.
debug	Specifies that all debug entries be logged in the event log.
firewall	Specifies that all firewall entries be logged in the event log.
log-level	Specifies the type of information about implied rules that you want to send to the event log. Type **brief**, **detail**, **none**, or **trap**.
nat	Specifies that all NAT entries be logged in the event log.
polmgr	Specifies that all policy manager entries be logged in the event log.
traffic	Specifies that all traffic entries be logged in the event log.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The specified firewall must be available.

Related commands

policy
show firewall logging

Example

The following example configures the gateway to log NAT and traffic entries in the event log.

```
CES# configure terminal
CES(config)# firewall logging nat
CES(config)# firewall logging traffic
CES(config)#
```

The following example configures the gateway to stop logging all types of firewall entries in the event log.

```
CES(config)# no firewall logging all
CES(config)#
```

The following example configures the gateway to log trap information about implied rules in the event log.

```
CES(config)# firewall logging log-level trap
```

firewall scan-detection

Use this command to configure scan detection on the gateway. When scan detection is enabled, some types of malicious network traffic are detected and logged before the traffic passes through the firewall. This traffic is logged to the security log with a medium severity level and persistent flags set. Use the **no** form of the command to disable scan detection.

Syntax

```
firewall scan-detection [interval <minutes> |
threshold-network <hosts> | threshold-port <ports>]
no firewall scan-detection
```

Parameters

interval	Specify the interval over which the number of port scans or host scans will be inspected. If the number of scans exceeds the configured threshold during this interval, the scan is logged in the security log.
minutes	Specifies the number of minutes in the inspection interval. Type an integer from 1 through 60.
threshold-network	Specify the number of hosts on the private side to which an attacking machine must send scan packets during the inspection interval to trigger an event in the security log.
hosts	Specifies the number of hosts that must be scanned during the inspection interval. Type an integer from 1 through 10000.
threshold-port	Specify the number of ports on one host on the private side to which an attacking machine must send scan packets during the inspection interval to trigger an event in the security log.
ports	Specifies the number of ports that must be scanned during the inspection interval. Type an integer from 1 through 10000.

Default

Detection interval: 10 minutes
Port scan threshold: 50
Network scan threshold: 20

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The Nortel VPN Router Stateful Firewall must be enabled.

Related commands

firewall
show firewall scan-detection

Example

The following example configures the gateway to trigger an event in the security log if 100 port scans are detected over a 5-minute interval.

```
CES# configure terminal
CES(config)# firewall scan-detection port-threshold 100
CES(config)# firewall scan-detection interval 5
CES(config)#
```

The following example disables scan detection on the gateway.

```
CES(config)# no firewall scan-detection
CES(config)#
```

firewall tunnel-filter

Use this command to enable Nortel VPN Router tunnel filters when the Nortel VPN Router Stateful Firewall is already enabled. If the Nortel VPN Router Stateful Firewall is not enabled, you cannot disable tunnel filters. In general, you use the tunnel filters while you migrate to the Nortel VPN Router Stateful Firewall.

After you create and test the new policies for the Nortel VPN Router Stateful Firewall, you can disable tunnel filters using the **no** form of the command. You can disable tunnel filters only when the Nortel VPN Router Stateful Firewall is enabled.

Syntax

```
firewall tunnel-filter
no firewall tunnel-filter
```

Parameters

None

Default

Enabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

filter
policy
show firewall tunnel-filter

Example

The following example enables tunnel filtering on a gateway that has the Nortel VPN Router Stateful Firewall enabled.

```
CES# configure terminal
CES(config)# firewall tunnel-filter
CES(config)#
```

The following example disables tunnel filtering on a gateway that has the Nortel VPN Router Stateful Firewall enabled.

```
CES(config)# no firewall tunnel-filter
CES(config)#
```

firewall tunnel-management-filter

Use this command to enable Nortel VPN Router tunnel filters for management traffic when the Nortel VPN Router Stateful Firewall is already enabled. (Management traffic is any traffic that has the Nortel VPN Router management IP address as the source or destination address.) If the Nortel VPN Router Stateful

Firewall is not enabled, you cannot disable tunnel management filters. Use the **no** form of the command to disable tunnel filters for management traffic. You can disable tunnel filters for management traffic only when the Nortel VPN Router Stateful Firewall is enabled.

Syntax

```
firewall tunnel-management-filter
no firewall tunnel-management-filter
```

Parameters

None

Default

Enabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
filter
policy
show firewall tunnel-management-filter
```

Example

The following example enables tunnel management filtering on a gateway that has the Nortel VPN Router Stateful Firewall enabled.

```
CES# configure terminal
CES(config)# firewall tunnel-management-filter
CES(config)#
```

The following example disables tunnel management filtering on a gateway that has the Nortel VPN Router Stateful Firewall enabled.

```
CES(config)# no firewall tunnel-management-filter
CES(config)#
```

nat-traversal

This command configures IPsec NAT traversal on branch office tunnels. Use the no form of the command to disable NAT traversal.

Syntax

```
nat-traversal <draft|rfc> keepalive <hh:mm:ss>
no nat-traversal
```

Parameters

draft

draft	Enables the draft mode of NAT traversal.
rfc	Enables the RFC mode of NAT traversal.
keepalive <hh:mm:ss>	Configures the interval when keepalive messages transmit to the NAT device.

Default

Disable

Command mode

Branch Office Group IPsec Configuration

Next command mode

Branch Office Group IPsec Configuration

Required privileges

System Management – Manage

User Management – None

Prerequisites

You must globally enable NAT traversal before you can configure it on a branch office tunnel.

Example

```
CES(config-bo_group/ipsec)#nat-traversal rfc keepalive
02:30:00
```

netobj

Use this command to add, edit, or delete a network object or network object group for the user scope in the Nortel VPN Router Stateful Firewall. Network objects of master scope are created dynamically; you cannot edit or delete them. Use the **no** form of the command to delete the network object.

Syntax

netobj [**add**] <*name*> {**host** <*ip-address*> | **ip-range** <*ip-address1*> <*ip-address2*> | **network** <*IP-address*>/<*mask*>}

netobj add <*name*> **group**

netobj <*name*> **description**

no netobj <*name*>



Note: When you use this command to create a network object, you can use the **NOT** operand to define an IP range or network that you want to exclude from using NAT. For an example of how to use the **NOT** operand, see "Example: Using the NOT operand to configure NAT" on page 1058.

Parameters

add	Create a new network object or group of network objects for the user scope, which can be assigned to policy rules.
name	Specifies the name of the network object or object group to be created or edited.
host	Designate the IP address of a network host as the network object.
ip-range	Designate a range of IP addresses as the network object. Type a start IP address and an ending IP address.
network	Designate a network as the network object. Type a network address and a mask, for example, 2.2.2.2/24.
description	Specify a text description of the network object. If you enter a string with spaces, enclose the string in quotation marks.
group	Create a network object group. You can only use this parameter with the keyword **add**, for example, **netobj add newobjgroup group**.

Default

None

Command mode

Policy Object Configuration

Next command mode

Policy Object Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Policy object does not exist
% Policy object already exists
```

Related commands

netobj-group
service
service-group
show netobjs

Example

The following example creates a network object called “test1” that is a host.

```
CES# config terminal
CES(config)# policy object
CES(config-policyobj)# netobj add test1 host 10.0.10.123
```

The following example edits the network object “test2” so that it designates a range of IP addresses.

```
CES(config-policyobj)# netobj test2 ip-range 10.0.0.1
10.0.0.50
CES(config-policyobj)#
```

The following example edits the network object “test3” so that it designates a network.

```
CES(config-policyobj)# netobj test3 network 10.23.0.0/16
CES(config-policyobj)#
```

The following example creates the network object group “testgroup.”

```
CES(config-policyobj)# netobj add testgroup group
CES(config-policyobj)#
```

The following example deletes the network object “test4.”

```
CES(config-policyobj)# no netobj test4
```

netobj-group

Use this command to add, edit, or delete a network object in a network object group for the user scope in the Nortel VPN Router Stateful Firewall. Network object groups of master scope are created dynamically; you cannot edit or delete them. Use the **no** form of the command to delete one or more network objects from a network object group.

Syntax

netobj-group <*netobj-group-name*> **add** <*netobj-name1*> [<*netobj-name2*> . . .]

netobj-group <*netobj-group-name*> **description** <*text*>

no netobj-group <*netobj-group-name*> <*netobj-name1*> [<*netobj-name2*> . . .]

Parameters

netobj-group-name	Specifies the name of the network object group that you are editing.
add	Add one or more network objects to the specified group.
description	Specify a text description of the network object group. If you enter a string with spaces, enclose the string in quotation marks.
netobj-name	Specifies one or more network objects to be added to or deleted from the specified network object group.

Default

None

Command mode

Policy Object Configuration

Next command mode

Policy Object Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Netobj xxx is read-only
% Netobj xxx does not exist
% Netobj xxx is not a group
% Netobj xxx already exists in group yyy
% Netobj xxx does not exist in group yyy
```

Related commands

netobj
service
service-group
show netobjs

Example

The following example adds two network objects called “test1” and “test2” to the network object group “testgroup.”

```
CES# config terminal
CES(config)# policy object
CES(config-policyobj)# netobj-group testgroup add test1
test2
CES(config-policyobj)#
```

The following example adds a text description to the network object group “testgroup.”

```
CES(config)# policy object
CES(config-policyobj)# netobj-group testgroup description
“This group is for NAT policy clmt3”
CES(config-policyobj)#
```

The following example deletes the network object “test4” from the network object group “testgroup” and then deletes the group “testgroup” itself.

```
CES(config-policyobj)# no netobj-group testgroup test4
CES(config-policyobj)# no netobj testgroup
CES(config-policyobj)#
```

policy nat

Use this command to create a NAT policy for the gateway and to navigate to NAT Policy Configuration mode. Use the **no** form of the command to delete a NAT policy.

Syntax

```
policy nat [add] <policy-name>
no policy nat <policy-name>
```

Parameters

add	Create a new NAT policy.
natname	Specifies the name of the NAT policy to create or edit.

Default

None

Command mode

Global Configuration

Next command mode

NAT Policy Configuration (when you enter the name of an existing policy)
Global Configuration (when you create or delete a policy)

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Policy does not exist
% Policy already exists
```

Related commands

policy object
policy security
rule
show policy nat

Example

The following example creates a NAT policy called “natpol2.”

```
CES# config terminal
CES(config)# policy nat add natpol2
CES(config)#
```

The following example navigates to NAT Policy Configuration mode to edit NAT policy “natpol2.”

```
CES(config)# policy nat natpol2
CES(config-natpolicy)#
```

The following example deletes NAT policy “natpol2.”

```
CES(config)# no policy nat natpol2
CES(config)#
```

policy nat enable

Enables operation of a NAT on a Nortel VPN Router gateway. Use the **no** form of this command to disable a NAT.

Syntax

[**no**] **policy nat enable**

Parameters

None

Default

Disabled

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management – Manage
User Management – None

Example

Example of a successful enabling of a NAT on a CES.

```
CES(config)# policy nat enable
```

Example of a successful disabling of a NAT on a CES.

```
CES(config)# no policy nat enable
```

policy nat interface

Use this command to assign a NAT policy to an interface and to enable NAT on the interface. Use the **no** form of the command to remove the NAT policy from the interface or to disable NAT on the interface.

Syntax

```
policy nat interface {assign <natpolicyname> | enable}
no policy nat interface {assign | enable}
```

Parameters

enable	Enables NAT on Nortel VPN Router interfaces.
assign	Specify a NAT policy for interface NAT.
natname	Specifies the name of the NAT policy to assign to interfaces.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% NAT set xxx does not exist!
% Interface NAT is already enabled!
% Interface NAT is already disabled!
```

Related commands

policy security
policy nat

Example

The following example enables NAT on non-tunneled interfaces that route traffic through the gateway.

```
CES# configure terminal
CES(config)# policy nat interface enable
CES(config)#
```

The following example assigns the NAT policy mynatset to non-tunneled interfaces on the gateway.

```
CES(config)# policy nat interface assign mynatset
CES(config)#
```

The following example disables NAT on non-tunneled interfaces.

```
CES(config)# no policy nat interface enable
CES(config)#
```

policy object

Use this command to change the mode from Global Configuration mode to Policy Object Configuration Mode to configure network and service objects.

Syntax

policy object

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Policy Object Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

netobj
netobj-group
service
service-group
show netobjs
show services

Example

The following example navigates the command line interface in Policy Object Configuration mode.

```
CES# config terminal
CES(config)# policy object
CES(config-policyobj)#
```

policy security

Use this command to perform the following tasks:

- Create a new firewall policy.
- Assign a specific policy to the gateway as a whole.
- Enter Firewall Policy Configuration mode to create or edit rules for the specified policy.

Use the **no** form of the command to delete the specified policy from the gateway.

Syntax

```
policy security [add | assign] <policy-name>
no policy security <policy-name>
```

Parameters

add	Create a new policy for the Nortel VPN Router Stateful Firewall.
assign	Specify the policy to be used for the firewall.
policy-name	Specifies the name of the policy that you are creating, editing, or assigning to the firewall.

Default

None

Command mode

Global Configuration

Next command mode

Firewall Policy Configuration (when you edit an existing policy)
Global Configuration (when you create a policy, assign the policy, or delete it)

Required privileges

System Management – Manage
User Management – None

Prerequisites

The Nortel VPN Router Stateful Firewall must be enabled on the gateway.

Warning messages

```
% Policy does not exist
% Policy already exists
% Policy is in use and cannot be deleted
```

Related commands

firewall
filter
policy nat
policy object
rule
show policy security

Example

The following example creates a firewall policy called “fwpol2.”

```
CES# config terminal
CES(config)# policy security add fwpol2
CES(config)#
```

The following example navigates to Firewall Policy Configuration mode to edit firewall policy “fwpol2.”

```
CES(config)# policy security fwpol2
CES(config-fwpolicy)#
```

The following example assigns the policy “fwpol2” to the Nortel VPN Router Stateful Firewall. This policy will be active on the gateway after you reboot.

```
CES(config)# policy security assign fwpol2
CES(config)#
```

The following example deletes firewall policy “fwpol2.”

```
CES(config-fwpolicy)# exit
CES(config)# no policy security fwpol2
CES(config)#
```

rule (Firewall Policy Configuration)

Use this command to add or edit a rule for the specified firewall policy. When you create a rule, the software adds the new rule to the top of the rule group. You cannot use the command line interface to reorder rules; you must create them in the order that you want them to be examined. For more information about rule parameters, see *Nortel VPN Router Security — Firewalls, Filters, NAT, and QoS*.

Syntax

```
rule {default| override | interface <interface-name>
{destination | source}} {add | <rule-number>}
[action {accept | drop | reject | user-auth {any |
<user-group-name>}]
[dst-address <network-object1> [<network-object2> ...]]
[dst-interface {any | branch:any | system | trusted |
tunnel:any | untrusted | user:any}]
[log {brief | detail | none | trap}]
[remark <text>]
[service <service-name1> [<service-name2> ...]] [src-address
<network-object1> [<network-object2> ...]]
[src-interface {any | branch:any | system | trusted |
tunnel:any | untrusted | user:any}]
[status {disable | enable}]

no rule {default | override | interface <interface-name>
{source | destination}} <rule-number>
```

Parameters

default	Add or edit a default rule.
override	Add or edit an override rule.
interface	Add or edit an interface rule.
interface-name	Specifies the interface name that will match the interface rule that you are configuring. (To see the names of the interfaces, use the **show interfaces** command at the Firewall Policy Configuration prompt.)
destination	Specify that this rule matches the designated interface when the interface is the packet destination.
source	Specify that this rule matches the designated interface when the interface is the packet source.
add	Create a new rule for this policy.
rule-number	Specifies the rule number; type an integer from 1 through 1000. (To see the rule numbers, use the **show rules** command at the Firewall Policy Configuration prompt.)
action	Specify the action that should take place when a packet matches this firewall policy rule.
accept	Accept packets that match this rule.
drop	Drop packets that match this rule.
reject	Drop packets that match this rule and send a rejection message to the source of the packet.
user-auth	Authenticate users for packets that match this rule. Type **user-auth any** (all users must be authenticated) or type the user group name.
dst-address	Specify the destination address that matches this rule. Type one or more network object names. (To see the network object names, use the **show netobjs** command at the Firewall Policy Configuration prompt.)
dst-interface	Specify the destination interface that matches this rule. Type **any**, **branch:any**, **system**, **trusted**, **tunnel:any**, **untrusted**, or **user:any**. If you are configuring a source interface rule, you can also use the prefix **tunnel:** for user groups and the prefix **bo_tunnel:** for branch office tunnels. You cannot use this parameter for destination interface rules.

src-address	Specify the source address that matches this rule. Type one or more network object names. (To see the network object names, use the **show netobjs** command at the Firewall Policy Configuration prompt.)
src-interface	Specify the source interface that matches this rule. Type **any**, **branch:any**, **system**, **trusted**, **tunnel:any**, **untrusted**, or **user:any**. You cannot use this parameter for source interface rules.
service	Specify the service that matches the firewall policy rule. Type **any** or one or more service object names. (To see the service object names, use the **show services** command at the Firewall Policy Configuration prompt.)
log	Specify the level of event logging. Type **none**, **brief**, **detail**, or **trap**. (The level **trap** is the same as **detail**, but also enables SNMP traps on a rule match.)
remark	Specify a text description for the rule. If the text contains spaces, enclose it in quotation marks.
status	Enable or disable this rule. (Type **disable** or **enable**.) By default, a rule is enabled when you create it.

Default

For newly created rules, the default action is **drop**. The firewall determines the default interface by the type of rule group to which it belongs. In an interface policy, either source interface or destination interface has a default value that you cannot change. The default settings of other fields are **any**.

Command mode

Firewall Policy Configuration

Next command mode

Firewall Policy Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Rule xxx does not exist
% Invalid interface name.
% Invalid network address.
% Invalid service name.
% Invalid number of arguments.
```

Related commands

netobj
netobj-group
policy security
service
service-group
show rules

Example

The following example edits override rule 3.

```
CES(config)# policy security fwtest
CES(config-fwpolicy)# rule override 3 src-interface
untrusted src-address 192.32.0.0 dst-address 192.32.240.11
service ftp action accept log brief remark "This is for test"
```

The following example creates a source interface rule.

```
CES(config-fwpolicy)# rule interface "Tunnel:/Base/myTunnel"
source add dst-address 192.32.240.11 service ftp action
accept log brief remark "This is for test"
```

The following example edits source interface rule 3.

```
CES(config-fwpolicy)# rule interface "Tunnel:/Base/myTunnel"
source 3 dst-address 192.32.240.12 service ftp action accept
log detail
```

The following example edits default rule 3.

```
CES(config-fwpolicy)# rule default 3 src-address 192.32.0.0
service ftp action accept
```

The following example deletes destination interface rule 3 and override rule 3.

```
CES(config-fwpolicy)# no rule interface "Tunnel:/Base/
myTunnel" destination 3
CES(config-fwpolicy)# no rule override 3
```

rule (NAT Policy Configuration)

Use this command to create or edit a NAT rule in the current NAT set.



Note: On the Nortel VPN Router, NAT definitions are named collections of NAT rules. These names, or *NAT sets*, can then be used when configuring branch office connections

Syntax

```
rule {add | <rule-number>} action {static | proxy | pooled |
port} source {any | <netobj>} destination {any | <netobj>}
translated-source <netobj>

rule {add | <rule-number>} action port-fwd
source {any | <netobj>} destination {any | <netobj>}
translated-destination <netobj>

rule {add | <rule-number>} action none
source {any | <netobj>} destination {any | <netobj>}

no rule <rule-number>
```

Parameters

add	Create a new rule for this NAT policy.
rule-number	Specifies the rule number; type an integer from 1 through 1000. (To see the rule numbers, use the **show rules** command at the NAT Policy Configuration prompt.)
action	Specify the action that should take place when this NAT policy rule is applied.
none	Do nothing to packets that match this rule.
pooled	Map an internal address to the next available address in the NAT address pool.
port	Map internal addresses to one external address by dynamically assigning ports to distinguish the internal addresses one from the other.
port-fwd	Forward incoming requests from one external address to many internal addresses based on the protocol port used (for example, FTP generally uses port 21).
static	Map an internal address range to a specific external address range.
proxy	Action type is proxy translate.
source	Specify the source address that matches this rule. Type **any** or type one or more network object names. (To see network object names, use the **show netobjs** command at the NAT Policy Configuration prompt.)
destination	Specify the destination address that matches this rule. Type **any** or type one or more network object names. (To see network object names, use the **show netobjs** command at the NAT Policy Configuration prompt.)

translated-destination	Specify the translated destination addresses for internal addresses that match this rule. Type a network object name that represents a single address or a range of addresses. (To see network object names, use the **show netobjs** command at the NAT Policy Configuration prompt.)
translated-source	Specify the translated source addresses for internal addresses that match this rule. Type a network object name that represents a single address or a range of addresses. (To see network object names, use the **show netobjs** command at the NAT Policy Configuration prompt.)

Default

None

Command mode

NAT Policy Configuration

Next command mode

NAT Policy Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Invalid address.
% NAT rule xxx does not exist.
% NAT rule xxx already exists.
```

Related commands

netobj
netobj-group
policy nat
service
service-group
show rules

Example

The following example creates a NAT rule for static translation.

```
CES(config)# policy nat testnat100
CES(config-natpolicy)# rule add action static source manu1
destination mainplant translated-source outaddresses
CES(config-natpolicy)#
```

The following example creates a NAT rule for pooled translation.

```
CES(config-natpolicy)# rule add action pooled source billing
destination backoffice translated-source
CES(config-natpolicy)#
```

The following example edits NAT rule 1 for port forwarding translation.

```
CES(config-natpolicy)# rule 1 action port-fwd source any
destination http translated-destination http_server
CES(config-natpolicy)#
```

The following example deletes NAT rule 2 from the policy.

```
CES(config-natpolicy)# no rule 2
CES(config-natpolicy)#
```

rule description (NAT Policy Configuration)

Use this command to type a text description for a NAT policy rule. To delete descriptive text from a rule, execute the command as follows:
`rule 1 description " "` (enter a space between the quotation marks).

Syntax

`rule` <*`rule-number`*> **`description`** <*`text`*>

Parameters

rule-number	Specifies the rule that you want to edit in the NAT policy. (To see NAT rule numbers, enter the **show rules** command at the NAT Policy Configuration prompt.)
text	Specifies an alphanumeric description of the rule in the NAT policy. If you enter a string with spaces, enclose the string in quotation marks. To remove the text, execute the command with the argument **description " "** (enter a space between the quotation marks).

Default

None

Command mode

NAT Policy Configuration

Next command mode

NAT Policy Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show policy nat

Example

The following example creates a description for the first rule of NAT policy "test1."

```
CES(config)# policy nat test1
CES(config-natpolicy)# rule 1 description "First rule in my
NAT policy"
CES(config-natpolicy)#
```

rule service (NAT Policy Configuration)

Use this command to attach a specified service or service group to a NAT rule. Use the **no** form of the command to detach the service or service group from the NAT rule.

Syntax

rule <*rule-number*> **service** {<*service-name*> | <*service-group-name*>}
no rule rule-number service {<*service-name*> | <*service-group-name*>}

Parameters

rule-number	Specifies the rule that you want to edit in the NAT policy. (To see NAT rule numbers, enter the **show rules** command at the NAT Policy Configuration prompt.)
service-name	Specifies the name of the service object that you want to associate with this NAT rule. (To see NAT service objects, enter the **show services** command at the NAT Policy Configuration prompt.)
service-group-name	Specifies the name of the service group object that you want to associate with this NAT rule. (To see NAT service object groups, enter the **show services group** command at the NAT Policy Configuration prompt.)

Default

None

Command mode

NAT Policy Configuration

Next command mode

NAT Policy Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% NAT rule xxx does not exist
% service does not exist
```

Related commands

show policy nat

Example

The following example attaches service object test1 to NAT rule 3.

```
CES(config)# policy nat testnat100
CES(config-natpolicy)# rule 3 service test1
CES(config-natpolicy)#
```

The following example detaches service group testgroup2 from NAT rule 2.

```
CES(config-natpolicy)# no rule 2 service testgroup2
CES(config-natpolicy)#
```

rule status (NAT Policy Configuration)

Use this command to enable a NAT rule. Use the **no** form of the command to disable the NAT rule.

Syntax

rule <*rule-number*> **status enable**
no rule <*rule-number*> **status enable**

Parameters

rule-number	Specifies the rule that you want to enable or disable. (To see NAT rule numbers, enter the **show rules** command at the NAT Policy Configuration prompt.)

Default

None

Command mode

NAT Policy Configuration

Next command mode

NAT Policy Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% NAT rule xxx does not exist
```

Related commands

show policy nat

Example

The following example disables NAT rule 3.

```
CES(config)# policy nat testnat
CES(config-natpolicy)# no rule 3 status enable
CES(config-natpolicy)#
```

The following example reenables NAT rule 3.

```
CES(config-natpolicy)# rule 3 status enable
CES(config-natpolicy)#
```

service (Firewall Policy Configuration)

Use this command to add, edit, or delete a service object or service object group for the user scope in the Nortel VPN Router Stateful Firewall. Service objects of master scope are created dynamically; you cannot edit or delete them. Use the **no** form of the command to delete the service object.

Syntax

```
service [add] <name> icmp [code {<num> | any} | code-range
<num1 num2>] [type {<num> | any}]

service [add] <name> ip protocol-num <num>

service [add] <name> {tcp | udp} {port-num <num> |
port-range <num1 num2>}

service add <name> group

service <name> description

no service <name>
```

Parameters

add	Create a new service object or group of service objects for the user scope that can be assigned to policy rules.
name	Specifies the name of the service object or object group to be created or edited.
icmp	Designate the ICMP protocol as the service object.
code	Specify an ICMP code number as the service object. Type a number from 0 through 255 or type **any**.
code-range	Specify a range of ICMP code numbers as the service object. Type two numbers from 0 through 255.
type	Specify an ICMP type number as the service object. Type a number from 0 through 255 or type **any**.
ip protocol-num	Specify an IP protocol number as the service object. Type a number from 0 through 255.

tcp	Specify a TCP port number or port number range as the service object.
udp	Specify a UDP port number or port number range as the service object.
port-num	Specify the TCP or UDP port number as the service object. Type a number from 0 through 65535.
port-range	Specify a TCP or UDP port number range as the service object. Type two numbers from 0 through 65535.
description	Specify a text description of the service object. If you enter a string with spaces, enclose the string in quotation marks.
group	Create a service object group. You can use this parameter only with the keyword **add**, for example, **service add servicegroup1 group**.

Default

None

Command mode

Policy Object Configuration

Next command mode

Policy Object Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Service xxx does not exist
% Service xxx already exists
```

Related commands

netobj
service-group
show services

Example

The following example creates a service object called “test1” for ICMP code range 45-50 with ICMP type 23.

```
CES# config terminal
CES(config)# policy object
CES(config-policyobj)# service add test1 icmp code 45 50
type 23
CES(config-policyobj)#
```

The following example creates a service object called “servtcp” for TCP port number 111.

```
CES(config-policyobj)# service add servtcp tcp 111
CES(config-policyobj)#
```

The following example edits the service object “test3” so that it designates IP protocol 10.

```
CES(config-policyobj)# service test3 ip protocol-num 10
CES(config-policyobj)#
```

The following example creates the service object group “testservgroup.”

```
CES(config-policyobj)# service add testservgroup group
CES(config-policyobj)#
```

The following example deletes the service object “test3.”

```
CES(config-policyobj)# no service test4
CES(config-policyobj)#
```

service (NAT Policy Configuration)

Use this command to add and specify a service, or to edit a service in a NAT policy rule.

Syntax

```
service add name
{tcp { port-num num | port-range num1 num2 }|
udp { port-num num | port-range num1 num2 }|
ip protocol-num num |
icmp { type-num num | any} | code-num num | any} |
   code-range num1 num2} | group}

service name
{tcp { port-num num | port-range num1 num2 }|
udp { port-num num | port-range num1 num2 }|
ip protocol-num num |
icmp { type-num num | any} | code-num num | any} |
   code-range num1 num2 } | group}
```

Parameters

name	Specifies name of service object
num	Specifies port number
num1	Specifies a minimum port number in a range
num2	Specifies a maximum port number in a range

Default

None

Command Mode

NAT Policy Configuration Mode

Next Command Mode

NAT Policy Configuration Mode

Required Privileges

System Management – Manage
User Management – None

Example

Example of a successful service configuration:

```
CES(config-natpolicy)# rule number service add foo ip
protocol-num 1211
```

service-group

Use this command to add, edit, or delete a service object in a service object group. Service object groups of master scope are created dynamically; you cannot edit or delete them. Use the **no** form of the command to delete one or more service objects from a service object group.

Syntax

```
service-group <service-group-name> add <service-name1>
[<service-name2> . . .]

service-group <service-group-name> description <text>

no service-group <service-group-name> <service-name1>
[<service-name2> . . .]
```

Parameters

service-group-name	Specifies the name of the service object group that you are editing.
add	Add one or more service objects to the specified group.
description	Specify a text description of the service object group. If you enter a string with spaces, enclose the string in quotation marks.
service-name	Specifies one or more service objects to be added to or deleted from the specified service object group.

Default

None

Command mode

Policy Object Configuration

Next command mode

Policy Object Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Service xxx is read-only
% Service xxx does not exist
% Service xxx is not a group
% Service xxx already exists in group yyy
% Service xxx does not exist in group yyy
```

Related commands

netobj
netobj-group
service
show services

Example

The following example adds two service objects called “test1” and “test2” to the service object group “testgroup.”

```
CES# config terminal
CES(config)# policy object
CES(config-policyobj)# service-group testgroup add test1
test2
CES(config-policyobj)#
```

The following example adds a text description to the service object group “testgroup.”

```
CES(config)# policy object
CES(config-policyobj)# service-group testgroup description
“This service group is for NAT policy clmt3”
CES(config-policyobj)#
```

The following example deletes the service object “test4” from the service object group “testgroup” and then deletes the group “testgroup” itself.

```
CES(config-policyobj)# no service-group testgroup test4
CES(config-policyobj)# no service testgroup
CES(config-policyobj)#
```

show firewall

Use this command to display all available firewall types or the firewall that is currently in use. It can also display firewall logging information.

Syntax

```
show firewall {alg | all | anti-spoof | connection-number |
enabled | logging | scan-detection | tunnel-filter |
tunnel-management-filter| hairpinning }
```

Parameters

alg	Display the state of firewall/NAT application level gateways (ALGs), either enabled or disabled.
all	Display all available firewall types: policy-based firewall, Nortel VPN Router Stateful Firewall, or policy and Nortel VPN Router Stateful Firewall, which can co-exist.
anti-spoof	Display the status of anti-spoofing, either enabled or disabled.
connection-number	Display the configured connection number and the minimum number for this gateway.
enabled	Display which types of firewall are enabled, if any.
logging	Display the state of each firewall logging type (traffic, policy manager, firewall, NAT, or debug), either disabled or enabled.
scan-detection	Display the status and configuration of firewall scan detection.
tunnel-filter	Display the status of tunnel filters: enabled or disabled.
tunnel-management-filter	Display the status of tunnel management filters: enabled or disabled.
hairpinning	Display the status of firewall hairpinning: enabled or disabled.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

firewall
policy security

Example

The following example displays the status of firewall ALGs.

```
CES(config)# show firewall alg
Firewall Application Level Gateways
  SNMP: Enabled
```

The following example displays the status of firewall ALGs.

```
CES(config)# show firewall anti-spoof
Anti-spoofing is disabled
```

The following example displays which types of firewall are enabled.

```
CES(config)# show firewall enabled
Nortel VPN Router Stateful Firewall enabled
```

The following example displays the status of firewall logging.

```
CES(config)# show firewall logging
Logging Type        Status

All     :           Disabled
Traffic :           Disabled
Polmgr  :           Disabled
Firewall:           Disabled
NAT     :           Disabled
Debug   :           Disabled
```

The following example displays the status of the firewall tunnel management filter.

```
CES(config)# show firewall tunnel-management-filter
Tunnel Management Filter is enabled
CES(config)#
```

show interfaces

Use this command to display the interfaces that you can use to define a policy or policy rule.

Syntax

```
show interfaces [all | bo_tunnel | physical | tunnel]
```

Parameters

all	Display all available interfaces on the gateway.
bo_tunnel	Display a list of branch office tunnel interfaces on the gateway.
physical	Display all available physical interfaces on the gateway.
tunnel	Display a list of tunnel interfaces on the gateway.

Default

None

Command mode

Firewall Policy Configuration

Next command mode

Firewall Policy Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

show netobjs
show rules
show services

Example

The following example displays all interfaces available for firewall rules.

```
CES(config)# policy security testpolicy
CES(config-fwpolicy)# show interfaces
Physical Interfaces
  any
  system
  trusted
  untrusted
  tunnel:any
  user:any
  branch:any
  clip
  slot 3 interface 1   (12.0.0.4)
  slot 1 interface 1   (15.0.0.2)
  lan   (47.17.249.228)
  lan   (47.17.249.229)
  slot 7 interface 1
Branch Office Tunnels
  bo-tunnel:/Base/CES3 to CES1
  bo-tunnel:/Base/CES3 to CES2
User Groups
  tunnel:/Base
  tunnel:/Base/Control Tunnels
CES(config-fwpolicy)#
```

The following example displays all branch office tunnel interfaces available for firewall rules.

```
CES(config-fwpolicy)# show interfaces bo_tunnel
Branch Office Tunnels
  bo-tunnel:/Base/CES3 to CES1
  bo-tunnel:/Base/CES3 to CES2
CES(config-fwpolicy)#
```

show netobjs

Use this command to display the configured network objects and network object groups that you can use for firewall and NAT policies.

Syntax

show netobjs [**group** | **host** | **ip-range** | **network**]

Parameters

group	Restrict the display of network objects to groups.
host	Restrict the display of network objects to hosts.
ip-range	Restrict the display of network objects to IP address ranges.
network	Restrict the display of network objects to networks.

Default

None

Command mode

Firewall Policy Configuration
NAT Policy Configuration
Policy Object Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

netobj

Example

The following example displays network objects at Policy Object Configuration mode.

```
CES(config)# policy object
CES(config-policyobj)# show netobjs

 PublicInterface
  type            : host
  ip address      : 192.33.37.45

 mynetwork
  type            : network
  subnet          : 2.2.2.2
  mask            : 255.0.0.0
  description     : None

 anothernewtestobject
  type            : netobjgroup
  members
                  : mynetwork
  description     : None

 2range
  type            : ip_range
  start address   : 2.2.2.2
  end address     : 2.2.2.4
CES(config-policyobj)#
```

show policy nat

Use this command to display all available NAT sets on the gateway. Include the **interface** option to display information about interface NAT.

Syntax

show policy nat [**interface**] [**enabled**]

Parameters

enabled	Display only enabled NAT sets or interface NAT sets.
interface	Display the status of interface NAT (enabled or disabled).

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

policy nat
policy nat interface

Example

The following example lists NAT policies on the gateway.

```
CES(config)# show policy nat
NAT Policies
  ChesterBranchNAT
  ChesterBranchNAT2
  ChesterBranchNATwithFWD
  ChesterBranchNATwithMAP
CES(config)#
```

show policy security

Use this command to display all configured firewall policies or the policy currently in use.

Syntax

show policy security [**all** | **enabled**]

Parameters

all	Display a list of all configured firewall policies.
enabled	Display the name of the firewall policy currently in use.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

policy security
show firewall

Example

The following example displays all configured firewall policies.

```
CES(config)# show policy security
Security Policies
  System Default (read-only) (applied)
  myfirewallpol
  mynewpol
CES(config)#
```

The following example displays the applied firewall policy.

```
CES(config)# show policy security enabled
Enabled Security Policy
CO3ALA
CES(config)#
```

show rules (Firewall Policy Configuration)

Use this command to display all configured rules for firewall policies. The displayed rules are ordered by number.

Syntax

show rules [**all** | **default** | **implied** | **interface** | **override**]

Parameters

all	Display all of the rules in the policy.
default	Display all rules in the default rule set.
implied	Display read-only implied rules.
interface	Display the rules in the interface rule set.
override	Display all rules in the override rule set.

Default

None

Command mode

Firewall Policy Configuration

Next command mode

Firewall Policy Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

rule

Example

The following example displays firewall and NAT policy rules.

```
CES(config-fwpolicy)# show rules
Implied Rules
  rule_number           : 1
  src-interface         : system
  dst-interface         : trusted
  src-address           : "_MngtIP"
  action                : accept
  status                : enable
  log                   :
  remark                :

  rule_number           : 2
  src-interface         : tunnel:any
  dst-interface         : system
  dst-address           : "_MngtIP"
  action                : accept
  status                : enable
  log                   :
  remark                :

rule_number        : 4
 src-interface      : private
 dst-interface      : sysprivate
 service               : "tcp8000" "l2xservicegroup"
"pptpservicegroup" "icmpse
vicegroup" "ipsecservicegroup"
 action           : accept
 status           : enable
 log              :
 remark               :  Allow/Deny services to come in from
any private interfaces and terminated at any private
interfaces
```

```
Override Rules
  None

Src-interface Rules
  None

Dst-interface Rules
  None

Default Rules
  None

Post-implied Rules
  rule_number          : 1
  src-interface        : any
  dst-interface        : any
  action               : drop
  status               : enable
  log                  :
  remark               :

CES(config-fwpolicy)#
```

show rules (NAT Policy Configuration)

Use this command to display one or all configured NAT rules.

Syntax

show rules [**all** | <*rule-number*>]

Parameters

all	Display all configured NAT rules.
rule-number	Display the NAT rule with the specified number. To see NAT rule numbers, use the **show rules all** command.

Default

None

Command mode

NAT Policy Configuration

Next command mode

NAT Policy Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

`% NAT rule` *`xxx`* `does not exist.`

Related commands

`rule`

Example

The following example displays NAT rule 1.

```
CES(config-natpolicy)# show rules 1
Rules:
  rule_number          : 1
  source               : mytestnetobj
  destination          : PublicInterface
  service              : pptp
  action               : dst_action
  action_type          : translate
  translation_mode     : port-forwading
  trans_address        : CopyOfPublicInterface
  status               : enable
  description          :
CES(config-natpolicy)#
```

show services

Use this command to display the configured service objects and service object groups that you can use for firewall and NAT policies.

Syntax

show services [**group** | **icmp** | **ip** | **tcp** | **udp**]

Parameters

group	Restrict the display of service objects to groups.
icmp	Restrict the display of service objects to ICMP services.
ip	Restrict the display of service objects to IP services.
tcp	Restrict the display of service objects to TCP services.
udp	Restrict the display of service objects to UDP services.

Default

None

Command mode

Firewall Policy Configuration
NAT Policy Configuration
Policy Object Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

service

Example

The following example displays IP service objects.

```
CES(config-natpolicy)# show services ip

 ospf
  type            : ip_protocol
  protocol        : 89

 ggp
  type            : ip_protocol
  protocol        : 3

 egp
  type            : ip_protocol
  protocol        : 8
```

```
 skip
  type            : ip_protocol
  protocol        : 57

 rsvp
  type            : ip_protocol
  protocol        : 46

 gre
  type            : ip_protocol
  protocol        : 47

 ah
  type            : ip_protocol
  protocol        : 51

 esp
  type            : ip_protocol
  protocol        : 50

 vrrp
  type            : ip_protocol
  protocol        : 112
CES(config-natpolicy)#
```

Example: Using the NOT operand to configure NAT

When you create a network object to use in NAT policy rules, you can use the **NOT** operand to define an IP range or network that you *exclude* from using NAT.

The following example illustrates how to create policy objects for NAT; one of these objects includes the **NOT** operand. The example then uses the objects as rules in a NAT policy that implements NAT on the address range when it is the source address range but excludes the same address range from using NAT when it is the destination.

The following commands create three policy objects that specify IP address ranges.

```
CES(config)# policy object
CES(config-policyobj)# netobj add "IP_RangePrvtNet" ip-range
10.10.10.128 10.10.10.159
CES(config-policyobj)# netobj add "NOT IP_RangePrvtNet"
ip-range 10.10.10.128 10.10.10.159
CES(config-policyobj)# netobj add
"NAT_StaticPublicAddressRange" ip-range 47.17.66.128
47.17.66.159
CES(config-policyobj)# exit
```

The following commands create a NAT policy called “NAT_InterfacePolicy” and adds a rule that uses the policy objects that you created. This policy implements NAT on the address range when it is the source address range but excludes the same address range from using NAT when it is the destination.

```
CES(config)# policy nat add NAT_InterfacePolicy
CES(config)# policy nat NAT_InterfacePolicy
CES(config-natpolicy)# rule add action static source
"IP_RangePrvtNet" destination "NOT IP_RangePrvtNet"
translated-source "NAT_StaticPublicAddressRange"
CES(config-natpolicy)# exit
```

Chapter 20
TunnelGuard configuration commands

This chapter describes TunnelGuard configuration commands.

Command	Page
show tunnel-guard filters	1060
show tunnel-guard policy	1061
show tunnel-guard server-port	1062
tunnel-guard agent-min-version	1063
tunnel-guard agent-query-timeout	1065
tunnel-guard banner	1067
tunnel-guard banner-fragment	1068
tunnel-guard enable	1069
tunnel-guard fail-action	1071
tunnel-guard noagent-action	1072
tunnel-guard recheck-interval	1074
tunnel-guard display-error-detail	1075
tunnel-guard heartbeat-interval	1077
tunnel-guard heartbeat-retry	1078
tunnel-guard jre-location	1080
tunnel-guard log-level	1082
tunnel-guard server-port	1083
use tunnel-guard filter	1085
use tunnel-guard policy	1087

show tunnel-guard filters

Use this command to display configuration information about the TunnelGuard filters that have previously been provisioned on the gateway.

Syntax

```
show tunnel-guard filters
```

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

```
use tunnel-guard filters
```

Example

The following example displays the filters for TunnelGuard.

```
CES# show tunnel-guard filters
Tunnel-guard filters:
   Deny all
   Entrust PKI
   New Filter
   Permit all
   Permit only dns/ftp single server
   Permit only dns/ftp
   Permit only dns/http single server
   Permit only dns
CES#
```

show tunnel-guard policy

Use this command to display the list of rules in the TunnelGuard policy.

Syntax

show tunnel-guard policy

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

use tunnel-guard policy

Example

The following example displays the TunnelGuard policy rules.

```
CES# show tunnel-guard policy
POLICY Rule Set:
  Antivirus & Firewall
  Not Both Test
  Not One
  Version Mismatch
CES#
```

show tunnel-guard server-port

Use this command to display the TunnelGuard server TCP/UDP port number.

Syntax

show tunnel-guard server-port

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard server-port

Example

The following example displays the TunnelGuard server port number.

```
CES# show tunnel-guard server-port
Server Port: 8088
CES#
```

tunnel-guard agent-min-version

Use this command to set the agent minimum version on the router.

Syntax

```
tunnel-guard agent-min-version  {feature <0-15> | major
<0-15> | minor <0-15> | patch <0-15>}
```

Parameters

feature	Sets the feature number.
major	Sets the major version number.
minor	Sets the minor version number.
patch	Sets the patch number.

Default

None

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard enable
tunnel-guard fail-action
tunnel-guard recheck-interval
tunnel-guard server-port
use tunnel-guard filter
use tunnel-guard policy

Example

The following example sets the agent-min-version for TunnelGuard:

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# tunnel-guard agent-min-version
feature 3
CES(config-group/conn)#
```

tunnel-guard agent-query-timeout

Use this command to set the agent query timeout interval for the TunnelGuard feature on the gateway.

Syntax

tunnel-guard agent-query-timeout <*interval*>

Parameters

interval	Specifies the agent query timeout interval in seconds. Type a value from 0 through 86400.

Default

2 seconds

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard enable
tunnel-guard fail-action
tunnel-guard recheck-interval
tunnel-guard server-port
use tunnel-guard filter
use tunnel-guard policy

Example

The following example sets the agent query timeout interval for TunnelGuard to 30 seconds.

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# tunnel-guard agent-query-timeout 30
CES(config-group/conn)#
```

tunnel-guard banner

Use this command to add text to the TunnelGuard banner on the router.

Syntax

tunnel-guard banner *<word>*

Parameters

<word>	Text of the banner in quotes and must be a single line of text.

Default

None

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard banner-fragment

Example

The following example adds banner text to the TunnelGuard banner.

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# tunnel-guard banner “new banner”
CES(config-group/conn)#
```

tunnel-guard banner-fragment

Use this command to add text to the TunnelGuard banner-fragment on the router.

Syntax

tunnel-guard banner-fragment *<word>*

Parameters

<word>	Text of the banner in quotes and must be a single line of text.

Default

None

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard banner

Example

The following example adds banner-fragment text to the TunnelGuard banner.

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# tunnel-guard banner-fragment
“description”
CES(config-group/conn)#
```

tunnel-guard enable

Use this command to enable the TunnelGuard feature on the gateway. Use the **no** form of this command to disable the TunnelGuard feature.

Syntax

```
tunnel-guard enable
no tunnel-guard enable
```

Parameters

None

Default

Disabled

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard agent-query-timeout
tunnel-guard fail-action
tunnel-guard recheck-interval
tunnel-guard server-port
use tunnel-guard filter
use tunnel-guard policy

Example

The following example enables TunnelGuard on the gateway.

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# tunnel-guard enable
CES(config-group/conn)#
```

The following example disables TunnelGuard.

```
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# no tunnel-guard enable
CES(config-group/conn)#
```

tunnel-guard fail-action

Use this command to set the fail action for the TunnelGuard feature on the gateway.

Syntax

tunnel-guard fail-action {**leave-restricted** | **no-action** | **teardown-tunnel**}

Parameters

leave-restricted	Specifies that the tunnel will be left up but that it will restrict traffic.
no-action	Specifies that no action will be taken.
teardown-tunnel	Specifies that the tunnel will be torn down.

Default

teardown-tunnel

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard agent-query-timeout
tunnel-guard enable
tunnel-guard recheck-interval
tunnel-guard server-port
use tunnel-guard filter
use tunnel-guard policy

Example

The following example sets the fail-action option to “no-action.”

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# tunnel-guard fail-action no-action
CES(config-group/conn)#
```

tunnel-guard noagent-action

Use this command to set the noagent-level for the TunnelGuard feature on the gateway.

Syntax

tunnel-guard noagent-action {**stay-restricted** | **teardown-tunnel**}

Parameters

stay-restricted	Specifies that the tunnel restricts traffic.
teardown-tunnel	Specifies that the tunnel will be torn down.s

Default

None

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard agent-query-timeout
tunnel-guard enable
tunnel-guard recheck-interval
tunnel-guard server-port
use tunnel-guard filter
use tunnel-guard policy

Example

The following example sets the noagent-level option to “stay-restricted.”

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# tunnel-guard noagent-action stay-
restricted
CES(config-group/conn)#
```

tunnel-guard recheck-interval

Use this command to set a recheck interval for the TunnelGuard feature on a gateway.

Syntax

tunnel-guard recheck-interval <*minutes*>

Parameters

minutes	Specifies the number of minutes for the recheck interval. Type a value from 0 through 1440 (24 hours).

Default

15 minutes

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard agent-query-timeout
tunnel-guard enable
tunnel-guard fail-action
tunnel-guard server-port
use tunnel-guard filter
use tunnel-guard policy

Example

The following example sets the recheck interval to 1 hour.

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# tunnel-guard enable
CES(config-group/conn)# tunnel-guard recheck-interval 60
CES(config-group/conn)#
```

tunnel-guard display-error-detail

Use this command to display error details on the router.

Syntax

tunnel-guard display-error-detail
no tunnel-guard display-error-detail

Parameters

None

Default

tunnel-guard display-error-detail

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard enable
tunnel-guard fail-action
tunnel-guard recheck-interval
tunnel-guard server-port
use tunnel-guard filter
use tunnel-guard policy

Example

The following example sets the display-error-detail to True.

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# tunnel-guard display-error-detail
CES(config-group/conn)#
```

tunnel-guard heartbeat-interval

Use this command to set the heartbeat interval for the TunnelGuard feature on the gateway.

Syntax

tunnel-guard heartbeat-interval <*interval*>

Parameters

interval	Specifies the heartbeat interval in seconds. Type a value from 30 through 3600.

Default

None

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard enable
tunnel-guard fail-action
tunnel-guard recheck-interval
tunnel-guard server-port
use tunnel-guard filter
use tunnel-guard policy

Example

The following example sets the heartbeat interval to 30 seconds.

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# tunnel-guard heartbeat-interval 30
CES(config-group/conn)#
```

tunnel-guard heartbeat-retry

Use this command to set the heartbeat retry for the TunnelGuard feature on the gateway.

Syntax

tunnel-guard heartbeat-retry <*retries*>

Parameters

retries	Specifies the heartbeat retry attempts. Type a value from 2 through 10.

Default

None

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard enable
tunnel-guard fail-action
tunnel-guard recheck-interval
tunnel-guard server-port
use tunnel-guard filter
use tunnel-guard policy

Example

The following example sets the heartbeat retry to 6 attempts.

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# tunnel-guard heartbeat-retry 6
CES(config-group/conn)#
```

tunnel-guard jre-location

Use this command to find the jre location for the TunnelGuard agent.

Syntax

tunnel-guard jre-location <*line*>

Parameters

line	Specifies the pathway for the location of jre.

Default

None

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard enable
tunnel-guard fail-action
tunnel-guard recheck-interval
tunnel-guard server-port
use tunnel-guard filter
use tunnel-guard policy

Example

The following example sets the pathway for the TunnelGuard agent to find the jre location.

```
CES# config terminal
CES(config)# group connectivity/Base/newgroup
CES(config-group/conn)# tunnel-guard jre-location c:\Program
Files\Nortel\tunnelguard\jre.exe
CES(config-group/conn)#
```

tunnel-guard log-level

Use this command to set the log level on the router.

Syntax

```
tunnel-guard log-level {fatal | error | warn |info | debug}]
```

Parameters

Fatal	Sets the log level to fatal. Fatal designates error events that can lead to TunnelGuard shutting down.
Error	Sets the log level to error. Error designates error events that still allow TunnelGuard to run.
Warn	Sets the log level to warn. Warn designates potentially harmful situations.
Info	Sets the log level to information. Info designates informational messages.
Debug	Sets the log level to debug. Debug designates information useful for debugging.

Default

None

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity configuration

Required privileges

System Management - Manage
User Management - None

Related commands

tunnel-guard enable
tunnel-guard fail-action
tunnel-guard recheck-interval
tunnel-guard server-port
use tunnel-guard filter
use tunnel-guard policy

Example

The following example sets the log level for TunnelGuard to information.

```
CES# config terminal
CES(config)# group connectivity/Base/newgroup
CES(config-group/conn)# tunnel-guard log-level info
CES(config-group/conn)#
```

tunnel-guard server-port

Use this command to change the default port number. Use the **no** form of the command to reset the default port number to its default value, 8082.

Syntax

tunnel-guard server-port *<number>*
no tunnel-guard server-port

Parameters

number	Specifies the TCP/UDP port number on the gateway for the TunnelGuard server.

Default

8082

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show tunnel-guard server-port
tunnel-guard agent-query-timeout
tunnel-guard enable
tunnel-guard fail-action
tunnel-guard recheck-interval
use tunnel-guard filter
use tunnel-guard policy

Example

The following example sets the TunnelGuard server port number to port number 8088.

```
CES# config terminal
CES(config)# tunnel-guard server-port 8088
CES(config)# exit
CES# show tunnel-guard server-port
Server Port: 8088
CES#
```

The following example resets the TunnelGuard server port number to its default value.

```
CES# config terminal
CES(config)# no tunnel-guard server-port
CES(config)# exit
CES# show tunnel-guard server-port
Server Port: 8082
CES#
```

use tunnel-guard filter

Use this command to specify the filter that TunnelGuard will use.

Syntax

use tunnel-guard filter <*name*>

Parameters

name	Specifies the name of the filter that will be applied to restrict access to the tunnel during client TunnelGuard software checking. Type an alphanumeric string.

Default

Deny all

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show tunnel-guard filters

Example

The following example configures TunnelGuard to use the filter "permit-only-pfwauth."

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# use tunnel-guard filter
permit-only-pfwauth
CES(config-group/conn)#
```

use tunnel-guard policy

Use this command to associate a policy to the TunnelGuard feature.

Syntax

use tunnel-guard policy <*name*>

Parameters

name	Specifies the name of the policy that contains the required client software modules that will be checked. Type an alphanumeric string.

Default

None

Command mode

Group Connectivity Configuration

Next command mode

Group Connectivity Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show tunnel-guard policy

Example

The following example configures the group /Base/newgroup to use the TunnelGuard policy “engineering.”

```
CES# config terminal
CES(config)# group connectivity /Base/newgroup
CES(config-group/conn)# use tunnel-guard policy engineering
CES(config-group/conn)#
```

Chapter 21
Ethernet configuration commands

This chapter describes Ethernet interface configuration commands.

Command	Page
arp timeout	1090
description	1091
duplex	1092
filter	1094
interface fastethernet	1095
interface gigabitethernet	1097
mac-pause	1099
mac-pause threshold	1100
mac-pause ticks	1101
mtu	1102
public	1104
service dhcp enable	1106
show interface fastethernet	1107
show interface gigabitethernet	1110
shutdown	1111
speed	1113
tcp-mss	1114
tcp-mss enable	1116

arp timeout

Use this command to specify how long an ARP entry remains in the ARP cache. Use the **no** form of the command to delete the timeout value.

Syntax

```
arp timeout <seconds>
no arp timeout
```

Parameters

seconds	Specifies the number of seconds that an ARP entry remains in the ARP cache. Set the value to 0 to configure the entry to remain in the cache permanently.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Related commands

```
arp
clear arp-cache
show arp
```

Example

The following example creates a static ARP entry and then configures it to be removed from the ARP cache after 3600 seconds (1 hour).

```
CES(config)# arp 47.10.11.22 00:e0:7b:58:7a:e1
CES(config)# interface fastethernet 2/1
CES(config-if)# arp timeout 3600
CES(config-if)#
```

The following example creates a static ARP entry and then configures it to never be removed from the ARP cache.

```
CES(config)# arp 47.10.11.22 00:e0:7b:58:7a:e1
CES(config)# interface fastethernet 2/1
CES(config-if)# arp timeout 0
CES(config-if)#
```

description

Use this command to set the description for the current interface. The **no** form of the command sets the description to an empty string.

The interface description appears in the result of the ifName MIB.

Syntax

description <*text*>
no description

Parameters

text	Specifies the text description for the interface. Type as may as 24 characters. If you use spaces in the text, you must enclose the text in quotation marks.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Related commands

show interface fastethernet
show interface gigabitethernet

Example

The following example adds a text description for the Fast Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# description “LAN Interface 1”
```

The following example deletes the text description from an interface.

```
CES(config-if)# no description
CES(config-if)#
```

duplex

Use this command to set the speed for the current interface. You must use this command in combination with the **speed** command to create a permitted speed-duplex combination. If you set the duplex or the speed to auto, the values for both duplex and speed will be autonegotiated. This command does not apply to Gigabit Ethernet fiber interfaces, which use only autonegotiation.

Syntax

```
duplex {auto | full | half}
```

Parameters

auto	Specifies that the duplex mode will be autonegotiated.
full	Specifies full-duplex mode.
half	Specifies half-duplex mode.

Default

Autonegotiated

Command mode

Interface Configuration

Next command mode

Interface Configuration

Related commands

```
show interface fastethernet
show interface gigabitethernet
speed
```

Example

The following example configures the Fast Ethernet interface for half-duplex operation.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# duplex half
CES(config-if)#
```

The following example configures the Gigabit Ethernet system interface for autonegotiation.

```
CES(config)# interface gigabitethernet 0/2
CES(config-if)# duplex auto
CES(config-if)#
```

filter

Use this command to set the interface filter for the current interface. The **no** form of the command removes the interface filter.

Syntax

filter <*name*>
no filter

Parameters

name	Specifies the name of the interface filter to use.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Warning messages

```
% Interface Filter name does not exist
```

Related commands

show interface fastethernet
show interface gigabitethernet

Example

The following example applies the interface filter “deny all/in” to interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# filter “deny all/in”
```

The following example deletes the configured interface filter from the interface.

```
CES(config-if)# no filter
CES(config-if)#
```

interface fastethernet

Use this command to enter Interface Configuration mode for the specified Fast Ethernet* interface or to enable a Fast Ethernet interface. Use the **no** form of the command to disable the interface.

Syntax

interface fastethernet <*slot*>/<*port*> [**enable**]
no interface fastethernet <*slot*>/<*port*> **enable**

Parameters

slot	Specifies the slot where the interface card resides (type 0 for the system board).
port	Specifies the port on the system board or interface card.

Default

None

Command mode

Global Configuration

Next command mode

Interface Configuration
Global Configuration (when you enter the **enable** option)

Warning messages

```
% Interface <slot/port> does not exist
```

Related commands

show interface fastethernet
show interface gigabitethernet

Example

The following example navigates from Global Configuration mode to Interface Configuration mode, where you can set parameters for the Fast Ethernet port 1/1.

```
CES(config)# interface fastethernet 1/1
CES(config-if)#
```

The following example enables Fast Ethernet port 1/1.

```
CES(config)# interface fastethernet 1/1 enable
CES(config)#
```

The following example disables Fast Ethernet port 1/1.

```
CES(config)# no interface fastethernet 1/1 enable
CES(config)#
```

interface gigabitethernet

Use this command to enter Interface Configuration mode for the specified Gigabit Ethernet interface or to enable a Gigabit Ethernet interface. Use the **no** form of the command to disable the interface.

Syntax

interface gigabitethernet <*slot*>/<*port*> [**enable**]
no interface gigabitethernet <*slot*>/<*port*> **enable**

Parameters

slot	Specifies the slot where the interface card resides (type 0 for the system board).
port	Specifies the port on the system board or interface card.

Default

None

Command mode

Global Configuration

Next command mode

Interface Configuration
Global Configuration (when you enter the **enable** option)

Warning messages

```
% Interface <slot/port> does not exist
% Interface <slot/port> is not a Gigabit Ethernet interface
```

Related commands

show interface fastethernet
show interface gigabitethernet

Example

The following example navigates from Global Configuration mode to Interface Configuration mode, where you can set parameters for Gigabit Ethernet port 0/1.

```
CES(config)# interface gigabitethernet 0/1
CES(config-if)#
```

The following example enables Gigabit Ethernet port 0/1.

```
CES(config)# interface gigabitethernet 0/1 enable
CES(config)#
```

The following example disables Gigabit Ethernet port 0/1.

```
CES(config)# no interface gigabitethernet 0/1 enable
CES(config)#
```

mac-pause

Use this command to enable Ethernet packet flow control. When you enable this option, the gateway automatically adjusts and controls the flow of incoming and outgoing packets from any standard-speed LAN device to prevent packet loss in a congested system. Use the **no** form of the command to disable flow control.

Syntax

```
mac-pause
no mac-pause
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Related commands

```
mac-pause threshold
mac-pause ticks
```

Example

The following example enables MAC pause flow control.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# mac-pause
CES(config-if)#
```

The following example disables MAC pause flow control.

```
CES(config-if)# no mac-pause
CES(config-if)#
```

mac-pause threshold

Use this command to set the free receive FIFO threshold. Use this command in conjunction with the **mac-pause** command, which enables Ethernet packet flow control.

Syntax

mac-pause threshold <*percentage*>

Parameters

percentage	Type one of the following percentage values: 0%, 15%, 35%, 40%, 50%, 60%, 65%, 75%, 85%.

Default

0

Command mode

Interface Configuration

Next command mode

Interface Configuration

Related commands

mac-pause
mac-pause ticks

Example

The following example sets the MAC pause flow control threshold to 40%.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# mac-pause
CES(config-if)# mac-pause threshold 40%
CES(config-if)#
```

mac-pause ticks

Use this command to set the value of MAC pause ticks. Use this command in conjunction with the **mac-pause** command, which enables Ethernet packet flow control.

Syntax

mac-pause ticks <*ticks-value*>

Parameters

ticks-value	Specifies the MAC pause ticks value. Type an integer from 31 through 65535.

Default

MAC pause ticks defaults to 0.

Command mode

Interface Configuration

Next command mode

Interface Configuration

Related commands

mac-pause
mac-pause threshold

Example

The following example sets the MAC pause ticks to 555.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# mac-pause
CES(config-if)# mac-pause ticks 555
CES(config-if)#
```

mtu

Use this command to reset the maximum transmission unit (MTU) of an interface. Use the **no** form of the command to reset the MTU value to its default value (see Table 9 on page 1103). If you are running IPX, Nortel recommends that you not change the MTU.

The MTU specifies the largest packet that can be sent out an interface; if a packet to be sent is larger than the MTU configured for the interface, the packet is fragmented or dropped. You can reset the MTU value as follows:

- For LAN interfaces: 576 through 1500 bytes
- For PPPoE interfaces: 576 through 1492 bytes
- For WAN interfaces: 576 through 1788 bytes

Syntax

```
mtu <bytes>
no mtu
```

Parameters

bytes	Specifies the maximum transmission unit in bytes. For an Ethernet interface, enter a value from 576 through 1500; for a PPPoE interface, enter a value from 576 through 1492; for other interfaces, enter a value from 576 through 1788.

Default

The default MTU value for each interface is based on the media type minus the Layer 2 encapsulation (Table 9).

Table 9 Default MTU by interface

Media/interface	Default MTU (bytes)
Ethernet	1500
Frame relay	1496
ISDN	1500
PPPoE	1492
Serial	1500
WAN (T1/T3)	1788

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show interface
tcp-mss
tcp-mss enable

Example

The following example sets the MTU for Ethernet interface 2/1 to 1400 bytes.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# mtu 1400
CES(config-if)#
```

The following example resets the MTU size to its default value (for an Ethernet interface, 1500 bytes).

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no mtu
CES(config-if)#
```

public

Use this command to set the current interface to be public. The **no** form of the command sets the current interface to be private.

Syntax

public
no public

Parameters

None

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Warning messages

```
% Cannot change this setting for this interface.

% This change in LAN settings will not take effect until you
reboot the system.
```

Related commands

show interface fastethernet
show interface gigabitethernet

Example

The following example configures Gigabit Ethernet interface 2/1 to be public.

```
CES(config)# interface gigabitethernet 2/1
CES(config-if)# public
CES(config-if)#
```

The following example configures interface 2/1 to be private.

```
CES(config-if)# no public
CES(config-if)#
```

service dhcp enable

Use this command to enable the DHCP server on this interface. Use the **no** form of the command to disable the DHCP server on the interface.

Syntax

```
service dhcp enable
no service dhcp enable
```

Parameters

None

Default

Enabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

service dhcp enable (Global Configuration command)

Example

The following example disables and reenables the DHCP server on the Fast Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no service dhcp enable
CES(config-if)# service dhcp enable
CES(config-if)#
```

show interface fastethernet

Use this command to display information about Fast Ethernet interfaces.

Syntax

show interface fastethernet [<*slot*>/<*port*>]

show interface fastethernet <*slot*>/<*port*> [**ip** [**routing** | **vrrp**] | **pppoe** | **qos**]

Parameters

slot	Specifies the slot where the Fast Ethernet interface card resides (type 0 for the system board).
port	Specifies the port on the system board or interface card.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

interface fastethernet

Example

The following example displays configuration parameters for Fast Ethernet interface 1/1.

```
CES# show interface fastethernet 1/1
FastEthernet Interface 1/1 Configuration
  Description                       : Private LAN
  DHCP-relay                        : Disabled
  Duplex                            : AutoNegotiate
  Filter                            : deny all
  IP Address                        : 10.10.10.2
  MAC pause                         : Enabled
    Threshold [%]                   : 40
    Ticks                           : 555
  MTU                               : 1500
  PPPoE                             : Enabled
  Public/Private                    : Public
  DHCP Service                      : Enabled
  Status                            : Up
  Speed [Mbps]                      : AutoNegotiate
  TCP-Maximum Segment Size Clamping: Enabled
  TCP-Maximum Segment Size [bytes] : 1460
  VLANs (802.1Q)                    : Enabled
CES#
```

The following example displays IP configuration parameters for Fast Ethernet interface 0/1.

```
CES# show interface fastethernet 0/1 ip
FastEthernet Interface 0/1 IP Configuration
  IP Address                : 47.17.248.55
  IP Address Type           : Static
  DHCP Relay
    Relay-IP                : 47.17.248.53
    Helper Server 1         : 0.0.0.0
    Helper Server 2         : 0.0.0.0
    Helper Server 3         : 0.0.0.0
    Rebroadcast DHCP        : Disabled
  Multicast Relay Boundary  : Enabled
  Routing                   : RIP
  VRRP                      : Disabled
CES#
```

The following example displays IP routing configuration parameters for Fast Ethernet interface 0/1.

```
CES#show interface fastethernet 0/1 ip routing
FastEthernet Interface 0/1 Routing Configuration
  IP Address                    : 47.17.248.53
    Type                        : Static
    Routing                     : RIP
      Authentication Mode       : none
      Export BO static metric   : 1
      Export Default metric     : 0
      Export OSPF metric        : 0
      Export Static Route metric: 1
      Import Default Route      : Disabled
      Poison Reverse            : Enabled
      Receive RIP Version       : 2
      Send RIP Version          : 2
CES#
```

show interface gigabitethernet

Use this command to display information about Gigabit Ethernet interfaces.

Syntax

show interface gigabitethernet [*<slot>*/*<port>*]

show interface gigabitethernet *<slot>*/*<port>* [**ip** [**routing** | **vrrp**] | **pppoe** | **qos**]

Parameters

slot	Specifies the slot where the Gigabit Ethernet interface card resides (type 0 for the system board).
port	Specifies the port on the system board or interface card.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Related commands

interface gigabitethernet

Example

The following example displays Gigabit Ethernet parameters.

```
CES# show interface gigabitethernet 0/1
Gigabit Ethernet Interface 9/1 Configuration
  Description                                 : Motherboard port
  DHCP-relay                                  :
  Duplex                                      : auto
  Filter                                      :
  IP Address                                  : 10.10.10.2
  MAC-pause                                   : Enabled
    Threshold [%]                             : 40
    Ticks                                     : 555
  PPPoE                                       : Disabled
  Public                                      : Public
  QoS                                         : Disabled
  Rebroadcast DHCP                            : Enabled
  Relay-IP                                    : 44.44.44.2
  Service (DHCP)                              : Enabled
  Status                                      : Active
  Speed                                       : 1000
CES#
```

shutdown

Use this command to disable the current interface. Use the **no** form of the command to reenable the interface.

Syntax

shutdown
no shutdown

Parameters

None

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Related commands

interface fastethernet
interface gigabitethernet

Example

The following example disables Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# shutdown
CES(config-if)#
```

The following example reenables interface 2/1.

```
CES(config-if)# no shutdown
CES(config-if)#
```

speed

Use this command to set the speed for the Ethernet interface. You must use this command in combination with the **duplex** command to create a permitted speed-duplex combination. If you set the speed or the duplex to auto, the values for both duplex and speed will be autonegotiated. This command does not apply to Gigabit Ethernet fiber interfaces, which use only autonegotiation.

Syntax

```
speed {10 | 100} [duplex {full | half}]
speed auto
```

Parameters

auto	Specifies that the interface autonegotiates the speed.
10	Sets the speed to 10 Mb/s.
100	Sets the speed to 100 Mb/s.
full	Specifies that the interface operate at full duplex.
half	Specifies that the interface operate at half duplex.

Default

Autonegotiation

Command mode

Interface Configuration

Next command mode

Interface Configuration

Related commands

duplex
show interface fastethernet
show interface gigabitethernet

Example

The following example configures Fast Ethernet interface 2/1 for half-duplex operation at 100 Mb/s.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# speed 100 duplex half
CES(config-if)#
```

The following example configures Gigabit Ethernet interface 0/1 for autonegotiation.

```
CES(config)# interface gigabitethernet 0/1
CES(config-if)# speed auto
CES(config-if)#
```

tcp-mss

Use this command to configure the TCP maximum segment size (MSS) on an interface. The TCP MSS specifies the largest TCP packet that a client can accept from a TCP peer server. You configure the TCP MSS independently from the MTU size.

Use the **no** form of the command to reset the TCP MSS to its default value. (On most PCs and on the Nortel VPN Router, the default value for the TCP MSS is MTU – 40 bytes.)

Syntax

tcp-mss <*bytes*>
no tcp-mss

Parameters

bytes	Specifies the maximum amount of TCP data in bytes. For an Ethernet interface, enter a value from 536 through 1460; for other interfaces, enter a value from 536 through 1748.

Default

1460

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

mtu
show interface
tcp-mss enable

Example

The following example sets the TCP MSS to 1400 bytes on Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# tcp-mss 1400
CES(config-if)#
```

The following example resets the TCP MSS on serial interface 4/1 to its default value (1460).

```
CES(config)# interface serial 4/1
CES(config-if)# no tcp-mss
CES(config-if)#
```

tcp-mss enable

Use this command to enable TCP MSS clamping. TCP MSS clamping is the substitution of a configured MSS for the MSS value negotiated with the TCP peer. To implement TCP MSS clamping, you must configure it on the interfaces that will receive or transmit the plain-text packets.

Note: Tunnels do not support clamping. To implement clamping across tunnels, configure TCP MSS clamping on the ingress private side network.

When you configure TCP MSS clamping, the packets affected are already "clamped" when they go through a tunnel. Use the **no** form of the command to disable TCP MSS clamping.

Syntax

```
tcp-mss enable
no tcp-mss enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

mtu
show interface
tcp-mss

Example

The following example enables TCP MSS clamping on serial interface 4/1.

```
CES(config)# interface serial 4/1
CES(config-if)# tcp-mss enable
CES(config-if)#
```

The following example disables TCP MSS clamping on serial interface 4/1.

```
CES(config)# interface serial 4/1
CES(config-if)# no tcp-mss enable
CES(config-if)#
```

Chapter 22
802.1Q VLAN configuration commands

This chapter describes 802.1Q VLAN configuration commands.

Command	Page
description	1121
dot1q enable	1122
dot1q interface untag egress	1124
dot1q interface untag ingress	1125
dot1q interface vlan-id	1129
encapsulation dot1q	1129
filter	1130
ip address	1132
ip address dhcp	1134
ip address type	1136
ip ospf	1138
ip rip	1140
ip vrrp	1141
ip vrrp backup	1142
ip vrrp backup enable	1144
ip vrrp backup disable	1145
ip vrrp master	1146
rule (Firewall Policy Configuration)	1147
show dot1q	1151
show dot1q statistics	1153
subinterface	1154

Command	Page
subinterface enable	1156
Configuration example	1158

description

Use this command to specify a text description for the subinterface. Use the **no** form of the command to delete this text.

The interface description appears in the result of the ifName MIB.

Syntax

```
description <text>
no description
```

Parameters

text	Specifies a text description for the subinterface. You can enter up to 127 characters. If you enter a string with spaces, enclose the string in quotation marks.

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

encapsulation dot1q
filter
ip address
show dot1q
subinterface

Example

The following example creates a description for subinterface 100 on Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# subinterface 100
CES(config-subif)# description “My local interface to CO”
CES(config-subif)#
```

dot1q enable

Use this command to set the encapsulation format on the Ethernet interface to IEEE 802.1Q. Use the **no** form of the command to disable 802.1Q encapsulation.

Syntax

dot1q enable
no dot1q enable

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

encapsulation dot1q
ip address
show dot1q
subinterface

Example

The following example disables 802.1Q encapsulation on Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no dot1q enable
CES(config-if)#
```

dot1q interface untag egress

Use this command to configure the interface VLAN to send untagged packets out without adding an 802.1Q tag header to the packets (this is the default behavior). Use the **no** form of the command to configure the interface VLAN to add an 802.1Q tag header to untagged packets before it sends the packets out. The 802.1Q tag header includes the VLAN ID of the interface VLAN.

If the interface has egress DSCP-802.1p mapping enabled and you configure this interface to send untagged packets, the packets are sent with the 802.1Q tag header containing the mapped 802.1p priority value but with a null VLAN ID.

Syntax

```
dot1q interface untag egress
no dot1q interface untag egress
```

Parameters

None

Default

Packets are sent out untagged.

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

dot1q enable
dot1q interface untag ingress
dot1q interface vlan-id
qos egress-dscp-map enable
show dot1q

Example

The following example configures Ethernet interface 2/1 to send out packets with an 802.1Q tag header containing the interface VLAN ID. Note the warning message that appears when you execute this command.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no dot1q interface untag egress
% This may cause loss of connectivity if connected hosts
% cannot process tagged frames
CES(config-if)#
```

The following example configures Ethernet interface 2/1 to send out untagged packets without adding an 802.1Q tag header.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# dot1q interface untag egress
CES(config-if)#
```

dot1q interface untag ingress

Use this command to configure the interface VLAN to accept untagged packets (that is, packets that have no VLAN tag). Use the **no** form of the command to configure the interface VLAN to drop untagged packets.

Syntax

dot1q interface untag ingress
no dot1q interface untag ingress

Parameters

None

Default

Untagged packets are accepted.

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

dot1q enable
dot1q interface untag egress
dot1q interface vlan-id
show dot1q

Example

The following example configures Ethernet interface 2/1 to drop packets that do not have an 802.1Q tag header. Note the warning message that appears when you execute this command.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no dot1q interface untag ingress
% This may cause loss of connectivity if connected hosts
% send untagged frames
CES(config-if)#
```

The following example configures the interface VLAN to accept untagged packets.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# dot1q interface untag ingress
CES(config-if)#
```

dot1q interface vlan-id

Use this command to assign a VLAN identifier to the interface. Use the **no** form of the command to reset the interface VLAN ID to 1 (the default value).

Syntax

dot1q interface vlan-id <*vlan-identifier*>
no dot1q interface vlan-id

Parameters

vlan-identifier	Specifies a numeric identifier for the interface VLAN. You can enter a value from 1 through 4094.

Default

VLAN ID is 1.

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

dot1q enable
dot1q interface untag egress
dot1q interface untag ingress
show dot1q

Example

The following example enables 802.1Q encapsulation on Ethernet interface 2/1 and then configures an interface VLAN ID.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# dot1q enable
CES(config-if)# dot1q interface vlan-id 33
CES(config-if)#
```

The following example resets the interface VLAN ID to the default value, 1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no dot1q interface vlan-id
CES(config-if)#
```

encapsulation dot1q

Use this command to set the encapsulation format on the subinterface to IEEE 802.1Q and to specify the VLAN identifier. Use the **no** form of the command to delete the VLAN identifier from the subinterface.

Syntax

```
encapsulation dot1q <vlan-identifier>
no encapsulation dot1q
```

Parameters

vlan-identifier	Specifies a numeric identifier for this VLAN. You can enter a value from 1 through 4094.

Default

0

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

description
dot1q enable
filter
ip address
show dot1q
subinterface
subinterface enable

Example

The following example enables 802.1Q encapsulation on subinterface 2 on Ethernet interface 2/1. The VLAN identifier is 14.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# dot1q enable
CES(config-if)# subinterface 2
CES(config-subif)# encapsulation dot1q 14
CES(config-subif)#
```

The following example deletes the VLAN identifier from subinterface 2.

```
CES(config-if)# subinterface 2
CES(config-subif)# no encapsulation dot1q
CES(config-subif)#
```

filter

Use this command to specify an interface filter for the 802.1Q subinterface. Use the **no** form of the command to delete the filter.

Syntax

filter {name}
no filter

Parameters

name	Specifies the interface filter to apply. Enter one of the configured interface filters. If the filter name includes a space, enclose it in quotation marks. You can also enter the name of a user-created filter.

Default

Deny all

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

You must specify an IP address for the subinterface before you specify a filter.

Warning messages

```
% Interface filter name does not exist

% You must define the IP address before setting the filter
```

Related commands

```
description
encapsulation dot1q
ip address
show dot1q
subinterface
```

Example

The following example assigns an IP address and then applies the interface filter "deny all/in" to subinterface 11.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# subinterface 11
CES(config-subif)# ip 10.10.10.1 255.255.255.0
CES(config-subif)# filter "deny all/in"
CES(config-subif)#
```

The following example deletes the configured filter from the subinterface.

```
CES(config-if)# subinterface 11
CES(config-subif)# no filter
CES(config-subif)#
```

ip address

Use this command to assign an IP address and mask to the VLAN subinterface. Use the **no** form of the command to delete the IP address.

Syntax

```
ip address {address|mask}
no ip address
```

Parameters

address	Specifies in dotted-decimal notation the IP address to be associated with the subinterface.
mask	Specifies the subnet mask for the IP address associated with the subinterface.

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

description
encapsulation dot1q
filter
show dot1q
subinterface

Example

The following example configures an IP address for subinterface 2 on Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# subinterface 2
CES(config-subif)# ip address 10.10.10.1 255.255.255.0
CES(config-subif)#
```

The following example deletes the IP address from subinterface 2.

```
CES(config-if)# subinterface 2
CES(config-subif)# no ip address
CES(config-subif)#
```

ip address dhcp

This command allows the user to cancel a pending DHCP request, to reacquire an IP address from a DHCP server, or to set the cost of the route to the DHCP server.

This command extends it to work on a VLAN subinterface.

Syntax

```
ip address dhcp cancel
ip address dhcp cost cost
ip address dhcp reacquire
ip address dhcp default-lease time
ip address dhcp disallow-rfc-1918
```

Parameters

cost	Cost associated with the route to the DHCP server. Numeric value in the range 0 - 65535.
default-lease-time	Sets default lease time.
disallow-rfc-1918	Disallows rfc-1918

Default

None

Command mode

Sub-interface configuration

Next command mode

Sub-interface configuration

Required privileges

System Management - Manage

User Management - None

Related commands

ip address type

Examples

To cancel the pending DHCP request, reacquire an IP address from the DHCP server and set a cost of 5 for the route to the host:

```
CES(config-subif)# ip address dhcp cancel
CES(config-subif)# ip address dhcp reacquire
CES(config-subif)# ip address dhcp cost 5
```

ip address type

This command selects whether the virtual circuit sub-interface has a static IP address (configured through the ip address command) or a dynamic, DHCP-provided address.

This command extends it to work on a VLAN subinterface.

Syntax

```
ip address type static
ip address type dhcp
```

Parameters

None

Default

None

Command Mode

Sub-interface configuration

Next Command Mode

Sub-interface configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

ip address dhcp

Example

Example of configuring a static IP address for subinterface slot 2 port 1 virtual circuit 2:

```
CES(config)# interface fastethernet 2/1
CES(config-if)# subinterface 2
CES(config-subif)# ip address type static
CES(config-subif)# ip address 10.10.10.1
CES(config-subif)#
```

Example of configuring a dynamic IP address for subinterface slot 2 port 1 virtual circuit 2:

```
CES(config)# interface fastethernet 2/1
CES(config-if)# subinterface 2
CES(config-subif)# ip address type dhcp
CES(config-subif)#
```

ip ospf

Use this command to enable OSPF on the 802.1Q subinterface. Use the **no** form of the command to disable OSPF.



Note: You can configure OSPF on an 802.1Q subinterface with the same commands that you use to configure it on a LAN interface. For information about OSPF commands, see Chapter 23, “IP interface configuration commands,” on page 1159.

OSPF can be configured only on private interfaces and VLANs. Because a VLAN inherits its public/private attribute from the interface on which it is configured, you must configure the interface as private if you want the VLAN to use OSPF.

Syntax

```
ip ospf
no ip ospf
```

Parameters

None

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% OSPF is only available when the sub-interface is Private
```

Related commands

ip address
ip rip
show dot1q
subinterface

Example

The following example enables OSPF on subinterface 2 of Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# subinterface 2
CES(config-subif)# ip ospf
CES(config-subif)#
```

The following example disables OSPF on subinterface 2.

```
CES(config-if)# subinterface 2
CES(config-subif)# no ip ospf
CES(config-subif)#
```

ip rip

Use this command to enable RIP on the 802.1Q subinterface. Use the **no** form of the command to disable RIP.



Note: You can configure RIP on an 802.1Q subinterface with the same commands that you use to configure it on a LAN interface. For information about RIP commands, see Chapter 23, “IP interface configuration commands,” on page 1159.

Syntax

```
ip rip
no ip rip
```

Parameters

None

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip address
ip ospf
show dot1q
subinterface

Example

The following example enables RIP on subinterface 3 of Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# subinterface 3
CES(config-subif)# ip rip
CES(config-subif)#
```

The following example disables RIP on subinterface 2.

```
CES(config-if)# subinterface 2
CES(config-subif)# no ip rip
CES(config-subif)#
```

ip vrrp

This command enables VRRP on the subinterface and the **no** form of this command disables it.

This command is extended to work on a VLAN subinterface.

Syntax

ip vrrp
no ip vrrp

Parameters

None

Default

None

Command mode

Sub-interface configuration

Next command mode

Sub-interface configuration

Required privileges

System Management - Manage

User Management - None

Related commands

ip vrrp backup
ip vrrp master

Example

```
CES(config-subif)# ip vrrp
```

ip vrrp backup

This command specifies the backup addresses of other virtual router subinterfaces that are backing up this router.

This command is extended to work on a VLAN subinterface.

Syntax

```
ip  vrrp backup [priority <priority>]
no ip vrrp backup  <ip-address>
```

Parameters

ip-address	SubInterface IP address of virtual router backing this router.
priority	Priority of the backup with ranges from 1 to 253.

Default

100

Command mode

Sub-interface configuration

Next command mode

Sub-interface configuration

Required privileges

System Management - Manage

User Management - None

Related commands

ip vrrp backup <ip-address> **enable**

Example

CES(config-subif)# **ip vrrp backup 10.0.3.191**

ip vrrp backup enable

This command enables the backup subinterface. This command is extended to work on a VLAN subinterface.

Syntax

ip vrrp backup <ip-address> **enable**

Parameters

ip-address	SubInterface IP address of the backup to enable.

Default

None

Command mode

Sub-interface configuration

Next command mode

Sub-interface configuration

Required privileges

System Management - Manage

User Management - None

Related commands

ip vrrp backup

Example

```
CES(config-subif)# ip vrrp  backup 10.0.3.191 enable
```

ip vrrp backup disable

This command disables the created backup subinterface. This command is extended to work on a VLAN subinterface.

Syntax

ip vrrp backup <ip-address> **disable**

Parameters

ip-address	SubInterface IP address of the backup to disable.

Default

None

Command mode

Sub-interface configuration

Next command mode

Sub-interface configuration

Required privileges

System Management - Manage

User Management - None

Related commands

ip vrrp backup

Example

```
CES(config-subif)# ip vrrp backup 10.0.3.191 disable
```

ip vrrp master

This command enables mastership on the subinterface on which VRRP is running. Typically, every virtual router is its own master and can be backed up to other virtual routers on the same or different LAN.

This command is extended to work on a VLAN subinterface.

Syntax

ip vrrp master

Parameters

None

Default

None

Command mode

Sub-interface configuration

Next command mode

Sub-interface configuration

Required privileges

System Management - Manage

User Management - None

Related commands

ip vrrp backup

Example

```
CES(config-subif)# ip vrrp master
```

rule (Firewall Policy Configuration)

This command edits or adds the specified firewall policy rule to the current firewall policy in the Nortel VPN Router Stateful Firewall.

Policy rules are divided into three types: default, interface and override. Interface rules are divided into two types: source and destination. The execution order of the rule set is: Override rules are the first rules checked for a packet.

Interface rules are specified for the packets that arrive on or departs from a particular interface and are checked next. Then, default rules are checked for all packets if there are no matches in the other two groups.

Syntax

```
rule { default | override | interface interface-name {
source | destination } {add | rule-number} [src-interface
interface-name] [dst-interface interface-name] [src-address
address] [dst-address address] [service service-name]
[action action-name] [log log-level ] [remark text]

no rule { default | override | { interface interface-name {
source | destination } } number
```

Parameters

default	Parameter specifying the rule is a default rule.
override	Parameter specifying the rule is an override rule.
interface	Parameter specifying the rule is an interface rule.
source	Parameter specifying that the interface rule is a source interface rule.
destination	Parameter specifying that the interface rule is a destination interface rule.
add	Parameter specifying the policy rule should be created.
rule-number	Rule number in this firewall policy rule set.
src-interface	Settings are for the source interface. Not recognized for source interface rules.
dst-interface	Settings are for the destination interface. Not recognized for destination interface rules.
interface-name	The interface-name for override rules can be trusted, untrusted, any or tunnel:any. For a source interface rule, the interface-name of destination interface can be any, an end user interface (T0 - Tn), a branch office interface (Tx, - Ty), a physical interface including VLAN subinterfaces (E0 - En), trusted, untrusted, tunnel:any or system-ip. For a destination interface rule, the interface-name of source interface can be any, trusted, untrusted, tunnel:any.
src-address	Settings are for the source address.
dst-address	Settings are for the destination address.
address	Address for the source or destination. Can be a network object name, a network object group name or any.
service	Set the service for the current firewall policy rule.
service-name	Name of the service. Can be any or a predefined protocols such as FTP, HTTP, Telnet, SMTP, etc. It can also be a protocol (TCP or UDP) followed by a port number.
action	Set the action for the current firewall policy rule.
action-name	Name of the action. Can be accept, drop or reject.
log	Event log.
log-level	Can be one of none | brief | detail | trap. 'trap' is the same as detail, but also enables SNMP trapping on a rule match.

remark	The comments users can put in.
text	The content of the remark. If the value for the text parameter contains spaces, it may be enclosed in double quotes so that it has a single parameter value.

Default

For newly created rules, the default action is drop. The default interface is determined by the kind of rule group to which it belongs. In interface rule set, either source interface or destination interface has a default value and cannot be changed. The default settings of other fields are Any.

Command mode

Firewall Policy Configuration

Next command mode

Firewall Policy Configuration

Required Privileges

System Management - Manage

User Management - None

Warnings

% Rule xxx does not exist

% Invalid interface name

% Invalid network address

% Invalid service name

% Invalid number of arguments

Related commands

policy

Example

```
CES(config-fwpolicy)# rule override 3 src-interface
untrusted src-address 192.32.0.0 dst-address 192.32.240.11
service ftp action accept log full remark "This is for test"
```

```
CES(config-fwpolicy)# rule interface "Tunnel:/Base/myTunnel"
source add dst-address 192.32.240.11 service ftp action
accept log full remark "This is for test"
```

```
CES(config-fwpolicy)# rule interface "Tunnel:/Base/myTunnel"
source 3 dst-address 192.32.240.12 service ftp action accept
log brief
```

```
CES(config-fwpolicy)# rule default 3 src-address 192.32.0.0
service ftp action accept
```

```
CES(config-fwpolicy)# no rule interface "Tunnel:/Base/
myTunnel" 3
```

```
CES(config-fwpolicy)# no rule override 3
```

show dot1q

Use this command to display information about the IEEE 802.1Q VLANs configured on the gateway.

Syntax

show dot1q [<*vlan-identifier*>]

Parameters

vlan-identifier	Specifies a numeric identifier for this VLAN. You can enter a value from 1 through 4094.

Default

Display information about all VLANs configured on the gateway.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

dot1q enable
ip address
show dot1q statistics
subinterface
subinterface enable

Example

The following example displays information about all the VLANs configured on the gateway.

```
CES# show dot1q
 Slot Port Sub-if VLAN IP Address      Subnet Mask      Status  State
 ---- ---- ------ ---- --------------- --------------- ------- --------
 1    1    4      3    10.1.1.1        255.255.255.0   enabled UP
 1    1    26     145  12.1.1.1        255.255.255.0   enabled DOWN
 2    1    2      145  13.2.2.2        255.255.255.0   enabled UP
CES#
```

The following example displays information about VLAN 145.

```
CES# show dot1q 145
  Interface: 1/1
    Subinterface: 26
      802.1Q VLAN: 145
        Description: Finance Department
        IP Address:  12.1.1.1
        Subnet Mask: 255.255.255.0
        Status: enabled
        State: UP

  Interface: 2/1
    Subinterface: 2
      802.1Q VLAN: 145
        Description: Release Engineering
        IP Address: 13.2.2.2
        Subnet Mask: 255.255.255.0
        Status: disabled
        State: DOWN
CES#
```

show dot1q statistics

Use this command to display statistics for the IEEE 802.1Q VLANs on the gateway.

Syntax

show dot1q [<*vlan-identifier*>] **statistics**

Parameters

vlan-identifier	Specifies a numeric identifier for this VLAN. You can enter a value from 1 through 4094.

Default

Display statistics for all VLANs configured on the gateway.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

dot1q enable
ip address
show dot1q
subinterface
subinterface enable

Example

The following example displays statistics for all the VLANs configured on the gateway.

```
CES# show dot1q statistics
Slot Port Sub-if VLAN Frames In  Frames Out Bytes In   Bytes Out
---- ---- ------ ---- ---------- ---------- ---------- ----------
1    1    4      3    1234567890 1234567890 1234567890 1234567890
1    1    26     145  1234567890 1234567890 1234567890 1234567890
2    1    2      145  1234567890 1234567890 1234567890 1234567890
CES#
```

The following example displays statistics for VLAN 145.

```
CES# show dot1q 145 statistics
Slot Port Sub-if VLAN Frames In  Frames Out Bytes In   Bytes Out
---- ---- ------ ---- ---------- ---------- ---------- ----------
1    1    26     145  1234567890 1234567890 1234567890 1234567890
2    1    2      145  1234567890 1234567890 1234567890 1234567890
CES#
```

subinterface

Use this command to create a subinterface or to enter Subinterface Configuration mode. Use the **no** form of the command to delete a subinterface.

Syntax

subinterface <*number*>
no subinterface <*number*>

Parameters

number	Specifies the subinterface number. You can enter a value from 1 through 65535.

Default

0

Command mode

Interface Configuration

Next command mode

Subinterface Configuration (when creating or navigating to a subinterface)
Interface Configuration (when deleting a subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

description
dot1q enable
encapsulation dot1q
filter
ip address
show dot1q
subinterface enable

Example

The following example enters Subinterface Configuration mode for subinterface 3 on Ethernet interface 2/1. If the subinterface does not exist, it will be created.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# subinterface 3
CES(config-subif)#
```

The following example deletes subinterface 3 on Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no subinterface 3
CES(config-if)#
```

subinterface enable

Use this command to enable a subinterface. Use the **no** form of the command to disable a subinterface.

Syntax

subinterface <*number*> **enable**
no subinterface <*number*> **enable**

Parameters

number	Specifies the subinterface number. You can enter a value from 1 through 65535.

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

dot1q enable
show dot1q
show dot1q statistics

Example

The following example enables subinterface 3 on Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# subinterface 3 enable
CES(config-subif)#
```

The following example disables subinterface 3.

```
CES(config-if)# no subinterface 3 enable
CES(config-if)#
```

Configuration example

The following commands create and enable an 802.1Q subinterface as follows:

1. Navigate to the Ethernet interface where you will create the subinterface.
2. Set the encapsulation format on the Ethernet interface to IEEE 802.1Q.
3. Create the VLAN subinterface on the interface.
4. Enable 802.1Q encapsulation on the subinterface and specify a VLAN ID (14) for the subinterface.
5. Assign an IP address and mask to the subinterface.
6. Specify a filter for the subinterface.
7. Enable the VLAN.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# dot1q enable
CES(config-if)# subinterface 2
CES(config-subif)# encapsulation dot1q 14
CES(config-subif)# ip address 10.10.10.1 255.255.255.0
CES(config-subif)# filter “permit all”
CES(config-subif)# exit
CES(config-if)# subinterface 2 enable
CES(config-if)#
```

Chapter 23
IP interface configuration commands

This chapter describes IP interface configuration commands.

Command	Page
ip address	1160
ip multicast-relay boundary	1161
ip ospf	1163
ip ospf authentication-key	1165
ip ospf cost	1166
ip ospf dead-interval	1168
ip ospf hello-interval	1169
ip ospf message-digest-key	1171
ip ospf network	1172
ip ospf poll-interval	1174
ip ospf priority	1175
ip ospf retransmit-interval	1177
ip ospf transmit-delay	1178
ip rip	1180
ip rip authentication mode	1181
ip rip cost	1183
ip rip export-bgp-metric	1185
ip rip export-bo-static-metric	1186
ip rip export-default-metric	1187
ip rip export-ospf-metric	1189
ip rip export-static-metric	1190

Command	Page
ip rip import-default	1192
ip rip poison-reverse	1194
ip rip receive version	1195
ip rip send version	1197
ip vrrp	1198
ip vrrp backup	1200
ip vrrp backup disable	1201
ip vrrp backup enable	1203
ip vrrp master	1204
show ip int	1204

ip address

Use this command to set the primary or secondary ip address and mask for the current interface. The **no** form of the command clears out the IP address and subnet mask for the interface. Only public interfaces may get their IP addresses from the DHCP server.

ip address *<ipAddr>* *<mask>* **secondary**

ip address dhcp {**cancel** | **cost** *<cosm>* | **reacquire**| **default lease-time**| **disallow-rfc-1918**}

no ip address *<ipAddr>* *<mask>*

Parameters

ipAddr	Specifies the primary static IP address for the interface.
mask	Specifies the IP subnet mask for the interface.
secondary	Specifies the secondary static IP address for the interface (multinet address).
dhcp	Specify that the interface should obtain its IP address from a DHCP server.

cancel	Cancel previously requested dynamic IP address.
cost	Set the cost for the interface.
costNum	Specifies the DHCP cost for this interface. Enter an integer from 0 through 65535.
reacquire	Force the DHCP client to release its currently assigned IP address and request another address from the DHCP server.
default lease-time	Sets the default lease-time
disallow rfc-1918	Disallows rfc-1918

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Example

```
CES(config-if)# ip address 1.2.3.4 255.255.255.0
CES(config-if)# ip address dhcp cost 10
CES(config-if)# ip address dhcp reacquire
CES(config-if)# ip address dhcp cancel
```

ip multicast-relay boundary

Use this command to add an IP interface to the multicast boundary list. Use the **no** form of the command to remove the IP interface from the multicast boundary list.

Syntax

```
ip multicast-relay boundary <access_list> {disable | enable}
no ip multicast-relay boundary <access_list>
```

Parameters

access_list	Specifies the access list to apply to the interface.
disable	Disable the interface for multicast relay.
enable	Enable the interface for multicast relay.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Access list <name> does not exist
```

Example

The following example adds the interface to the multicast boundary list and enables the interface for multicast relay.

```
CES(config-if)# ip multicast-relay boundary
permit_10.254.1.x enable
CES(config-if)#
```

The following example disables the interface for multicast relay.

```
CES(config-if)# ip multicast-relay boundary
permit_10.254.1.x disable
CES(config-if)#
```

The following example deletes the interface from the multicast boundary list.

```
CES(config-if)# no ip multicast-relay boundary
permit_10.254.1.x
CES(config-if)#
```

ip ospf

Use this command to enable OSPF on the interface. Use the **no** form of the command to disable it. For Multinetting, you can configure OSPF over a secondary address.

Syntax

```
ip ospf
no ip ospf

ip ospf <secondary address>
no ip ospf <secondary address>
```

Parameters

None

Default

Enabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

OSPF on this IP interface should have been configured prior to this.

Warning messages

A warning is displayed if OSPF has not been configured on this interface.

```
OSPF is not configured on interface.
```

Example

```
CES(config-if)# ip ospf
CES(config-if)# no ip ospf
```

ip ospf authentication-key

Use this command to enable OSPF simple password authentication. Use the **no** form or the command to remove OSPF password authentication.

Syntax

no ip ospf authentication-key
ip ospf authentication-key <*key*> <*ip address*>

Parameters

key	Alphanumeric password; maximum length 16.
ip address	The IP address of the interface.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

A warning is displayed if OSPF has not been configured on this interface.

```
% OSPF is not configured on an interface.
```

Example

This example sets the interface to be in simple authentication mode with password "123456789" for IP address 70.70.70.70.

```
CES(config-if)# ip ospf authentication-key 123456789
70.70.70.70
```

This example removes the authentication.

```
CES(config-if)# no ip ospf authentication-key
```

ip ospf cost

Use this command to specify the cost of sending a packet on an OSPF interface. Use the **no** form of the command to reset the cost to its default value, 10.

Syntax

```
ip ospf cost <cost>
no ip ospf cost

ip ospf cost <cost> <secondary address>
no ip ospf cost <secondary address>
```

Parameters

cost	Cost of the route on an interface. Range is from 1 through 65535.

Default

10

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

A warning is displayed if OSPF has not been configured on this interface.

```
OSPF is not configured on an interface
```

Example

This example sets the OSPF cost to 20.

```
CES(config-if)# ip ospf cost 20
```

This example sets the OSPF cost back to 10.

```
CES(config-if)# no ip ospf cost
```

ip ospf dead-interval

Use this command to set the number of seconds since Hello packets were seen before its neighbors declare the OSPF routers down, as well as on a secondary address. The **no** form sets it back to the default value. The dead interval should be 4 times the Hello interval.

Syntax

```
ip ospf dead interval <seconds>
ip ospf dead interval <seconds><secondary address>
```

Parameters

seconds	The number of seconds that can elapse between Hello packets. Range is from 1 through 65535.

Default

40 seconds

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

A warning is displayed if OSPF has not been configured on this interface.

```
% OSPF is not configured on an interface.
```

A warning is also displayed if the dead interval is less than 4 times the Hello interval.

```
Dead interval has been at least 4 times the hello interval.
```

Example

This example sets the dead interval to 50.

```
CES(config-if)# ip ospf dead-interval 50
```

This example sets the dead interval back to 40.

```
CES(config-if)# no ip ospf dead-interval
```

ip ospf hello-interval

Use this command to set the rate at which Hello packets are sent on an OSPF interface or on a secondary address. Use the **no** form of the command to set it to the default value of 10.

Syntax

```
ip ospf hello interval <seconds>
no ip ospf hello interval

ip ospf hello interval <seconds> <secondary address>
no ip ospf hello interval <secondary address>
```

Parameters

seconds	The number of seconds that can elapse between Hello packets. Range is from 1 through 65535.

Default

10 seconds

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

A warning is displayed if OSPF has not been configured on this interface.

```
% OSPF is not configured on an interface.
```

Example

This example sets the Hello interval to 20.

```
CES(config-if)# ip ospf hello-interval 20
```

This example sets the Hello interval back to 10.

```
CES(config-if)# no ip ospf hello-interval
```

ip ospf message-digest-key

Use this command to enable OSPF MD5 authentication. Use the **no** form of the command to remove OSPF MD5 authentication. You cannot remove or change the key ID alone. To change a key ID, you must retype the entire command with the new key ID and key.

Syntax

ip ospf message-digest-key <*keyid*> **md5** <*key*>
no ip ospf message-digest-key

ip ospf message-digest-key <*keyid*> **md5** <*key*> <*secondary address*>
no ip ospf message-digest-key <*secondary address*>

Parameters

keyid	Numeric value; ranges from 1 to 255.
key	Alphanumeric password; maximum length 16.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

A warning is displayed if OSPF has not been configured on this interface.

```
% OSPF is not configured on an interface.
```

Example

This example sets MD5 authentication with password “1234.”

```
CES(config-if)# ip ospf message-digest-key 2 md5 1234
```

This example removes MD5 authentication.

CES(config-if)# **no ip ospf message-digest-key**

ip ospf network

Use this command to configure the OSPF network type for a specified interface. Use the **no** form of the command to reset the network type to its default value, broadcast mode.

Syntax

```
ip ospf network {broadcast | point-to-point}
no ip ospf network

ip ospf network {broadcast | point-to-point}<secondary
address>
no ip ospf network <secondary address>
```

Parameters

broadcast	Specifies broadcast network.
point-to-point	Specifies point-to-point network.

Default

Broadcast mode

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

A warning is displayed if OSPF has not been configured on this interface.

```
% OSPF is not configured on an interface
```

Example

Sets the interface to be point-to-point.

```
CES(config-if)# ip ospf network point-to-point
```

Sets the interface to be default.

```
CES(config-if)# no ip ospf network
```

ip ospf poll-interval

Use this command to set the OSPF poll interval. The poll interval is the longest time (in seconds) allowed between Hello packets sent to an inactive neighbor. The default poll interval is 120 seconds. Use the **no** form of the command to set the poll interval to the default value of 120.

Syntax

```
ip ospf poll interval <seconds>
no ip ospf poll interval

ip ospf poll interval <seconds> <secondary address>
no ip ospf poll interval <secondary address>
```

Parameters

seconds	Specifies the number of seconds that can elapse between Hello packets sent to an inactive neighbor. Enter an integer from 1 through 65535.

Default

120 seconds

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

A warning is displayed if OSPF has not been configured on this interface.

```
% OSPF is not configured on an interface.
```

Example

The following example sets the poll interval to 320 seconds.

```
CES(config-if)# ip ospf poll-interval 320
```

The following example resets the poll interval to 120 seconds.

```
CES(config-if)# no ip ospf poll-interval
```

ip ospf priority

Use this command to set the priority to help determine the OSPF designated router for a network. The **no** form of the command sets it to the default value of 1.

Syntax

ip ospf priority <*number*>
ip ospf priority <*number*><*secondary address*>

Parameters

number	Numerical value; ranges from 0 through 255.

Default

1

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

A warning is displayed if OSPF has not been configured on this interface.

```
% OSPF is not configured on an interface.
```

Example

```
CES(config-if)# ip ospf priority 0
```

ip ospf retransmit-interval

Use this command to specify the number of seconds between link state advertisement retransmissions for adjacencies belonging to the OSPF interface. Use the **no** form of the command to reset the retransmission interval to its default value, 5 seconds.

Syntax

```
ip ospf retransmit-interval <seconds>
no ip ospf retransmit-interval

ip ospf retransmit-interval <seconds><secondary address>
no ip ospf retransmit-interval<secondary address>
```

Parameters

seconds	Specifies the interval between link state advertisement retransmissions for adjacencies. Type an integer from 1 through 3600.

Default

5 seconds

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

A warning is displayed if OSPF has not been configured on this interface.

```
% OSPF is not configured on an interface.
```

Example

This example sets the retransmission interval to 10.

```
CES(config-if)# ip ospf retransmission-interval 10
```

This example sets the retransmission interval back to 5.

```
CES(config-if)# no ip ospf retransmission-interval
```

ip ospf transmit-delay

Use this command to set the estimated number of seconds it takes to retransmit a link state update packet on an OSPF interface. The **no** form sets it back to the default value.

Syntax

```
ip ospf transmit-delay <seconds>
no ip ospf transmit-delay

ip ospf transmit-delay <seconds><secondary address>
no ip ospf transmit-delay <secondary address>
```

Parameters

seconds	Delay in seconds. Range is from 1 through 3600.

Default

1 second

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

A warning is displayed if OSPF has not been configured on this interface.

```
% OSPF is not configured on an interface.
```

Example

This example sets the transmit delay to 30.

```
CES(config-if)# ip ospf transmit-delay 30
```

This example sets the transmit delay back to the default.

```
CES(config-if)# no ip ospf transmit-delay
```

ip rip

Use this command to enable RIP on the interface as well as on a secondary address. Use the **no** form of the command to disable RIP.

Syntax

```
ip rip
no ip rip

ip rip <secondary address>
no ip rip <secondary address>
```

Parameters

None

Default

Enabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The IP interface should have been created prior to this and RIP should have been configured on this interface.

Warning messages

```
% RIP is not configured on this interface.
```

Example

```
CES(config-if)# ip rip
CES(config-if)# no ip rip
```

ip rip authentication mode

Use this command to enable plain-text or MD5 authentication on a RIP interface. If you configure RIP to use MD5 authentication, you can also use this command to enable RFC 2082 compliance if the Nortel VPN Router must communicate with a network device that implements RFC 2082 compliant MD5. (By default, MD5 on the Nortel VPN Router does not comply with RFC 2082.) Use the **no** form of the command to disable RFC 2082 compliance or to disable authentication.

Syntax

ip rip authentication mode {**none** | **text** <*password*> | **md5** <*password*> [<*key-ID*>] | **rfc2082**}
no ip rip authentication mode [**md5 rfc2082**]

ip rip authentication mode {**none** | **text** <*password*> | **md5** <*password*> [<*key-ID*>] | **rfc2082**} <*secondary address*>
no ip rip authentication mode [**md5 rfc2082**] <*secondary address*>

Parameters

none	Specify no authentication for RIP.
text	Specify simple text authentication.
md5	Specify MD5 authentication.
rfc2082	Enable or disable RFC 2082 compliance for MD5 authentication.
password	Specifies an alphanumeric password for simple or MD5 authentication.
key-ID	Specifies a numeric key to be used with the MD5 password if you enable RFC 2082 compliance. Type an integer from 0 through 255. You must specify a key ID if the Nortel VPN Router is communicating with an RFC 2082 compliant device.

Default

The default authentication is none.

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

You can enable RIP authentication only if you are sending or receiving RIP Version 2 packets.

Warning messages

```
% RIP is not configured on this interface.
% Not supported for RIP version 1
```

Example

The following example configures RIP on the interface to use a simple text password (abc123) for authentication.

```
CES(config-if)# ip rip authentication mode text abc123
```

The following example configures RIP on the interface to use MD5 authentication in compliance with RFC 2082. To comply with RFC 2082, you must specify a key ID (0-255) as well as a password.

```
CES(config-if)# ip rip authentication mode md5 rfc2082
CES(config-if)# ip rip authentication mode md5 s792gyz 22
```

The following example disables RFC 2082 compliance for MD5.

```
CES(config-if)# no ip rip authentication mode md5 rfc2082
```

The following example configures RIP to use no authentication.

```
CES(config-if)# no ip rip authentication mode
```

ip rip cost

Use this command to set the cost of the RIP interface.

Syntax

ip rip cost <*cost*>
ip rip cost <*cost*> <*secondary address*>

Parameters

cost	Specifies an interface cost from 1 through 15 (default is 1).

Default

1

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The IP interface was created and RIP is configured on the interface.

Warning messages

```
% RIP is not configured on this interface.
```

Example

The following example sets the RIP interface cost to 10.

```
CES(config-if)# ip rip cost 10
CES(config-if)#
```

ip rip export-bgp-metric

Use this command to set and reset the BGP metric.

Syntax

ip rip export-bgp-metric <*value*>
no ip rip export-bgp-metric

Parameters

value	Specifies the BGP metric. Type an integer from 1 through 15.

Default

1

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The IP interface was created and RIP is configured on the interface.

Warning messages

```
% RIP is not configured on this interface.
```

Example

In the first example, the BGP will be sent out as RIP routes with a metric of 10. In the second example, the **no** form resets the metric to the default value of 1.

```
CES(config-if)# ip rip export-bgp-metric 10
CES(config-if)# no ip rip export-bgp-metric 10
```

ip rip export-bo-static-metric

Use this command to set and reset the branch office (BO) static route metric.

Syntax

```
ip rip export-bo-static-metric <value>
no ip rip export-bo-static-metric

ip rip export-bo-static-metric <value> <secondary address>
no ip rip export-bo-static-metric <secondary address>
```

Parameters

value	Specifies the static route metric. Type an integer from 1 through 15.

Default

1

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The IP interface was created and RIP is configured on the interface.

Warning messages

```
% RIP is not configured on this interface.
```

Example

In the first example, the branch office static routes will be sent out as RIP routes with a metric of 10. In the second example, the **no** form resets the metric to the default value of 1.

```
CES(config-if)# ip rip export-bo-static-metric 10
CES(config-if)# no ip rip export-bo-static-metric
```

ip rip export-default-metric

Use this command to set and reset the default route metric. <*secondary address*>

Syntax

```
ip rip export-default-metric <value>
no ip rip export-default-metric

ip rip export-default-metric <value><secondary address>
no ip rip export-default-metric <secondary address>
```

Parameters

value	Numeric value; ranges from 1 through 15.

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The IP interface should have been created prior to this and RIP should have been configured on this interface.

Warning messages

```
% RIP is not configured on this interface.
```

Example

In the first example, the default route is sent with a metric of 3 on this interface. In the second example, the **no** form disables sending default route on this interface.

```
CES(config-if)# ip rip export-default-metric 3
CES(config-if)# no ip rip export-default-metric
```

ip rip export-ospf-metric

Use this command to set and reset the OSPF route metric.

Syntax

ip rip export-ospf-metric <*value*>
no ip rip export-ospf-metric

ip rip export-ospf-metric <*value*><*secondary address*>
no ip rip export-ospf-metric <*secondary address*>

Parameters

value	Numeric value; ranges from 1 through 15.

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The IP interface should have been created prior to this and RIP should have been configured on this interface.

Warning messages

```
% RIP is not configured on this interface.
```

Example

In the first example, the OSPF routes are sent out as RIP routes with a metric of 10. In the second example, the **no** form disables sending OSPF routes on this interface.

```
CES(config-if)> ip rip export-ospf-metric 10
CES(config-if)> no ip rip export-ospf-metric
```

ip rip export-static-metric

Use this command to set the static route metric. This metric is the relative cost for the gateway. You use a lower number, such as 1, for the least expensive route. If the number is greater than 1, the lowest cost route is the preferred route.

Syntax

```
ip rip export-static-metric <value>
no ip rip export-static-metric

ip rip export-static-metric <value> <secondary address>
no ip rip export-static-metric <secondary address>
```

Parameters

value	Specifies the static route metric. Type an integer from 1 through 15.

Default

1

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% RIP is not configured on this interface.
```

Example

In the first example, the static routes are sent out as RIP routes with a metric of 10 on this interface. In the second example, the **no** form resets the metric to 1.

```
CES(config-if)# ip rip export-static-metric 10
CES(config-if)# no ip rip export-static-metric
```

ip rip import-default

Use this command to enable importing of a default route. Use the **no** form of the command to disable importing a default route.

Syntax

```
ip rip import-default
no ip rip import-default

ip rip import-default <secondary address>
no ip rip import-default <secondary address>
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The IP interface should have been created prior to this and RIP should have been configured on this interface.

Warning messages

```
% RIP is not configured on this interface.
```

Example

```
CES(config-if)# ip rip import-default
CES(config-if)# no ip rip import-default
```

ip rip poison-reverse

Use this command to enable RIP poison reverse. Using split horizon with poison reverse, the gateway sends back the routes that it learns from a neighboring router, but it sets the metric for the connection to infinity. Use the **no** form of the command to disable poison reverse.

Syntax

```
ip rip poison-reverse
no ip rip poison-reverse

ip rip poison-reverse <secondary address>
no ip rip poison-reverse <secondary address>
```

Parameters

None

Default

Poison reverse is enabled.

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The IP interface should have been created prior to this and RIP should have been configured on this interface.

Warning messages

```
% RIP is not configured on this interface.
```

Example

The following example enables and then disables poison reverse:

```
CES(config-if)# ip rip poison-reverse
CES(config-if)# no ip rip poison-reverse
```

ip rip receive version

Use this command to set the versions of RIP that the interface will receive (only Version 1 or 2, both versions, or neither). Use the **no** form of the command to reset the RIP versions received to the default value, RIP Version 2 only.

Syntax

ip rip receive version {**none** | **1** | **2** | **1 2**}
no ip rip receive version

ip rip receive version {**none** | **1** | **2** | **1 2**} <*secondary address*>
no ip rip receive version <*secondary address*>

Parameters

none	Receive no RIP updates.
1	Receive RIP Version 1 only.

2	Receive RIP Version 2 only.
1 2	Receive RIP Version 1 and 2 both.

Default

RIP Version 2 only

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

The IP interface has been created and RIP is configured on the interface.

Warning messages

```
% RIP is not configured on this interface.
```

Related commands

`ip rip send version`

Example

The first example sets the receive version to be both and the **no** form sets it back to version 2 only.

```
CES(config-if)# ip rip receive version 1 2
CES(config-if)# no ip rip receive version
```

ip rip send version

Use this command to set the versions of RIP that the interface will send (Version 1, Version 2, or both versions). Use the **no** form of the command to reset the RIP version sent to the default value, RIP Version 2 only.

Syntax

```
ip rip send version {none | 1 | 2}
no ip rip send version

ip rip send version {none | 1 | 2} <secondary address>
no ip rip send version <secondary address>
```

Parameters

none	Send no RIP updates.
1	Send RIP Version 1 only.
2	Send RIP Version 2 only.

Default

RIP Version 2 only

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – Manage

Prerequisites

The IP interface should have been created prior to this and RIP should have been configured on this interface.

Warning messages

```
% RIP is not configured on this interface.
```

Related commands

ip rip receive version

Example

The first example sets the sending version number to be 1 and the **no** form sets it back to version 2.

```
CES(config-if)# ip rip send version 1
CES(config-if)# no ip rip send version
```

ip vrrp

Use this command to enable VRRP on the interface. Use the **no** form of the command to disable VRRP. This command is the first VRRP command that you need to enter to configure VRRP for the interface.

Syntax

ip vrrp
no ip vrrp

Parameters

None

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Warning messages

```
% VRRP not configured on interface.
% This feature is not enabled. Contact your sales
representative to purchase a key to enable this feature. The
key can then be entered using the ‘license install’ command
from Global Configuration mode.
```

Example

```
CES(config-if)# ip vrrp
```

ip vrrp backup

Use this command to specify the backup addresses of other virtual router interfaces that are backing up this router. All backups must be on the same LAN segment. Use the **no** form of the command to delete the backup created.

Syntax

```
ip vrrp backup <ip-address> [priority <priority>]
no ip vrrp backup <ip-address>
```

Parameters

ip-address	Interface IP address of the virtual router backing up this router.
priority	Priority of the backup; enter an integer from 1-253. Priority 254 is reserved for use with the master delay mode.

Default

100

Command mode

Interface Configuration

Next command mode

Interface Configuration

Prerequisites

The backup interface should be in the same subnet as the interface it is backing up.

Warning messages

Command executes unsuccessfully if the backup is not in the same subnet as the interface it is backing up.

```
% VRRP address x.x.x.x does not exist.
% VRRP not configured on interface.
% This feature is not enabled. Contact your sales
representative to purchase a key to enable this feature. The
key can then be entered using the ‘license install’ command
from Global Configuration mode.
```

Related commands

ip vrrp backup <*ip-address*> **enable**
ip vrrp backup <*ip-address*> **disable**

Example

This example sets 10.0.3.191 on another virtual router as a backup for this router interface.

```
CES(config-if)# ip vrrp backup 10.0.3.191
```

This example sets 10.0.3.191 as a backup for this interface and overrides the default priority by setting to 150.

```
CES(config-if)# ip vrrp backup 10.0.3.191 priority 150
```

This example deletes the backup interface previously created on 10.0.3.191.

```
CES(config-if)# no ip vrrp backup 10.0.3.191
```

ip vrrp backup disable

Use this command to disable the backup interface created.

Syntax

ip vrrp backup <*ip-address*> **disable**

Parameters

ip-address	Interface address of the backup to disable.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Prerequisites

The backup interface should be created prior to disabling.

Related commands

ip vrrp backup

Example

This example disables the backup on 10.0.3.191.

```
CES(config-if)# ip vrrp backup 10.0.3.191 disable
```

ip vrrp backup enable

Use this command to enable the backup interface created.

Syntax

ip vrrp backup <*ip-address*> **enable**

Parameters

ip-address	Interface address of the backup to enable.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Prerequisites

The backup interface should be created prior to enabling.

Related commands

ip vrrp backup

Example

This example enables the backup on 10.0.3.191.

```
CES(config-if)# ip vrrp backup 10.0.3.191 enable
```

ip vrrp master

Use this command to enable mastership on the interface on which VRRP is running. Typically every virtual router is its own master and can be a backup to other virtual routers on the same or different LAN. Use the **no** form of the command to disable mastership.

Syntax

```
ip vrrp master
no ip vrrp master
```

Parameters

None

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Prerequisites

This interface needs to be configured as a virtual router prior to enabling its master status. This should be specified in the context of the VRRP process.

Warning messages

If the advanced routing feature is not paid for, then this command aborts with a warning message. Also, this interface must be configured as a virtual router for it to assume the role of a master.

```
% VRRP address x.x.x.x does not exist.
% VRRP not configured on interface.
% This feature is not enabled. Contact your sales
representative to purchase a key to enable this feature. The
key can then be entered using the ‘license install’ command
from Global Configuration mode.
```

Related commands

ip vrrp backup
ip vrrp backup priority

Example

```
CES(config-if)# ip vrrp master
CES(config-if)# no ip vrrp master
```

show ip int

Syntax

show ip int

Parameters

Default

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

Example

```
CES# show ip int
```

Chapter 24
Circuitless IP interface configuration commands

This chapter describes configuration commands for circuitless IP interfaces.

Command	Page
clip enable	1208
clip ip	1209
clip ip interface-type	1211
clip ip services	1213
clip ip state	1215
show clip	1216
show clip services	1218

clip enable

Use this command to globally enable and disable the circuitless IP (CLIP) capability on the gateway. Use the **no** form of the command to disable circuitless IP on the gateway.

Syntax

```
clip enable
no clip enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

clip ip
clip ip interface-type
clip ip services
clip ip state
show clip
show clip services

Example

The following example enables circuitless IP on the gateway.

```
CES# configure terminal
CES(config)# clip enable
CES(config)#
```

The following example disables circuitless IP on the gateway.

```
CES(config)# no clip enable
CES(config)#
```

clip ip

Use this command to create a circuitless IP interface. You can create as many as six circuitless IP interfaces. Use the **no** form of the command to delete the circuitless IP interface.

Syntax

clip ip <*ip-address*>
no clip ip <*ip-address*>

Parameters

ip-address	Specifies in dotted-decimal notation the IP address of the circuitless interface.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

clip enable
clip ip interface-type
clip ip services
clip ip state
show clip
show clip services

Example

The following example specifies the circuitless IP address 190.160.1.100.

```
CES# configure terminal
CES(config)# clip ip 190.160.1.100
CES(config)#
```

The following example deletes the circuitless IP address 190.160.1.100.

```
CES(config)# no clip ip 190.160.1.100
CES(config)#
```

clip ip interface-type

Use this command to specify the interface type for a circuitless IP interface. Depending on the interface type that you configure with this command, the circuitless IP interface terminates tunnels initiated from the private side of the gateway, the public side, both private and public, or neither. For example, if you set the interface type to private, the circuitless IP interface can terminate tunnels initiated from the private side of the gateway only.

Syntax

clip ip <*ip-address*> [**interface-type** {**both** | **none** | **private** | **public**}]

Parameters

ip-address	Specifies in dotted-decimal notation the IP address of the circuitless interface.
interface-type	Specifies the interface type: private, public, both, or none.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

clip enable
clip ip
clip ip services
clip ip state
show clip
show clip services

Example

The following example sets the interface type for circuitless IP address 190.160.1.100 to public. Only tunnels initiated on the public side of the gateway can be terminated at this circuitless IP address.

```
CES# configure terminal
CES(config)# clip ip 190.160.1.100 interface-type public
CES(config)#
```

clip ip services

Use this command to specify the services for this circuitless IP address and whether the services are available on the private side of the gateway, the public side, or both.

Syntax

clip ip <*ip-address*> **services** {**fwua** | **ipsec** | **l2tp&l2f** | **pptp**} {**none** | **public** | **private** | **both**}

Parameters

ip-address	Specifies in dotted-decimal notation the IP address of the circuitless IP interface.
fwua	Specifies whether the firewall user authentication service (FWUA) is supported on the public side, the private side, both sides, or neither.
ipsec	Specifies whether the IPsec service is supported on the public side, the private side, both sides, or neither.
l2tp&l2f	Specifies whether the L2TP and L2F services are supported on the public side, the private side, both sides, or neither.
pptp	Specifies whether the PPTP service is supported on the public side, the private side, both sides, or neither.

Default

FWUA is disabled; IPsec, L2TP, L2F, and PPTP are enabled on both public and private interfaces.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

clip enable
clip ip
clip ip interface-type
clip ip state
show clip
show clip services

Example

The following example configures the circuitless IP address 190.160.1.100 to allow firewall user authentication traffic for public interfaces and to disallow PPTP traffic on both public and private interfaces.

```
CES# configure terminal
CES(config)# clip ip 190.160.1.100 services fwua public
CES(config)# clip ip 190.160.1.100 services pptp none
CES(config)#
```

clip ip state

Use this command to enable or disable a circuitless IP interface.

Syntax

clip ip <*ip-address*> **state** {**enable** | **disable**}

Parameters

ip-address	Specifies in dotted-decimal notation the IP address of the circuitless interface.

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

clip enable
clip ip
clip ip interface-type
clip ip services
show clip
show clip services

Example

The following example globally enables circuitless IP on the gateway and then enables the circuitless IP address 190.160.1.100.

```
CES# configure terminal
CES(config)# clip enable
CES(config)# clip ip 190.160.1.100 state enable
CES(config)#
```

show clip

Use this command to display configuration information about all the circuitless IP interfaces configured on the gateway.

Syntax

show clip

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - View
User Management - None

Related commands

clip enable
clip ip
clip ip interface-type
clip ip services
clip ip state
show clip services

Example

The following example displays information about the configured circuitless IP addresses on the gateway.

```
CES# show clip

Configured Circuitless IP
  CLIP: Enabled
  CLIP Address     State       Interface Type
  190.160.1.100    enabled     public
  190.168.1.100    disabled    private
CES#
```

show clip services

Use this command to display the configuration of tunneling services for the circuitless IP addresses on the gateway.

Syntax

```
show clip services
```

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - View
User Management - None

Related commands

clip enable
clip ip
clip ip interface-type
clip ip services
clip ip state
show clip

Example

The following example displays information about the services allowed on each circuitless IP interface.

```
CES# show clip services

Allowed Circuitless Services

  CLIP Address    IPSEC     PPTP      L2TP&L2F   FWUA
  -------------   --------  ----      --------   ----
  190.160.1.100   public    both      none       private
  193.168.1.100   private   private   public     none
CES#
```

Chapter 25
PPP over Ethernet configuration commands

This chapter describes Point-to-Point Protocol over Ethernet (PPPoE) configuration commands.

Command	Page
debug interface fastethernet pppoe	1222
interface	1223
pppoe admin-state enable	1224
pppoe cost	1226
pppoe enable	1228
pppoe idle-timeout	1229
pppoe ip local	1231
pppoe ip tcp adjust-mss enable	1233
pppoe on-demand enable	1234
pppoe ppp authentication	1236
pppoe ppp ipcp vj-connect-id-compression-negotiation	1238
pppoe ppp ipcp vj-max-slots	1239
pppoe ppp ipcp vj-negotiation	1241
pppoe ppp lcp echo-fault-threshold	1242
pppoe ppp lcp echo-interval	1243
pppoe ppp lcp protocol-field-compression	1245
pppoe ppp username	1246
pppoe service-name	1248
show interface pppoe	1249
PPPoE configuration example	1252

debug interface fastethernet pppoe

Use this command to start debug-level logging for PPPoE on the LAN interface. Use the **no** form of the command to stop the logging of debug messages.

Syntax

```
debug interface fastethernet <slot/port> pppoe
no debug interface fastethernet <slot/port> pppoe
```

Parameters

slot	Specifies the slot of the LAN interface.
port	Specifies the port of the LAN interface.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe enable

Warning messages

```
% Interface <slot/port> does not exist
```

Example

The following example starts debug logging for PPPoE on interface 1/1.

```
CES# debug interface fastethernet 1/1 pppoe
CES#
```

The following example stops debug logging for PPPoE on interface 1/1.

```
CES# no debug interface fastethernet 1/1 pppoe
CES#
```

interface

Use this command to configure PPP over Ethernet (PPPoE) on the LAN interface. Use the **no** form of this command to delete the PPPoE interface.

Syntax

```
interface <type> <slot/port>
no interface <type> <slot/port>
```

Parameters

type	Specifies the interface type. For PPP over Ethernet, the value of this parameter is **fastethernet**.
slot	Specifies the slot of the LAN interface.
port	Specifies the port of the LAN interface.

Default

None

Command mode

Global Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe enable
show interface fastethernet pppoe

Warning messages

% Interface <*slot/port*> does not exist

Example

The following example configures PPPoE on a LAN interface.

```
CES# configure terminal
CES(config)# interface fastethernet 1/1
CES(config-if)#
```

pppoe admin-state enable

Use this command to enable PPPoE on a LAN interface, that is, to set the administrative state to “enabled.” Use the **no** form of this command to disable PPPoE on the interface.

Syntax

```
pppoe admin-state enable
no pppoe admin-state enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
pppoe enable
pppoe on-demand enable
show interface fastethernet pppoe
```

Example

The following example configures and enables PPPoE on LAN interface 1/1.

```
CES# configure terminal
CES(config)# interface fastethernet 1/1
CES(config-if)# pppoe enable
CES(config-if)# pppoe admin-state enable
```

pppoe cost

Use this command to set the PPPoE cost attribute. Use the **no** form of the command to revert to the default cost value: 1 for Ethernet interfaces; 20 for ATM subinterfaces.

Syntax

pppoe cost <*value*>
no pppoe cost

Parameters

value	Specifies the cost of the interface or subinterface configured for PPPoE. Enter an integer from 1–2,097,150.

Default

1 (Ethernet interface)
20 (ATM subinterface)

Command mode

Interface Configuration (Ethernet interface)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (Ethernet interface)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe idle-timeout
pppoe ip tcp adjust-mss enable
pppoe on-demand enable
pppoe service-name
show interface

Example

The following example sets the PPPoE cost attribute for the subinterface on ATM interface 3/1.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# encapsulation pppoesnap
CES(config-subif)# pppoe cost 1000
CES(config-subif)#
```

The following example removes the PPPoE cost attribute from Fast Ethernet interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no pppoe cost
CES(config-if)#
```

pppoe enable

Use this command to set the protocol encapsulation method on the LAN interface to PPP over Ethernet (PPPoE). Use the **no** form of this command to set the encapsulation method to its default value (IP).

Syntax

```
pppoe enable
no pppoe enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
interface fastethernet
pppoe admin-state enable
pppoe on-demand enable
show interface fastethernet pppoe
```

Example

The following example adds PPPoE to LAN interface 1/1 and specifies PPPoE as the protocol encapsulation method for the interface.

```
CES(config)# interface fastethernet 1/1
CES(config-if)# pppoe enable
CES(config-if)#
```

The following command removes PPPoE as the encapsulation method for the LAN interface and reverts to the default encapsulation method (IP encapsulation).

```
CES(config-if)# no pppoe enable
```

pppoe idle-timeout

Use this command to set the PPPoE idle timeout value. The idle timeout is the number of minutes that can elapse with no activity before the interface terminates the connection. Set the idle timeout only if you configured PPPoE for on-demand activation. Use the **no** form of the command to revert to the default timeout, 15 minutes.

Syntax

```
pppoe idle-timeout <minutes>
no pppoe idle-timeout
```

Parameters

minutes	Specifies the idle timeout value for PPPoE in minutes. Enter an integer from 1–71,582,788. A value of 0 disables the idle timeout timer.

Default

15 minutes

Command mode

Interface Configuration (Ethernet interface)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (Ethernet interface)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe cost
pppoe ip tcp adjust-mss enable
pppoe on-demand enable
pppoe service-name
show interface

Example

The following example configures PPPoE for on-demand operation, configures an interface filter, and specifies an idle timeout value of 60 minutes.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# pppoe on-demand enable
CES(config-if)# filter permit-ftp
CES(config-if)# pppoe idle-timeout 60
CES(config-if)#
```

The following example resets the PPPoE idle timeout for the subinterface on ATM interface 3/1 to the default value, that is, 15 minutes.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# no pppoe idle-timeout
CES(config-subif)#
```

pppoe ip local

Use this command to specify a static IP address for the local PPPoE LAN interface. Use the **no** form of this command to revert to the default address, 0.0.0.0. The default setting allows the local IP address to be assigned by the ISP.

Syntax

pppoe ip local <*address*>
no pppoe ip local

Parameters

address	Specifies in dotted-decimal notation the IP address of the local LAN interface.

Default

The default value, 0.0.0.0, allows the local IP address to be acquired through dynamic routing.

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
pppoe admin-state enable
pppoe enable
show interface fastethernet pppoe
```

Example

The following example configures and enables PPPoE on LAN interface 1/1 and assigns a static IP address to the interface.

```
CES(config)# interface fastethernet 1/1
CES(config-if)# pppoe enable
CES(config-if)# pppoe admin-state enable
CES(config-if)# pppoe ip local 192.10.10.1
CES(config-if)#
```

pppoe ip tcp adjust-mss enable

PPPoE enforces an MTU size of 1492 bytes. For this reason, all PCs that connect to the Nortel VPN Router also need to enforce an MTU of 1492 bytes, instead of the usual 1500 bytes. If it is impractical to change the MTU for your PCs, you can use this command as a workaround. Use the **no** form of the command to revert to the default setting.

Syntax

```
pppoe ip tcp adjust-mss enable
no pppoe ip tcp adjust-mss enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration (Ethernet interface)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (Ethernet interface)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe cost
pppoe idle-timeout
pppoe on-demand enable
pppoe service-name
show interface

Example

The following example configures the ATM subinterface to accommodate an MTU size of 1500 bytes on all connecting PCs.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# pppoe ip tcp adjust-mss enable
CES(config-subif)#
```

The following example disables the TCP adjust MSS function.

```
CES(config)# interface fastethernet 1/1
CES(config-if)# no pppoe ip tcp adjust-mss enable
CES(config-if)#
```

pppoe on-demand enable

Use this command to allow on-demand connections for the PPPoE interface. Use the **no** form of the command to disallow on-demand connections.

Syntax

```
pppoe on-demand enable
no pppoe on-demand enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration (Ethernet interface)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (Ethernet interface)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

```
pppoe cost
pppoe idle-timeout
pppoe ip tcp adjust-mss enable
pppoe service-name
show interface
```

Example

The following example enables PPPoE on an Ethernet interface and configures PPPoE for on-demand operation.

```
CES(config)# interface fastethernet 1/1
CES(config-if)# pppoe enable
CES(config-if)# pppoe admin-state enable
CES(config-if)# filter permit-ftp
CES(config-if)# pppoe on-demand enable
CES(config-if)#
```

The following example disables on-demand connections on the subinterface of ATM interface 3/1.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# no pppoe on-demand enable
CES(config-subif)#
```

pppoe ppp authentication

Use this command to enable the Challenge Handshake Authentication Protocol (CHAP) or the Password Authentication Protocol (PAP) for PPPoE sessions. Use the **no** form of the command to disable the authentication protocol. After you enable CHAP or PAP, use the **pppoe ppp username** command to set the CHAP or PAP user ID and password.

Syntax

```
pppoe ppp authentication {chap | pap}
no pppoe ppp authentication
```

Parameters

chap	Enables the Challenge Handshake Authentication Protocol (CHAP) on this interface.
pap	Enables the Password Authentication Protocol (PAP) on this interface.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe ppp username
show interface fastethernet pppoe

Example

The following example enables PAP authentication for PPPoE sessions on this interface and then sets the PAP user ID and password.

```
CES(config-if)# pppoe ppp authentication pap
CES(config-if)# pppoe ppp username george13 password
eewG32L=73
CES(config-if)#
```

pppoe ppp ipcp vj-connect-id-compression-negotiation

Use this command to enable or disable Van Jacobson (VJ) connect ID compression negotiation. In conjunction with VJ compression negotiation, VJ connect ID compression negotiation further reduces the TCP/IP packet header to increase packet transmission performance.

Syntax

```
pppoe ppp ipcp vj-connect-id-compression-negotiation
{disable | enable}
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe on-demand enable
pppoe ppp ipcp vj-max-slots
pppoe ppp ipcp vj-negotiation
show interface fastethernet pppoe

Example

The following example enables Van Jacobson compression negotiation and VJ connect ID compression negotiation on the PPPoE interface.

```
CES(config-if)# pppoe on-demand enable
CES(config-if)# pppoe ppp ipcp vj-negotiation enable
CES(config-if)# pppoe ppp ipcp
vj-connect-id-compression-negotiation enable
CES(config-if)#
```

pppoe ppp ipcp vj-max-slots

Use this command to specify the maximum number of concurrent Van Jacobson (VJ) compressed TCP/IP flows.

Syntax

pppoe ppp ipcp vj-max-slots <*value*>

Parameters

value	Specifies the maximum number of concurrent VJ-compressed TCP/IP flows. Enter an integer from 2–16.

Default

8

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe on-demand enable
pppoe ppp ipcp vj-connect-id-compression-negotiation
pppoe ppp ipcp vj-negotiation
show interface fastethernet pppoe

Example

The following example sets the maximum number of VJ-compressed flows to 4.

```
CES(config-if)# pppoe ppp ipcp vj-max-slots 4
CES(config-if)#
```

pppoe ppp ipcp vj-negotiation

Use this command to enable or disable Van Jacobson (VJ) compression negotiation. VJ compression negotiation compresses the TCP/IP header fields on a per TCP/IP flow basis to reduce packet overhead.

Syntax

pppoe ppp ipcp vj-negotiation {**enable** | **disable**}

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
pppoe on-demand enable
pppoe ppp ipcp vj-connect-id-compression-negotiation
pppoe ppp ipcp vj-max-slots
show interface fastethernet pppoe
```

Example

The following example enables Van Jacobson compression negotiation on the PPPoE interface.

```
CES(config-if)# pppoe on-demand enable
CES(config-if)# pppoe ppp ipcp vj-negotiation enable
```

The following example disables VJ compression negotiation on the PPPoE interface.

```
CES(config-if)# pppoe ppp ipcp vj-negotiation disable
```

pppoe ppp lcp echo-fault-threshold

Use this command to specify a value for the Link Control Protocol (LCP) echo fault threshold. The echo fault threshold is the number of consecutive unanswered echo requests that LCP sends before it disconnects the link.

Syntax

pppoe ppp lcp echo-fault-threshold <*value*>

Parameters

value	Specifies the number of consecutive unanswered echo requests the interface sends before it disconnects the link. Enter an integer from 0–255. The value 0 disables the threshold.

Default

1

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe ppp lcp echo-interval
pppoe ppp lcp protocol-field-compression
show interface fastethernet pppoe

Example

The following example sets the number of unanswered echo requests to 2.

```
CES(config-if)# pppoe ppp lcp echo-fault-threshold 2
CES(config-if)#
```

pppoe ppp lcp echo-interval

Use this command to specify the number of seconds between echo requests. You can use this interval with the echo request threshold to determine whether the link has been disconnected.

Syntax

pppoe ppp lcp echo-interval <*seconds*>

Parameters

seconds	Specifies the number of seconds between LCP echo requests. Enter an integer from 0–255.

Default

0

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe ppp lcp echo-fault-threshold
pppoe ppp lcp protocol-field-compression
show interface fastethernet pppoe

Example

The following example sets the LCP echo interval to 2 seconds.

```
CES(config-if)# pppoe ppp lcp echo-interval 2
CES(config-if)#
```

pppoe ppp lcp protocol-field-compression

Use this command to enable or disable LCP protocol field compression. This option compresses the protocol field in the packet header and reduces packet overhead by 1 byte.

Syntax

pppoe ppp lcp protocol-field-compression {**enable** | **disable**}

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe ppp lcp echo-fault-threshold
pppoe ppp lcp echo-interval
show interface fastethernet pppoe

Example

The following example enables LCP protocol field compression.

```
CES(config-if)# pppoe ppp lcp protocol-field-compression
enable
CES(config-if)#
```

The following example disables LCP protocol field compression.

```
CES(config-if)# pppoe ppp lcp protocol-field-compression
disable
CES(config-if)#
```

pppoe ppp username

Use this command to configure the CHAP or PAP user name and password. Use the **pppoe ppp authentication** command to enable CHAP or PAP.

Syntax

pppoe ppp username <*username*> **password** <*password*>

Parameters

username	Specifies the CHAP or PAP user ID for this interface.
password	Specifies the CHAP or PAP user password.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

pppoe ppp authentication
show interface fastethernet pppoe

Example

The following example enables CHAP on the interface and then specifies a CHAP user name and password for the PPPoE interface.

```
CES(config-if)# pppoe ppp authentication chap
CES(config-if)# pppoe ppp username george13 password
eewG32L=73
```

pppoe service-name

Use this command to specify a service name to be associated with the local PPPoE interface. You can enter any text string to describe the PPPoE connection. Use the **no** form of the command to delete the service name.

Syntax

```
pppoe service-name <text>
no pppoe service-name
```

Parameters

text	Specifies a text string that describes the connection, for example, a location, class of service, or an ISP name. You can enter a string up to 32 characters long.

Default

No service name is configured.

Command mode

Interface Configuration (Ethernet interface)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (Ethernet interface)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Service Name length is more than 32 characters long
```

Related commands

pppoe cost
pppoe idle-timeout
pppoe ip tcp adjust-mss enable
pppoe on-demand enable
show interface

Example

The following example configures a service name for PPPoE on the subinterface of ATM interface 3/1.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# pppoe service-name connecttocentraloffice
CES(config-subif)#
```

The following example deletes the PPPoE service name on Ethernet interface 1/1.

```
CES(config)# interface fastethernet 1/1
CES(config-if)# no pppoe service-name
CES(config-if)#
```

show interface pppoe

Use this command to display PPPoE configuration information.

Syntax

show interface {**fastethernet** | **gigabitethernet**}
<*slot*>/<*port*> **pppoe**

Parameters

slot	Specifies the slot where the Ethernet interface card resides.
port	Specifies the port on the interface card.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

interface fastethernet
pppoe admin-state enable

Warning messages

```
% IP protocol encapsulation is already configured on this
interface!
% Interface <slot>/<port> does not exist
```

Example

The following example shows the type of information displayed by the command.

```
CES# show interface fastethernet 2/1 pppoe

FastEthernet Interface 1/1 PPPoE Configuration
  PPPoE                                  : Enabled
  Administrative state                   : Disabled
  Cost                                   : 20
  Idle Time-out                          : 15
  Local IP Address                       : 0.0.0.0
  On-demand                              : Disabled
  PPP
    Authentication                       : none
  IPCP
    VJ Connect ID Compression Negotiation: Disabled
    VJ Max Slots                         : 8
    VJ Negotiation                       : Disabled
  ICP
    Echo Fault Threshold                 : 1
    Echo Interval                        : 0
    Protocol Field Compression           : Disabled
  User Name                              :
  Service Name                           :
CES#
```

PPPoE configuration example

The following commands configure a PPPoE interface.

```
CES# configure terminal
Enter configuration commands, one per line. End with Ctrl-z.
CES(config)# interface fastEthernet 1/1
CES(config-if)# filter "permit all"
CES(config-if)# pppoe enable
CES(config-if)# pppoe ppp ?
Configures PPP attributes for this PPPoE interface
  authentication  Enables PPP authentication for this PPPoE interface
  ipcp            Enables PPP IPCP parameters for this PPPoE interface
  lcp             Enables PPP LCP parameters for this PPPoE interface
  username        Configure PPP authentication user identification
CES(config-if)# pppoe ppp authentication chap
CES(config-if)# pppoe ppp username contivity password contivity
CES(config-if)# pppoe ppp lcp ?
  echo-fault-threshold
  echo-interval
  protocol-field-compression
CES(config-if)# pppoe ppp lcp echo-interval 10
CES(config-if)# pppoe ppp lcp echo-fault-threshold 2
CES(config-if)# pppoe ip ?
  local  Specifies the local IP address for this PPPoE interface
  tcp    pppoe tcp settings
CES(config-if)# pppoe ip local 192.168.3.2
CES(config-if)# pppoe ip tcp adjust-mss enable
CES(config-if)# pppoe admin-state enable
CES(config-if)# exit
CES(config)# exit
CES# show ip route

S    0.0.0.0/32        [0/20] via 192.168.3.2, 0 00:00:07, CircId 66 [PPPoE
DefaultRoute]
D    192.168.1.0/24    [0/0] via 192.168.1.1, 0 05:07:46, CircId 1
D    192.168.1.1/32    [0/0] via 127.0.0.1, 0 05:07:46, CircId 1
D    192.168.1.2/32    [0/0] via 127.0.0.1, 0 05:07:46, CircId 1
D    192.168.3.2/32    [0/0] via 127.0.0.1, 0 00:00:07, CircId 66 [PPPoE Static
Address]

CES#
```

Chapter 26
Dial serial port commands

This chapter describes dial commands for serial interfaces.

Command	Page
auto-answer	1254
baud-rate	1255
connect	1256
dial-prefix-string	1258
interface dial	1260
interface dial enable	1261
menu-access-level	1263
microcode	1264
microcode reload	1266
mode	1267
modem-command-string	1269
modem-initialization-string	1271
modem-termination-string	1272
phone	1274
reset	1276
serial-port baud-rate	1276
serial-port mode	1279
show interface dial	1281
show interface dial statistics	1283
show microcode	1285
shutdown	1286

auto-answer

Use this command to specify the number of rings after which an incoming call is answered. Use the **no** form of the command to disable the automatic answering of incoming calls.

Syntax

```
auto-answer {1 | 2 | 3}
no auto-answer
```

Parameters

1, **2**, or **3**	Specifies the number of rings after which the interface answers an incoming call.

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show interface dial

Example

The following example configures the dial interface to automatically answer an incoming call after two rings.

```
CES(config)# interface dial 7/1
CES(config-if)# auto-answer 2
CES(config-if)#
```

The following example disables the automatic answering of incoming calls.

```
CES(config-if)# no auto-answer
CES(config-if)#
```

baud-rate

Use this command to reset the baud rate on the motherboard serial port to match the baud rate of a terminal. The default baud rate is 9600 bits/s.

Syntax

```
baud-rate {9600 | 19200 | 38400 | 57600}
```

Parameters

None

Default

9600 bits/s

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

menu-access-level
mode
modem-initialization-string
modem-termination-string
show serial-port

Example

The following example sets the baud rate for the serial port on the motherboard to 19,200 bits/s.

```
CES(config)# interface dial 7/1
CES(config-if)# baud-rate 19200
CES(config-if)#
```

connect

Use this command to start a serial call. Use the **no** form of the command to disconnect the previously established call.

Syntax

connect <*type*> <*slot*>/<*port*>
no connect <*type*> <*slot*>/<*port*>

Parameters

type	Specifies the interface type. For a serial dial interface, the value of this parameter is **dial**.
slot	Specifies the slot where the interface card is installed. Enter a value from 0 through 7.
port	Specifies the port on the interface card. For type **dial**, you can set the port to **1** only.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

If you try to execute this command on a slot/port that does not have an ISDN BRI or V.90 interface card, the following message is displayed:

```
% Slot/Port and Type mismatch.
```

If an invalid slot/port combination is entered, the following message is displayed:

```
% Invalid Slot/Port.
```

Related commands

interface dial
interface serial
phone

Example

The following example starts a call.

```
CES# connect dial 7/1
  Call established
CES#
```

The following example disconnects a call.

```
CES# no connect dial 7/1
  Call disconnected
CES#
```

dial-prefix-string

Use this command to set the dial prefix string.

Syntax

dial-prefix-string <*string*>

Parameters

string	Specifies a dial prefix string.

Default

+++ATDT

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

baud-rate
menu-access-level
mode
modem-initialization-string
modem-termination-string
reset
show serial-port

Example

The following example configures a dial prefix string for serial port 1 on card 3.

```
CES(config)# interface serial 3/1
CES(config-if)# dial-prefix-string +++ATDT0
CES(config-if)#
```

interface dial

Use this command to navigate to a dial interface and enter Interface Configuration mode.

Syntax

interface dial <*slot*>/<*port*>

Parameters

slot	Specifies the slot where the interface card is installed. Enter a value from 0 through 7.
port	Specifies the port on the interface card. Type **1** as the port number.

Default

None

Command mode

Global Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

connect
interface dial enable
show interface dial

Example

The following example navigates to the interface on slot 1 port 1.

```
CES(config)# interface dial 7/1
CES(config-if)#
```

interface dial enable

Use this command to enable a dial interface. Use the **no** form of the command to disable a dial interface.

Syntax

interface dial <*slot*>/<*port*> **enable**
no interface dial <*slot*>/<*port*> **enable**

Parameters

slot	Specifies the slot where the interface card is installed. Enter a value from 0 through 7.
port	Specifies the port on the interface card. Type **1** as the port number.

Default

Enabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

connect
interface dial
reset
show interface dial
shutdown

Example

The following example enables the interface on slot 4 port 1.

```
CES(config)# interface dial 4/1 enable
CES(config-if)#
```

The following example disables the dial interface on slot 4 port 1.

```
CES(config)# no interface dial 4/1 enable
CES(config-if)#
```

menu-access-level

Use this command to reset the menu access level for the motherboard serial port. This setting determines which commands on the serial menu are available. By default, all commands are available. If you specify one of the restricted mode settings, the gateway can only be managed through a control tunnel by someone with administrator privileges who is allowed to configure a control tunnel.

Syntax

menu-access-level {**unrestricted** | **restricted1** | **restricted2**}

Parameters

unrestricted	Specifies that all commands on the serial menu are available. This value is the default setting.
restricted1	Specifies that only system reset commands and the commands to change interface IP address and mask are available on the serial menu.
restricted2	Specifies that only system reset commands are available on the serial menu.

Default

unrestricted

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

baud-rate
mode
modem-initialization-string
reset
show serial-port

Example

The following example sets the menu access level to “retricted1.”

```
CES(config)# interface dial 7/1
CES(config-if)# menu-access-level restricted1
CES(config-if)#
```

microcode

Use this command to specify the name of the firmware file that you will apply to the V.90 modem cards that require a firmware upgrade. After you execute this command, you use the **microcode reload** command to upgrade the firmware.

Syntax

microcode <*filename*>

Parameters

filename	Specifies the file name (file URL) for the firmware.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

microcode reload
show microcode

Example

The following example specifies a firmware file for interface 3/1 and then loads that file on to the interface.

```
CES(config)# interface serial 3/1
CES(config-if)# microcode /ide0/system/bin/sp120w.lm
CES(config-if)# exit
CES(config)# exit
CES# microcode reload serial 3/1
Reload may take several minutes per card and should be done
off-line. Reboot after all reloads are complete.
CES#
```

microcode reload

Use this command to reload firmware on one or V.90 interfaces. Before you execute this command, you first execute the **microcode** command to specify the file name of the new firmware. After all reloads are completed, reboot the gateway.



Caution: Reboot the gateway after you execute this command. Otherwise, unexpected results may occur.

Download firmware at an off-peak time; the reloading of the firmware can take several minutes for each interface card. Before you download the firmware, do the following:

- Make sure that the gateway will not be rebooted or restarted during the firmware download.
- Make sure that the V.90 interface is in an enabled state.
- Disconnect the call (use the **no connect dial** command).

Syntax

microcode reload

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

microcode
show microcode

Example

The following example upgrades the firmware for a V.90 interface on the gateway.

```
CES# microcode reload
Reload may take several minutes per card and should be done
off-line. Reboot after all reloads are complete.
CES#
```

mode

Use this command to set the mode of operation for the motherboard serial port. Select one of the following modes:

- Serial menu (default)
- PPP
- Autodetect

Note: To change the mode from serial menu to PPP or the reverse, you must restart the gateway after you execute the command.

Syntax

```
mode {serial-menu | ppp | autodetect}
```

Parameters

serial-menu	Sets the serial port to display a standard menu interface. This setting is the default mode. When the serial port is set to serial menu mode, you connect directly to the gateway using the COM port to start a serial menu terminal session. If you change the default baud rate (9600) for the serial port, you must press the Reset button.
ppp	Sets the gateway to use the Point-to-Point Protocol (PPP) over the serial port. Using serial PPP, you can manage the gateway from a remote location and access all management services (HTTP, Telnet, FTP, SNMP) through the Web interface. When a serial PPP session is established, the serial interface acts as a private WAN interface with an internal IP address (0.0.1.7). If the gateway becomes unreachable over the Internet, you can dial up and manage it through the serial interface menu.
autodetect	Sets the serial port to automatically detect whether the gateway is using PPP or serial menu mode at startup. If the serial port is set to autodetect mode, the gateway checks the serial mode each time that it is restarted. If a modem is attached when the gateway performs its autodetection check, the gateway sends out AT command set characters to configure the modem. If a terminal session is established and the terminal baud rate is the same as the gateway's, the terminal displays the AT command sets on the screen. Press Enter until a serial menu session is started.

Default

serial-menu

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

baud-rate
menu-access-level
modem-initialization-string
show serial-port

Example

```
CES(config)# interface dial 7/1
CES(config-if)# mode autodetect
CES(config-if)#
```

modem-command-string

Use this command to send an arbitrary command string to the modem (a string other than the initialization or termination string). Refer to the modem documentation for the vendor-specific character strings. This command is used to test the modem; it may take a few seconds to execute.

Syntax

modem-command-string <*string*>

Parameters

string	Specifies a vendor-specific character string for testing the modem. See the documentation for the modem.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

baud-rate
dial-prefix-string
menu-access-level
mode
modem-initialization-string
modem-termination-string
show serial-port

Example

The following example sets the modem command string for the gateway serial port.

```
CES(config)# interface serial 3/1
CES(config-if)# modem-command-string ATZ&B1AT&N10
CES(config-if)#
```

modem-initialization-string

Use this command to set the modem initialization string. Refer to the modem documentation for the vendor-specific character initialization string.



Note: Nortel recommends that you configure the modem to use the default initialization string for the gateway (ATZ).

Syntax

modem-initialization-string <*string*>

Parameters

string	Specifies the vendor-specific character initialization string for the modem. See the documentation for the modem to locate this string.

Default

ATZ

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

baud-rate
dial-prefix-string
menu-access-level
mode
modem-command-string
modem-termination-string
show serial-port

Example

The following example sets the modem initialization string for the gateway serial port. This example shows a 3Com/US Robotics 56K modem initialization string that instructs the external modem to connect at 19,200 bits/s.

```
CES(config)# interface serial 3/1
CES(config-if)# modem-initialization-string ATZ&B1AT&N10
CES(config-if)#
```

modem-termination-string

Use this command to set the modem termination string. Refer to the modem documentation for the vendor-specific character termination string.

Note: Nortel recommends that you configure the modem to use the default termination string for the gateway (ATH).

Syntax

modem-termination-string <*string*>

Parameters

string	Specifies the vendor-specific character termination string for the modem. See the documentation for the modem to locate this string.

Default

ATH

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

baud-rate
dial-prefix-string
menu-access-level
mode
modem-command-string
modem-initialization-string
show serial-port

Example

The following example sets the modem termination string for a serial port. This example shows a 3Com/US Robotics 56K modem termination string.

```
CES(config)# interface serial 3/1
CES(config-if)# modem-termination-string ATH0
CES(config-if)#
```

phone

Use this command to configure the remote telephone number that the V.90 interface calls. Use the **no** form of this command to delete the previously configured telephone number.

Syntax

phone *<number>*
no phone

Parameters

number	Specifies the telephone number of the device that the interface calls. Enter up to 255 digits. You can enter only one outgoing telephone number.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

connect
show interface dial

Example

The following example specifies the telephone number that this V.90 interface calls.

```
CES(config)# interface serial 1/1
CES(config-if)# phone 17775551111567
CES(config-if)#
```

The following example deletes the configured telephone number from this serial interface.

```
CES(config)# interface serial 1/1
CES(config-if)# no phone
CES(config-if)#
```

reset

Use this command to apply any changes that you made to the modem configuration on a serial port. For example, if you reset the baud rate on the serial port, you must execute the **reset** command to implement the new baud rate.

Syntax

reset

Parameters

None

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

baud-rate
connect
dial-prefix-string
menu-access-level
mode
show serial-port
shutdown

Example

This following example resets the baud rate for serial port 2/1 to 19,200 bits/s and then applies the change.

```
CES(config)# interface serial 2/1
CES(config-if)# baud-rate 19200
CES(config-if)# reset
CES>
```

serial-port baud-rate

Use this command to configure baud rate for the serial port.

Syntax

serial-port baud-rate <*baud-rate*>

Parameters

None

Default

9600

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

None

Prerequisites

None

Related commands

None

Example

Example of a successful help for this command:

```
CES(config)# serial-port baud-rate ?
19200                   Sets the terminal baud rate to 19200
2400                    Sets the terminal baud rate to 2400
38400                   Sets the terminal baud rate to 38400
4800                    Sets the terminal baud rate to 4800
57600                   Sets the terminal baud rate to 57600
9600                    Sets the terminal baud rate to 9600
<cr>
```

Example of a successful execution:

```
CES(config)# serial-port baud-rate 2400
CES(config)#
```

serial-port mode

Use this command to configure the mode for the serial port.

Syntax

serial-port mode <*mode*>

Parameters

None

Default

Serial-menu

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – None
User Management – Manage

Warning

None

Prerequisites

None

Related commands

None

Example

Example of a successful help for this command:

```
CES(config)# serial-port mode ?
autodetect              Enables the switch to determine
                        whether to use PPP or serial-menu
ppp                     Enables serial port management
                        using PPP
serial-menu             Enables the standard serial menu
                        interface
TCP                     Enables TCP
<cr>
```

Example of a successful execution:

```
CES(config)# serial-port mode TCP
CES(config)#
```

show interface dial

Use this command to display the configuration of dial interfaces.

Syntax

show interface dial [*<slot>/<port>*]

Parameters

slot	Specifies the slot where the dial interface is installed. Enter a value from 0 through 7.
port	Specifies the port on the system serial interface or the modem interface card. Type **1** for the port number.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

interface dial
show interface dial statistics
show microcode

Example

The following example displays information about dial interface 7/1.

```
CES# show interface dial 7/1
Interface Dial 7/1
  Menu Access Level           : UNRESTRICTED
  Auto answer                 : 1 ring
  Baud Rate                   : 9600
  Circuit ID                  : exi
  Description                 :
  Dial Prefix String          : +++ATDT
  Filter                      : deny all
  Modem Command String        :
  Modem Init String           : +++ATZ
```

```
  Modem Termination String    : +++ATH
  Phone                       : 15559999
  Mode                        : PPP
  Connection Status           : Modem Response Timeout
  Serial Interface Type       : SerialUart
  Status                      : Enabled
  Vj negotiation              : Disabled
  .
  .
  PPP description             :
CES#
```

show interface dial statistics

Use this command to display statistics for configured dial interfaces.

Syntax

show interface dial <*slot*>/<*port*> **statistics**

Parameters

slot	Specifies the slot where the dial interface is installed. Enter a value from 0 through 7.
port	Specifies the port on the system serial interface or the modem interface card. Type **1** for the port number.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

interface
show interface
show microcode

Example

The following example displays statistics for dial interface 7/1.

```
CES# show interface dial 7/1 statistics
Date 07/26/2003  Time 05:40:52
Statistics for COM port on slot 7

Administrative State:  Enabled
Call State          :  Not Connected

Bytes Out    : 0                        Bytes In      : 0
PPP Bytes Out: 0                        PPP Bytes In  : 0
Packets Out  : 0                        Packets In    : 0
Bad Packets  : 0                        Framing Errors: 0
Parity Errors: 0                        Overrun Errors: 0
Call Duration: 00:00:00 (Days Hours:Minutes:Seconds)
CES#
```

show microcode

Use this command to display the version of microcode running on V.90 interface cards.

Syntax

show microcode

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

microcode
microcode reload
show interface statistics

Example

The following example displays the names of the microcode files for all relevant cards.

```
CES# show microcode
Interface ISDN BRI 1/1
  Microcode: sfus22.bin
Interface serial 2/1
  Microcode: sfus11a.bin
CES#
```

shutdown

Use this command to disable the current interface. The **no** form of the command reenables the interface.

Syntax

shutdown
no shutdown

Parameters

None

Default

The interface is not shut down.

Command mode

Interface Configuration

Next command mode

Interface Configuration

Related commands

interface enable
reset

Example

The following example disables serial interface 3/1.

```
CES(config)# interface serial 3/1
CES(config-if)# shutdown
CES(config-if)# exit
CES(config)#
```

The following example reenables dial interface 3/1.

```
CES(config)# interface dial 3/1
CES(config-if)# no shutdown
CES(config-if)# exit
CES(config)#
```

Chapter 27
ISDN BRI configuration commands

This chapter describes ISDN BRI configuration commands.

Command	Page
connect	1290
interface bri	1292
interface bri enable	1293
interface bri isdn calls-per-tei	1295
isdn auto-answer	1296
isdn auto-spid-detection enable	1298
isdn auto-switch-detect	1299
isdn bandwidth-monitor enable	1301
isdn country-code	1303
isdn manual-tei	1305
isdn microcode	1306
isdn not-end-to-end	1308
isdn phone	1309
isdn public	1311
isdn spid1	1312
isdn spid2	1314
isdn switch-type	1316
line-power-detection enable	1318
microcode reload bri	1320
reset	1322
show interface bri	1323

Command	Page
show interface bri statistics	1326
show microcode bri	1328
shutdown	1330

connect

Use this command to start an ISDN BRI call. Use the **no** form of the command to disconnect the previously established call.

Syntax

connect *<type> <slot>/<port>*
no connect *<type> <slot>/<port>*

Parameters

type	Specifies the interface type. For an ISDN BRI interface, the value of this parameter is **bri**.
slot	Specifies the slot where the ISDN interface card is installed. Enter a value from 0 through 6.
port	Specifies the port on the ISDN interface card. For type **bri**, you can set the port to **1** only.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

If you try to execute this command on a slot/port that does not have an ISDN BRI or V.90 interface card, the following message is displayed:

```
% Slot/Port and Type mismatch.
```

If an invalid slot/port combination is entered, the following message is displayed:

```
% Invalid Slot/Port.
```

Related commands

interface bri
interface bri enable
isdn phone

Example

The following example starts an ISDN call.

```
CES# connect bri 2/1
  Call established
CES#
```

The following example disconnects an ISDN call.

```
CES# no connect bri 2/1
  Call disconnected
CES#
```

interface bri

Use this command to navigate to an ISDN BRI interface and enter Interface Configuration mode.

Syntax

interface bri <*slot*>/<*port*>

Parameters

slot	Specifies the slot where the ISDN BRI interface card is installed. Enter a value from 0 through 6.
port	Specifies the port on the ISDN BRI interface card. Type **1** as the port number.

Default

None

Command mode

Global Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

If you try to configure ISDN BRI on a non-ISDN card, the following message is displayed:

```
% BRI configuration not permitted for this card type
```

Related commands

connect
interface bri enable
show interface bri

Example

The following example navigates to the ISDN BRI interface on slot 1 port 1.

```
CES(config)# interface bri 1/1
CES(config-if)#
```

interface bri enable

Use this command to enable an ISDN BRI interface. Use the **no** form of the command to disable an ISDN BRI interface.

Syntax

interface bri <*slot*>/<*port*> **enable**
no interface bri <*slot*>/<*port*> **enable**

Parameters

slot	Specifies the slot where the ISDN BRI interface card is installed. Enter a value from 0 through 6.
port	Specifies the port on the ISDN BRI interface card. Type **1** as the port number.

Default

Enabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

connect
interface bri
reset
show interface bri
shutdown

Example

The following example enables the ISDN BRI interface on slot 4 port 1.

```
CES(config)# interface bri 4/1 enable
CES(config-if)#
```

The following example disables the ISDN BRI interface on slot 4 port 1.

```
CES(config)# no interface bri 4/1 enable
CES(config-if)#
```

interface bri isdn calls-per-tei

Use this command to enable an ISDN BRI interface with ISDN Terminal Endpoint Identifier (TEI) to permit bearer calls. Some older ISDN providers do not support two bearer calls on a single TEI; therefore, Nortel added this option to support these older providers.

Syntax

interface bri isdn calls-per-tei *1/2*

Parameters

1	1 permits only one bearer call per TEI.
2	2 permits two bearer calls on a single TEI. This is the default value.

Default

2

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

connect
interface bri
reset
show interface bri
shutdown

Example

The following example enables the ISDN BRI interface to make two bearer calls.

```
CES(config)# interface bri isdn calls-per-tei 2
CES(config-if)#
```

isdn auto-answer

Use this command to specify the number of rings after which an incoming call is answered. Use the **no** form of the command to disable the automatic answering of incoming calls.

Syntax

```
isdn auto-answer {1 | 2 | 3}
no isdn auto-answer
```

Parameters

1, **2**, or **3**	Specifies the number of rings after which the interface answers an incoming call.

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
show interface bri
```

Example

The following example configures the ISDN BRI interface to automatically answer an incoming call after two rings.

```
CES(config-if)# isdn auto-answer 2
CES(config-if)#
```

The following example disables the automatic answering of incoming calls.

```
CES(config-if)# no isdn auto-answer
CES(config-if)#
```

isdn auto-spid-detection enable

Use this command to enable automatic detection of the service profile ID (SPID) for ISDN BRI. This command applies only to NI-2 ISDN switches (North America only). Use the **no** form of the command to disable automatic detection of the SPID.

Syntax

```
isdn auto-spid-detection enable
no isdn auto-spid-detection enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

isdn auto-switch-detect
isdn spid1
isdn spid2

Example

The following example enables the automatic SPID detection feature.

```
CES(config-if)# isdn auto-spid-detection enable
CES(config-if)#
```

The following example disables the automatic SPID detection feature.

```
CES(config-if)# no isdn auto-spid-detection enable
CES(config-if)#
```

isdn auto-switch-detect

Use this command to enable and disable the automatic switch detection option for ISDN BRI. This command applies to type NI-2 ISDN switches only (North America only).

Syntax

isdn auto-switch-detect {**auto** | **disable** | **on-reset**}

Parameters

auto	Specifies that the ISDN switch type will be automatically detected.
disable	Disables automatic ISDN switch type detection.
on-reset	Specifies that the ISDN switch type will be automatically detected after the gateway is reset.

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
isdn auto-spid-detection enable
isdn spid1
isdn spid2
```

Example

The following example enables the automatic switch detection feature.

```
CES(config-if)# isdn auto-switch-detect auto
CES(config-if)#
```

The following example enables the automatic switch detection feature after the gateway is reset.

```
CES(config-if)# isdn auto-spid-detection on-reset
CES(config-if)#
```

The following example disables the automatic switch detection feature.

```
CES(config-if)# isdn auto-spid-detection disable
CES(config-if)#
```

isdn bandwidth-monitor enable

Use this command to enable bandwidth monitoring for ISDN BRI. Use the **no** form of the command to disable bandwidth monitoring.



Note: This command applies only if you enable multilink using the **ppp multilink outgoing enable** command.

Syntax

```
isdn bandwidth-monitor enable
no isdn bandwidth-monitor enable
```

Parameters

None

Default

Enabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp multilink outgoing enable
show interface bri

Example

The following example enables bandwidth monitoring for ISDN BRI.

```
CES(config-if)# isdn bandwidth-monitor enable
CES(config-if)#
```

The following example disables bandwidth monitoring for ISDN BRI.

```
CES(config-if)# no isdn bandwidth-monitor enable
CES(config-if)#
```

isdn country-code

Use this command to specify which country or continent this Nortel VPN Router will operate in. When you execute this command, the gateway automatically loads country-specific information. Each country or continent has a set of valid ISDN switch types.

Note: Not all ISDN parameters are valid for all countries.

Table 10 lists the country codes and some of the ISDN switch types for various locations.

Table 10 ISDN country codes and switch types

Location	CLI country code	Switch types
Europe	europe	ETSI
Hong Kong	hong-kong	HKT
Japan	japan	KDD
		NTT
Korea	korea	KOR
North America	north-america	Lucent 5E10
		DMS-100
		NI-2

Syntax

```
isdn country-code {europe | hong-kong | japan | korea |
north-america}
```

Parameters

europe **hong-kong** **japan** **korea** **north-america**	Specifies the country or continent in which this Nortel VPN Router will operate. When you set this parameter, you enable the automatic loading of country-specific information.

Default

North America

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

isdn switch-type
show interface bri

Example

The following example sets the country code for ISDN BRI to Japan.

```
CES(config-if)# isdn country-code japan
CES(config-if)#
```

isdn manual-tei

Use this command to specify that the terminal end-point identifier (TEI) will be entered manually. Some switches do not support automatic TEI. The TEI number is obtained from the local ISDN provider.

Syntax

isdn manual-tei <*number*>

Parameters

number	Specifies the terminal end-point identifier, an integer that is one of the following: • 0 (PBX) • 0-63 (TEI supplied by the ISDN provider) • 127 (broadcast)

Default

127

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show interface bri

Example

The following example manually sets the TEI for ISDN BRI interface 3/1 to 27.

```
CES(config)# interface bri 3/1
CES(config-if)# isdn manual-tei 27
CES(config-if)#
```

isdn microcode

Use this command to specify the name of the firmware file that you will apply to the ISDN BRI cards that require a firmware upgrade. After you execute this command, you use the **microcode reload** command to upgrade the firmware.

Syntax

isdn microcode <*filename*>

Parameters

filename	Specifies the file name (file URL) for the firmware.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

microcode reload
show microcode

Example

The following example specifies a firmware file for ISDN BRI on interface 3/1 and then loads that file on to the interface.

```
CES(config)# interface bri 3/1
CES(config-if)# isdn microcode /ide0/system/bin/sp120w.lm
CES(config-if)# exit
CES(config)# exit
CES# microcode reload bri 3/1
Reload may take several minutes per card and should be done
off-line. Reboot after all reloads are complete.
CES#
```

isdn not-end-to-end

Use this command to implement data over voice bearer services (DOVBS). An adaptation rate of 56 Kb/s is typically used to send digital data over a call line that is used for voice communication.



Note: This command does not apply to all countries and all switch types. Check with your local ISDN provider.

Syntax

```
isdn not-end-to-end {56 | 64}
```

Parameters

56	Sets the adaptation rate to 56 Kb/s.
64	Sets the adaptation rate to 64 Kb/s.

Default

64

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show interface bri

Example

The following example sets the adaptation rate on ISDN BRI interface 3/1 to 56 Kb/s:

```
CES(config)# interface bri 3/1
CES(config-if)# isdn not-end-to-end 56
CES(config-if)#
```

isdn phone

Use this command to configure the remote telephone number that the ISDN BRI interface calls. Use the **no** form of this command to delete the previously configured telephone number.

Syntax

isdn phone <*number*>
no isdn phone

Parameters

number	Specifies the telephone number of the device that the ISDN interface calls. Enter up to 127 digits. You can enter only one outgoing telephone number.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

connect
show interface bri

Example

The following example specifies the telephone number that this ISDN BRI interface calls.

```
CES(config)# interface bri 1/1
CES(config-if)# isdn phone 17775551111567
CES(config-if)#
```

The following example deletes the configured telephone number from this ISDN BRI interface.

```
CES(config)# interface bri 1/1
CES(config-if)# no isdn phone
CES(config-if)#
```

isdn public

Use this command to configure an ISDN BRI interface as a public interface. Use the **no** form of the command to configure the interface as a private interface.

Syntax

```
isdn public
no isdn public
```

Parameters

None

Default

Public

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
show interface bri
```

Example

The following example configures the ISDN BRI interface as a public interface.

```
CES(config)# interface bri 1/1
CES(config-if)# isdn public
CES(config-if)#
```

The following example configures the ISDN BRI interface as a private interface.

```
CES(config)# interface bri 1/1
CES(config-if)# no isdn public
CES(config-if)#
```

isdn spid1

Use this command to set the service profile ID (SPID) for registration of the B1 channel with the service provider's ISDN switch. You also use this command to specify the local directory number, with or without an SPID. Use the **no** form of the command to delete the SPID, thereby preventing access to the switch.

If you do not have an SPID number (used mostly in North America), enter **none** as the SPID number.

Syntax

isdn spid1 <*spid-number*> [<*ldn*>]
isdn spid1 none <*ldn*>
no isdn spid1

Parameters

spid-number	Specifies the service profile ID (SPID) that identifies the service to which you have subscribed. The ISDN provider assigns the SPID, which is usually a 10-digit telephone number with some extra digits. You can enter up to 20 digits. If you do not have an SPID (used mostly in North America), enter **none** to leave the SPID undefined.
ldn	Specifies the 13-digit local directory number as delivered by the service provider in the incoming setup message.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

isdn auto-spid-detection enable
isdn spid2
show interface bri

Example

The following example configures the SPID and the LDN for the B1 channel of ISDN BRI interface 1/1.

```
CES(config)# interface bri 1/1
CES(config-if)# isdn spid1 7816461111 7124567890
CES(config-if)#
```

The following example configures only the LDN for the B1 channel of the ISDN BRI interface when no SPID is available (for example, if the gateway is not located in North America).

```
CES(config-if)# isdn spid1 none 7124567890
CES(config-if)#
```

The following example deletes the SPID for the B1 channel (if an LDN was specified, it is also deleted).

```
CES(config-if)# no isdn spid1
CES(config-if)#
```

isdn spid2

Use this command to set the service profile ID (SPID) for registration of the B2 channel with the service provider's ISDN switch. You also use this command to specify the local directory number, with or without an SPID. Use the **no** form of the command to delete the SPID, thereby preventing access to the switch.

If you do not have an SPID number (used mostly in North America), enter **none** as the SPID number.

Syntax

isdn spid2 <*spid-number*> [<*ldn*>]
isdn spid2 none <*ldn*>
no isdn spid2

Parameters

spid-number	Specifies the service profile ID (SPID) that identifies the service to which you have subscribed. The ISDN provider assigns the SPID, which is usually a 10-digit telephone number with some extra digits. You can enter up to 20 digits. If you do not have an SPID (used mostly in North America), enter **none** to leave the SPID undefined.
ldn	Specifies the 13-digit local directory number as delivered by the service provider in the incoming setup message.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

isdn auto-spid-detection enable
isdn spid1
show interface bri

Example

The following example configures the SPID and the LDN for the B2 channel of ISDN BRI interface 1/1.

```
CES(config)# interface bri 1/1
CES(config-if)# isdn spid2 7816461111 7124567890
CES(config-if)#
```

The following example configures only the LDN for the B2 channel of the ISDN BRI interface when no SPID is available (for example, if the gateway is not located in North America).

```
CES(config-if)# isdn spid2 none 7124567890
CES(config-if)#
```

The following example deletes the SPID for the B2 channel (if an LDN was specified, it is also deleted).

```
CES(config-if)# no isdn spid2
CES(config-if)#
```

isdn switch-type

Use this command to specify the ISDN switch type at the central office.

Syntax

isdn switch-type {**basic-5ess** | **basic-dms100** | **basic-net3** | **basic-ni** | **hkt** | **kdd** | **kor** | **ntt**}

Parameters

basic-5ess	Specifies the Lucent* 5ESS* switch.
basic-dms100	Specifies the Nortel DMS-100* switch.
basic-net3	Specifies the NET3 ISDN BRI switches (Norway NET3, Australia NET3, and New Zealand NET3). Also covers the ETSI-compliant Euro-ISDN E-DSS1 signaling system.
basic-ni	Specifies the NI-2 (National ISDN) switch type (used in North America).
hkt	Specifies the Hong Kong CR13 ISDN BRI switch type.
kdd	Specifies the Japanese KDD ISDN BRI switch type.
kor	Specifies the Korean KOR ISDN BRI switch type.
ntt	Specifies the Japanese NTT ISDN BRI switch type.

Default

basic-ni

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

isdn country-code
show interface bri

Example

The following example specifies that the ISDN switch is a DMS-100.

```
CES(config)# interface bri 1/1
CES(config-if)# isdn switch-type basic-dms100
CES(config-if)#
```

line-power-detection enable

Use this command to enable phantom line power detection on an ISDN interface. The **no** form of the command disables phantom line power detection.

If line power detection is enabled and the ISDN BRI card is reset, the card will look for the presence of power on the ISDN line. (Not all networks supply power.) If power is detected, the ISDN BRI card automatically initiates certain Layer 2 negotiations.

If line power detection is disabled, the card usually requires a trigger (for example, an outgoing call request) to initiate Layer 2 negotiations. Because these negotiations take time, the first call attempt may fail.

Syntax

```
line-power-detection enable
no line-power-detection enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Related commands

reset
show interface bri

Example

The following example enables phantom line power detection.

```
CES(config)# interface bri 3/1
CES(config-if)# line-power-detection enable
CES(config-if)#
```

The following example disables phantom line power detection.

```
CES(config)# interface bri 3/1
CES(config-if)# no line-power-detection enable
CES(config-if)#
```

microcode reload bri

Use this command to reload ISDN firmware on one or all ISDN BRI interfaces. Before you execute this command, you first execute the **isdn microcode** command to specify the file name of the new firmware. After all reloads are completed, reboot the gateway.



Caution: Reboot the gateway after you execute this command. Otherwise, unexpected results may occur.

Download ISDN firmware at an off-peak time; the reloading of the firmware can take several minutes for each interface card. Before you download the ISDN firmware to an ISDN interface, do the following:

- Make sure that the gateway will not be rebooted or restarted during the firmware download.
- Make sure that the ISDN interface is in an enabled state.
- Disconnect the ISDN call (use the **no connect bri** command).

Syntax

microcode reload bri [<*slot*>/<*port*>]

Parameters

slot	Specifies the slot where the ISDN BRI interface card is installed. Enter a value from 0 through 6.
port	Specifies the port on the ISDN BRI interface card. Type **1** for the port number.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

isdn microcode
show microcode

Example

The following example upgrades the firmware for all ISDN BRI interfaces on the gateway.

```
CES# microcode reload bri
Reload may take several minutes per card and should be done
off-line. Reboot after all reloads are complete.
CES#
```

The following example specifies a firmware file for ISDN BRI interface 3/1 and then loads that file on to the interface.

```
CES(config)# interface bri 3/1
CES(config-if)# isdn microcode /ide0/system/bin/sp120w.lm
CES(config-if)# exit
CES(config)# exit
CES# no connect bri
CES# microcode reload bri 3/1
Reload may take several minutes per card and should be done
off-line. Reboot after all reloads are complete.
```

reset

Use this command to reset the ISDN BRI card.

Syntax

reset *<type> <slot>/<port>*

Parameters

type	Specifies the interface or server to be reset. For an ISDN BRI interface, the value of this parameter is **bri**.
slot	Specifies the slot where the ISDN BRI interface card is installed. Enter a value from 0 through 6.
port	Specifies the port on the ISDN BRI interface card. Type **1** for the port number.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

connect
interface bri enable
shutdown

Example

The following example resets the ISDN BRI card in slot 2.

```
CES# reset bri 2/1
Interface ISDN BRI 2/1 reset
CES#
```

show interface bri

Use this command to display the configuration of ISDN BRI interfaces. If you do not enter a slot and port, all ISDN BRI interfaces are displayed.

Syntax

show interface bri [<*slot*>/<*port*>]

Parameters

slot	Specifies the slot where the ISDN interface card is installed. Enter a value from 0 through 6.
port	Specifies the port on the ISDN interface card. Type **1** for the port number.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% ISDN BRI Interface <slot>/<port> does not exist
% Slot/Port and Type mismatch
```

Related commands

interface bri
show interface bri statistics
show microcode

Example

The following example displays information about ISDN BRI interface 3/1.

```
CES# show interface bri 3/1
ISDN Configuration:
ISDN Interface Type: Public
ISDN Status: Enabled
Connection Status: Not Connected
Auto-answer: Disabled
Auto-spid-detection: Disabled
Auto-switch-detect: Disabled
Bandwidth-monitor: Disabled
Country-code: NorthAmerica
Not-end-to-end: 64
```

```
Manual TEI: 127
Microcode Location:
Phone: 97845678901230
SPID1: 1234567890 1234567890
SPID2:
Switch-type: NI2
Incoming: Disabled
Outgoing: Disabled
High-threshold-percent: 80
High-threshold-duration: 5
Low-threshold-percent: 20
Low-threshold-duration: 60
Low-minimum-duration: 180
Minimum-links: 1
MRRU: 1500

Interface Configuration:
Description:
Circuit ID:
Interface Filter: deny all
Dial Out Multilink: Disable
Dial Out Phone Number: 9785551111890

PPP Interface Configuration:
Description:
Local IP Address: Accepted Negotiated Address
Remote IP Address: Accepted Negotiated Address
Remote PAP Negotiation: FALSE
Remote UID: Not Configured
Remote password: Not Configured
Local PAP Negotiation: FALSE
Local CHAP Negotiation: FALSE
Local UID: Not Configured
Local Password: Not Configured
Primary DNS Status: FALSE
Secondary DNS Status: FALSE
Address Control Field Compression : TRUE
Protocol Field Compression: TRUE
Echo Fault Threshold: 1
Echo Interval: 0
VJ Negotiation: TRUE
VJ Connect ID Compression Negotiation: TRUE
VJ Max Slots: 8
Interface Debug: Enabled
```

show interface bri statistics

Use this command to display statistics for configured ISDN BRI interfaces.

Syntax

show interface bri <*slot*>/<*port*> **statistics**

Parameters

slot	Specifies the slot where the ISDN interface card is installed. Enter a value from 0 through 6.
port	Specifies the port on the ISDN interface card. Type **1** for the port number.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

interface bri
show interface bri
show microcode

Example

The following example displays statistics for ISDN BRI interface 3/1.

```
CES# show interface bri 3/1 statistics
ISDN BRI Interface 3/1 Statistics
  Date: 03/12/2003     Time: 17:55:43
  Administrative State: Enabled
  Call State          : Not Connected
  Bytes Sent   : 39               Bytes Received: 0
  PPP Bytes Out: 17               PPP Bytes In  : 0
  Packets Out  : 2                Packets In    : 0
  Bad Packets  : 0                Framing Errors: 0
  Parity Errors: 0                Overrun Errors: 0
  Call Duration: 00:00:03 (Hours:Minutes:Seconds)
ISDN BRI Card Firmware Version: ISM SINGLE S0/T0/U0, SP120W-2.29 ,
December 2002
  Parameter settings on the BRI Card:
   Gci_Mod: 77      Tei_ass: 16      Tei_rem: 32      Co    : 1
   Iver   : 20      Cmode  : 2       Sp_ism : 0       Synclk : 0
   Subscr : 7       FaConf : 60      FaTrf  : 61      FaDrop : 62
    FaMw   : 63       Power  : 0         56k    : 0
    Nb     : ""                        Sa     : ""
   Spid1  : ""                       NbSpid1: ""
   Spid2  : ""                       NbSpid2: ""
   Spid3  : ""                      Ch     : 7       Tei_sig: 127
   Tei    : 1       NbAsyn : ""      SaAsyn : "1"     IpAsyn : 10
   NbPPP  : ""      SaPPP  : ""      IpPPP  : 0       NbV120 : ""
   SaV120 : "10"    IpV120 : 8       FsV120 : 256     WsV120 : 3
   NbPadB : ""      SaPadB : "11"    IpPadB : 12      NbRTel : ""
   SaRTel : "16"    IpRTel : 40      NbRData: ""      SaRData: "18"
   IpRData: 40      NbMPPP : ""      SaMPPP : ""      IpMPPP : 28
   MRRU   : 1500    Lnkmin : 1       En_EDO : 1       En_Bod : 1
   MpHPer : 80      MpHDur : 5000    MpLPer : 20      MpLDur : 60000
   MpMDur : 180000   NbRc   : ""     SaRc   : "99"    AdX25Rc: "99"
    IpRc   : 255       RemNbRc: ""
```

```
   PassRc : “”                        AdX251 : “”       ProfD  : “ID”
   Ps     : 1024      Pws    : 3       Lcn    : 1        Fws    : 3
   T1     : 400       PsB    : 128     PwsB   : 2        LcnB   : 1
CES#
```

show microcode bri

Use this command to display the version of microcode running on ISDN BRI interface cards.

Syntax

show microcode bri [<*slot*>/<*port*>]

Parameters

slot	Specifies the slot where the ISDN interface card is installed. Enter a value from 0 through 6.
port	Specifies the port on the ISDN interface card. Type **1** as the port number.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

isdn microcode
microcode reload
show interface bri statistics

Example

The following example displays the names of the microcode files for all relevant cards.

```
CES# show microcode bri
Interface ISDN BRI 1/1
  Microcode: sfus22.bin
Interface serial 2/1
  Microcode: sfus11a.bin
CES#
```

The following example displays the name of the microcode file for the ISDN BRI card in slot 1 only.

```
CES# show microcode bri 1/1
Interface ISDN BRI 1/0
  Microcode: sfus22.bin
CES#
```

shutdown

Use this command to disable the current interface. The **no** form of the command reenables the interface.

Syntax

```
shutdown
no shutdown
```

Parameters

None

Default

The interface is not shut down.

Command mode

Interface Configuration

Next command mode

Interface Configuration

Related commands

```
interface bri enable
reset
```

Example

The following example disables ISDN BRI interface 3/1.

```
CES(config)# interface bri 3/1
CES(config-if)# shutdown
CES(config-if)# exit
CES(config)#
```

The following example reenables ISDN BRI interface 3/1.

```
CES(config)# interface bri 3/1
CES(config-if)# no shutdown
CES(config-if)# exit
CES(config)#
```

Chapter 28
ADSL and ATM configuration commands

This chapter describes ADSL and ATM interface configuration commands.

Command	Page
circuit-id	1334
controller atm	1335
debug atm	1337
description (interface)	1339
description (subinterface)	1340
dsl operating-mode	1342
encapsulation	1344
filter	1346
interface atm	1348
ip local	1349
ip local address-type	1352
ip remote	1353
ip remote address-type	1355
mac-crc-included	1357
public	1359
show dsl interface atm	1360
show interface atm	1362
show interface atm statistics	1364
shutdown (interface)	1367
shutdown (subinterface)	1368

Command	Page
subinterface	1370
virtual-circuit	1371

circuit-id

Use this command to specify a text description for the transmission vendor's circuit identifier (this ID is useful for troubleshooting). Use the **no** form of the command to delete this text.

Syntax

```
circuit-id <text>
no circuit-id
```

Parameters

text	Specifies an alphanumeric description of the ATM circuit. You can enter up to 31 characters. If the text includes spaces, enclose it in quotation marks.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% circuit-id longer than 31 characters
```

Related commands

description
filter
interface atm
show interface atm
shutdown

Example

The following example creates a circuit description for ATM interface 2/1.

```
CES(config)# interface atm 2/1
CES(config-if)# circuit-id “9786708760-1”
CES(config-if)#
```

controller atm

Use this command to enter Controller Configuration mode. (Use the **exit** command to leave Controller Configuration mode and return to Global Configuration mode.)

Syntax

controller atm *<slot>/<port>*

Parameters

slot	Specifies the slot where the ADSL interface card is installed.
port	Specifies the port on the ADSL interface card (type **1**).

Default

None

Command mode

Global Configuration

Next command mode

Controller Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Slot/Port and Type mismatch
% Invalid Slot/Port
```

Related commands

dsl operating-mode
show dsl interface atm

Example

The following example enters ATM Controller Configuration mode and then exits from it.

```
CES(config)# controller atm 1/1
CES(config-controller)# exit
CES(config)#
```

debug atm

Use this command to start debug-level logging for ATM interfaces and subinterfaces. Use the **no** form of the command to stop the logging of debug messages.

Syntax

debug atm [<*slot*>/<*port*>[.<*subinterface*>]]
no debug atm [<*slot*>/<*port*>[.<*subinterface*>]]

Parameters

slot	Specifies the slot where the ADSL interface card is installed.
port	Specifies the port on the ADSL interface card (type **1**).
subinterface	Specifies the subinterface number of the ATM interface (type **1**).

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

show interface atm statistics

Example

The following example starts debug logging for all ATM interfaces and then stops debug logging.

```
CES# debug atm
CES# no debug atm
CES#
```

The following example starts debug logging for ATM interface 1/1 and then stops debug logging.

```
CES# debug atm 1/1
CES# no debug atm 1/1
CES#
```

The following example starts debug logging for subinterface 1 on ATM interface 1/1 and then stops debug logging.

```
CES# debug atm 1/1.1
CES# no debug atm 1/1.1
CES#
```

description (interface)

Use this command to specify a text description for the ATM interface. Use the **no** form of the command to delete this text.

The interface description appears in the result of the ifName MIB.

Syntax

description <*text*>
no description

Parameters

text	Specifies an alphanumeric description of the ATM physical interface. You can enter up to 23 characters. If the text includes spaces, enclose it in quotation marks.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% description longer than 23 characters
```

Related commands

circuit-id
filter
interface atm
show interface atm
shutdown

Example

The following example specifies a description for ATM interface 2/1.

```
CES(config)# interface atm 2/1
CES(config-if)# description “ADSL link to ISP”
CES(config-if)#
```

description (subinterface)

Use this command to specify a text description for an ATM subinterface (virtual circuit). Use the **no** form of the command to delete this text.

The interface description appears in the result of the ifName MIB.

Syntax

description <*text*>
no description

Parameters

text	Specifies an alphanumeric description of the ATM virtual circuit. You can enter up to 23 characters. If the text includes spaces, enclose it in quotation marks.

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% description longer than 23 characters
```

Related commands

encapsulation
ip local
public
show interface atm
subinterface
virtual-circuit

Example

The following example specifies a description for the subinterface of ATM interface 2/1.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# description “ATM VC on ADSL link”
CES(config-subif)#
```

dsl operating-mode

Use this command to modify the operating mode of the ADSL physical interface. Make sure that the new operating mode is compatible with the ADSL interface card installed in the gateway.

Syntax

dsl operating-mode {**ansi-dmt** | **itu-dmt annex** {**a** | **b**} | **splitterless**}

Parameters

ansi-dmt	Specifies that the ANSI DMT version of ADSL is used on this interface. ANSI DMT—also called full-rate ADSL—is used with POTS and is specified in ANSI T1.413.
itu-dmt annex a **itu-dmt annex b**	Specifies that the ITU DMT version of ADSL is used on this interface. ITU-T DMT is specified in ITU G992.1. Annex A is ADSL over POTS; Annex B is ADSL over ISDN.
splitterless	Specifies that the G.Lite version of ADSL is used on this interface. G.Lite is specified in ITU G992.2. Based on ANSI T1.413, G.Lite is designed to work without the use of a splitter.

Default

Splitterless

Command mode

Controller Configuration

Next command mode

Controller Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

controller atm
show dsl interface atm

Example

The following example sets the line coding to ANSI DMT.

```
CES# config terminal
CES(config)# controller atm 1/1
CES(config-controller)# dsl operating-mode ansi-dmt
CES(config-controller)#
```

The following example sets the line coding to G.Lite.

```
CES# config terminal
CES(config)# controller atm 1/1
CES(config-controller)# dsl operating-mode splitterless
CES(config-controller)#
```

The following example sets the line coding to G.DMT (Annex B).

```
CES# config terminal
CES(config)# controller atm 1/1
CES(config-controller)# dsl operating-mode itu-dmt annex b
CES(config-controller)#
```

encapsulation

Use this command to set the encapsulation of the current subinterface. The MUX option is a null encapsulation and allows only one protocol to run over the virtual circuit; the SNAP option allows multiple protocols to run over a virtual circuit. Use the **no** form of the command to remove the encapsulation type from the subinterface.

Syntax

encapsulation {**aal5mux** | **aal5snap** | **mpoamux** | **mpoasnap** | **pppoemux** | **pppoesnap**}

no encapsulation

Parameters

aal5mux	Specifies that PPP over ATM multiplexed will be used on this subinterface.
aal5snap	Specifies that PPP over ATM with LLC/SNAP will be used on this subinterface.
mpoamux	Specifies that multiprotocol over ATM routed (MPoA(R)) multiplexed will be used on this subinterface.
mpoasnap	Specifies that MPoA(R) with LLC/SNAP will be used on this subinterface.
pppoemux	Specifies that PPP over Ethernet (PPPoE) multiplexed will be used on this subinterface.
pppoesnap	Specifies that PPP over Ethernet (PPPoE) with LLC/SNAP will be used on this subinterface.

Default

MPoA(R)

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

description
ip local
mac-crc-included
public
show interface atm
subinterface
virtual-circuit

Example

The following example configures PPPoE with LLC/SNAP encapsulation on subinterface 1.

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# encapsulation pppoesnap
CES(config-subif)#
```

The following example removes encapsulation from the subinterface on ATM 1/1.

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# no encapsulation
CES(config-subif)#
```

filter

Use this command to specify an interface filter for the ATM interface. Use the **no** form of the command to reset the interface filter to its default value (deny all).

Syntax

filter *<name>*
no filter

Parameters

name	Specifies the interface filter to apply. Enter one of the following strings: deny-all, permit-all, permit-dns-tcp, permit-dns-udp, permit-entrust-ca, permit-finger, permit-ftp, permit-http, permit-ldap, permit-nntp, permit-ntp, permit-ping, or permit-telnet. You can also enter the name of a user-created filter.

Default

Deny all

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

circuit-id
description
interface atm
show interface atm
shutdown

Example

The following example sets the interface filter for ATM interface 2/1 to permit-ftp.

```
CES(config)# interface atm 2/1
CES(config-if)# filter permit-ftp
CES(config-if)#
```

interface atm

Use this command to navigate to an ATM interface to add or edit ATM interface parameters.

Syntax

interface atm <*slot*>/<*port*>

Parameters

slot	Specifies the slot where the ADSL interface card is installed.
port	Specifies the port on the ADSL interface card (type **1**).

Default

None

Command mode

Global Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

An appropriate interface card must be installed in the specified slot.

Warning messages

```
% Slot/Port and Type mismatch
% Invalid Slot/Port
```

Related commands

circuit-id
description
filter
show interface atm
shutdown
subinterface

Example

The following example enters Interface Configuration mode for the ATM interface card in slot 2.

```
CES(config)# interface atm 2/1
CES(config-if)# exit
CES(config)#
```

ip local

Use this command to configure a static IP address and mask for the local ATM subinterface. Use the **no** form of the command to delete the IP address.

Syntax

```
ip local <address> [<mask>]
no ip local
```

Parameters

address	Specifies in dotted-decimal notation the IP address associated with the local ATM subinterface.
mask	Specifies in dotted-decimal notation the subnet mask for the IP address configured on the local ATM subinterface.

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip local address-type
ip remote
ip remote address-type
show interface atm subinterface

Example

The following example configures a static IP address and mask for subinterface 1 on ATM interface 2/1.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# ip local 10.10.10.1 255.255.255.0
CES(config-subif)#
```

The following example deletes the IP address from ATM subinterface 1.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# no ip local
CES(config-subif)#
```

ip local address-type

Use this command to specify whether the IP address for the local ATM subinterface will be obtained dynamically or will be statically configured.

Syntax

```
ip local address-type {dynamic | static}
```

Parameters

dynamic	Specifies that the IP address for this ATM subinterface will be obtained dynamically.
static	Specifies that the IP address for this ATM subinterface will be statically configured using the **ip local** command.

Default

Static

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip local
ip remote
ip remote address-type
show interface atm
subinterface

Example

The following example specifies that the IP address for the local ATM subinterface will be dynamically obtained.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# ip local address-type dynamic
CES(config-subif)#
```

The following example specifies that the IP address for the local ATM subinterface will be statically configured and then specifies the address and subnet mask for the subinterface.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# ip local address-type static
CES(config-subif)# ip local 10.10.10.1 255.255.255.0
CES(config-subif)#
```

ip remote

Use this command to configure a static IP address for the remote side of the ATM subinterface. Use the **no** form of the command to delete the IP address.

Syntax

ip remote *<address>*
no ip remote

Parameters

address	Specifies in dotted-decimal notation the IP address associated with the remote ATM subinterface.

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip local
ip local address-type
ip remote address-type
show interface atm subinterface

Example

The following example configures a static IP address for the remote side of the local ATM subinterface.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# ip remote 10.10.10.2
CES(config-subif)#
```

The following example deletes the remote IP address from virtual circuit 1.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# no ip remote
CES(config-subif)#
```

ip remote address-type

Use this command to specify whether the IP address for the remote ATM subinterface will be obtained dynamically or will be statically configured.

Syntax

ip remote address-type {**dynamic** | **static**}

Parameters

dynamic	Specifies that the IP address for the remote ATM subinterface will be obtained dynamically.
static	Specifies that the IP address for the remote ATM subinterface will be statically configured using the **ip remote** command.

Default

Static

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ip local
ip local address-type
ip remote
show interface atm
subinterface

Example

The following example specifies that the IP address for the remote ATM subinterface will be dynamically obtained.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# ip remote address-type dynamic
CES(config-subif)#
```

The following example specifies that the IP address for the remote ATM subinterface will be statically configured and then specifies the address for the subinterface.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# ip remote address-type static
CES(config-subif)# ip remote 10.10.10.2
CES(config-subif)#
```

mac-crc-included

Use this command to enable the inclusion of the Ethernet MAC CRC in PPPoE-encapsulated frames to be transmitted. Use the **no** form of the command to disable the inclusion of the MAC CRC.

Syntax

```
mac-crc-included enable
no mac-crc-included enable
```

Parameters

None

Default

Enabled

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

description
encapsulation
public
show interface atm
subinterface

Example

The following example specifies that the MAC CRC not be included in PPPoE-encapsulated frames.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# no mac-crc-included enable
CES(config-subif)#
```

The following example specifies that the MAC CRC will be included in PPPoE-encapsulated frames.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# mac-crc-included enable
CES(config-subif)#
```

public

On the Nortel VPN Router device, a subinterface is defined as public (untrusted) or private (trusted). Use this command to configure a subinterface as a public subinterface. Use the **no** form of the command to reset the value to the default (private).

Syntax

```
public
no public
```

Parameters

None

Default

Private

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

description
encapsulation
show interface atm
subinterface

Example

The following example configures subinterface 1 of ATM interface 1/1 as public.

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# public
CES(config-subif)#
```

The following example configures subinterface 1 of ATM interface 1/1 as private.

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# no public
CES(config-subif)#
```

show dsl interface atm

Use this command to display DSL attributes.

Syntax

show dsl interface atm [<*slot*>/<*port*>]

Parameters

slot	Specifies the slot where the ADSL interface card is installed.
port	Specifies the port on the ADSL interface card (type **1**).

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Slot/Port and Type mismatch
% Invalid Slot/Port
```

Related commands

controller atm
dsl operating-mode
show interface atm
show interface atm statistics

Example

The following example displays DSL information about the card in slot 2 port 1.

```
CES# show dsl interface atm 2/1
Interface: slot 2 port 1
  ADI 6483 chipset information
  DSL Mode: ITU G.992.2 (G.LITE)
CES#
```

show interface atm

Use this command to display configuration information about an ATM interface or subinterface.

Syntax

show interface atm [<*slot*>/<*port*>[.<*subinterface*>]]

Parameters

slot	Specifies the slot where the ADSL interface card is installed.
port	Specifies the port on the ADSL interface card (type **1**).
subinterface	Specifies the subinterface number of the ATM interface (type **1**).

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

interface atm
show dsl interface atm
show interface atm statistics

Example

The following example displays information about ATM interface 1/1.

```
CES# show interface atm 1/1
CES ATM interface 1/1
  circuit-id: 9786708760-1
  debug: no
  description:
  filter: permit all
  mtu: 1500
  shutdown: no
  subinterface: 1
  tcp-mss enable: no
  tcp-mss: 1460
CES#
```

The following example displays information about the subinterface on ATM interface 2/1.

```
CES# show interface atm 2/1.1
CES ATM virtual circuit 2/1.1
  debug:
  description: Corporate HQ backup 1
  encapsulation: mpoamux
  public: no
  shutdown: no
  virtual-circuit: 0/70
  ip local address-type: static
  ip local address: 2.2.2.2 255.255.255.255
  ip remote address-type: dynamic
CES#
```

show interface atm statistics

Use this command to display statistical information for an ATM interface or subinterface.

Syntax

show interface atm [<*slot*>/<*port*>[.<*subinterface*>]] **statistics**

Parameters

slot	Specifies the slot where the ADSL interface card is installed.
port	Specifies the port on the ADSL interface card (type **1**).
subinterface	Specifies the subinterface number on the ATM interface (type **1**).

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

Services Management - Manage
User Management - None

Related commands

debug atm
interface atm
show dsl interface atm
show interface atm

Example

The following example displays statistics for ATM interface 2/1.

```
CES# show interface atm 2/1 statistics
ATM Slot 2  Interface 1
PHY: Up
Administrative State: Enabled
ADSL Line Protocol: Glite

Interface Packet Statistics
===========================
InPackets = 69045            OutPackets = 60039
InGood = 69045               OutGood = 60039
InOctets = 5102736           OutOctets = 4285440
InErrors = 0                 OutErrors = 0
InNoBuffErrs = 0             OutNoBuffErrs = 0
InOverrunErrs = 0            OutOverrunErrs = 0
InAal5CrcErrs = 0

Link Level Cell Statistics
==========================
InCells = 0                  OutCells = 0
InAtmHecErrs = 0

Hardware Information
====================
I/O Option: ADSL_Glite_Gdmt_ANSI
Microcode type:    Annex A
Microcode version: 0
Outgoing Rate: 352 kbps
Incoming Rate: 2048 kbps
CES#
```

The following example displays statistics for a subinterface.

```
CES# show interface atm 2/1.1 statistics
Interface 2/1 subinterface 1 Statistics
  VPI/VCI: 3/2
    State : Enabled
    Status: Up
    Total Packets In: 0             Total Packets Out: 0
    Total Octets In : 0             Total Octets Out : 0
    IP Software-level Packet Data:
      IP Packets Received  : 0      IP Packets Sent  : 0
      IP Octets Received   : 0      IP Octets Sent   : 0
      IP Octets Dropped    : 0
      IP Packets Accepted  : 0
      IP Packets Forwarded : 0
      IP Fragments Received: 0
      IP Packets Fragmented: 0
      IP Packet Fragments  : 0

IP Packet Drops:
  IP Routing Filter Drops        : 0
  IP Local System Filter Drops   : 0
  IP Local Interface Filter Drops: 0
  IP PAT Drops                   : 0
  IP Header Error Drops          : 0
  IP QoS Random Drops            : 0
  IP QoS Forced Drops            : 0
  IP Zero Source Address Drops   : 0
  IP Source Address Equals
      Destination Address Drops  : 0
  IP Bad Packet Length Drops     : 0
  IP Bad Header Length Drops     : 0
  IP Bad Checksum Drops          : 0
  IP Packet Too Short Drops      : 0
  IP Bad Options Drops           : 0
  IP No Buffer To Fragment Drops : 0
  IP Cannot Fragment Drops       : 0
  IP Cannot Forward Drops        : 0
  IP No Protocol Drops           : 0
  IP No Route Drops              : 0
  IP Bad Version Drops           : 0
  TOTAL: 0

CES#
```

shutdown (interface)

Use this command to disable the current interface. Use the **no** form of the command to reenable the interface.

Syntax

```
shutdown
no shutdown
```

Parameters

None

Default

The interface is not shut down.

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

Services Management - Manage
User Management - None

Related commands

```
exit
interface atm
show interface atm
```

Example

The following example disables ATM interface 1/1.

```
CES(config)# interface atm 1/1
CES(config-if)# shutdown
CES(config-if)# exit
CES(config)#
```

The following example reenables ATM interface 1/1.

```
CES(config)# interface atm 1/1
CES(config-if)# no shutdown
CES(config-if)# exit
CES(config)#
```

shutdown (subinterface)

Use this command to disable the current ATM subinterface. Use the **no** form of the command to reenable the subinterface.

Syntax

```
shutdown
no shutdown
```

Parameters

None

Default

The subinterface is not shut down.

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

Services Management - Manage
User Management - None

Related commands

exit
show interface atm
subinterface

Example

The following example disables subinterface 1 on ATM interface 1/1.

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# shutdown
CES(config-subif)# exit
CES(config-if)#
```

The following example reenables subinterface 1 on ATM interface 1/1.

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# no shutdown
CES(config-subif)# exit
CES(config-if)#
```

subinterface

Use this command to create an ATM subinterface and to navigate to Subinterface Configuration mode. Use the **no** form of the command to delete an ATM subinterface.

Syntax

```
subinterface <subinterface>
no subinterface <subinterface>
```

Parameters

subinterface	Specifies the subinterface number on the ATM interface (type **1**).

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration (when deleting a subinterface)
Subinterface Configuration (when creating or navigating to a subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

description
encapsulation
public
show interface atm
shutdown
virtual-circuit

Example

The following example navigates to subinterface 1 on port 1 of the card in slot 2. If the subinterface does not exist, it will be created.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)#
```

The following example deletes subinterface 1 on port 1 of the ADSL card in slot 2.

```
CES(config)# interface atm 2/1
CES(config-if)# no subinterface 1
CES(config-if)#
```

virtual-circuit

Use this command to specify a virtual circuit (VC) number for the current subinterface. Use the **no** form of the command to reset the VC number to the default value (0/32).

Syntax

virtual-circuit *<vpi>/<vci>*
no virtual-circuit

Parameters

vpi	Specifies the ATM virtual path identifier (VPI). Type an integer from 0 through 255.
vci	Specifies the ATM virtual circuit identifier (VCI). Type an integer from 0 through 65355.

Default

0/32

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

description
encapsulation
show interface atm
subinterface

Example

The following example sets the VC number for the subinterface on the ADSL interface card in slot 1 as follows: VPI=5, VCI=100.

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# virtual-circuit 5/100
CES(config-subif)#
```

The following example resets the VPI and VCI to their default values (0/32).

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# no virtual-circuit
CES(config-subif)#
```

Chapter 29
PPP configuration commands

This chapter describes Point-to-Point Protocol (PPP) configuration commands.

Command	Page
circuit-id	1377
description	1378
encapsulation	1380
filter	1381
interface	1383
ppp authentication chap	1384
ppp authentication pap	1386
ppp ip default-route	1388
ppp ip local (ATM subinterfaces)	1390
ppp ip local (dial interfaces)	1392
ppp ip local (serial interfaces)	1394
ppp ip ospf	1396
ppp ip primary-dns-obtain enable	1398
ppp ip remote (ATM subinterfaces)	1399
ppp ip remote (dial interfaces)	1401
ppp ip remote (serial interfaces)	1403
ppp ip rip	1405
ppp ip secondary-dns-obtain enable	1407
ppp ipcp vj-connect-id-compression-negotiation	1408
ppp ipcp vj-max-slots	1410
ppp ipcp vj-negotiation	1412

Command	Page
ppp lcp address-control-field-compression	1413
ppp lcp echo-fault-threshold	1415
ppp lcp echo-interval	1417
ppp lcp protocol-field-compression	1418
ppp lcp-ncp interface-debug	1420
ppp local authentication chap	1422
ppp local authentication pap	1424
ppp local password	1426
ppp local username	1428
ppp multilink high-threshold-duration	1430
ppp multilink high-threshold-percent	1431
ppp multilink incoming enable	1433
ppp multilink low-minimum-duration	1435
ppp multilink low-threshold-duration	1437
ppp multilink low-threshold-percent	1439
ppp multilink minimum-links	1440
ppp multilink outgoing enable	1442
ppp password	1444
ppp public	1446
ppp remote authentication pap	1447
ppp remote password	1449
ppp remote username	1451
ppp username	1453
show interface serial	1455
show interface serial	1455
show interface serial statistics	1458

circuit-id

Use this command to enter an alphanumeric description of the circuit, for example, a site name, location, or contact name.

Syntax

circuit-id <*value*>

Parameters

value	Specifies an alphanumeric description of the circuit. You can enter up to 31 characters. If you enter a string with spaces, enclose the string in quotation marks.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

description
encapsulation
filter
interface
show interface bri
show interface dial
show interface serial

Example

The following example configures a circuit description on serial interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# circuit-id “ST-1 555-2222”
CES(config-if)#
```

description

Use this command to provide a textual description of the PPP interface. The interface description appears in the result of the ifName MIB.

Syntax

description <*text*>

Parameters

text	Specifies an alphanumeric description of the interface. You can enter up to 24 characters. If you enter a string with spaces, enclose the string in quotation marks.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

circuit-id
encapsulation
filter
interface
show interface bri
show interface dial
show interface serial

Example

The following example configures a text description for serial interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# description “This is our main serial
interface.”
CES(config-if)#
```

encapsulation

Use this command to enable a synchronous encapsulation protocol on a serial interface: either PPP (the default) or frame relay.

Syntax

encapsulation {**frame-relay** | **ppp**}

Parameters

ppp	Specifies that PPP will be used on this interface.
frame-relay	Specifies that frame relay will be used on this interface.

Default

PPP

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

circuit-id
description
filter
interface
show interface serial ppp

Example

The following example configures PPP encapsulation on serial interface 3/1.

```
CES(config)# interface serial 3/1
CES(config-if)# encapsulation ppp
CES(config-if)#
```

filter

Use this command to select one of the interface filters for this PPP interface.

Syntax

filter [<*value*>]

Parameters

value	Specifies the interface filter to apply. Enter one of the following strings: deny-all, permit-all, permit-dns-tcp, permit-dns-udp, permit-entrust-ca, permit-finger, permit-ftp, permit-http, permit-ldap, permit-nntp, permit-ntp, permit-ping, or permit-telnet. You can also enter the name of a user-created filter.

Default

deny-all

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

circuit-id
description
encapsulation
show interface bri
show interface dial
show interface serial

Example

The following example configures the filter “permit-ftp” on serial interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# filter permit-ftp
CES(config-if)#
```

interface

Use this command to navigate to an interface on which you can configure PPP.

Syntax

interface <*type*> <*slot/port*>

Parameters

type	Specifies the interface type (for PPP, enter **bri**, **dial**, or **serial**).
slot	Specifies the slot of the interface.
port	Specifies the port of the interface.

Default

None

Command mode

Global Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

An appropriate interface card must be installed in the specified slot.

Warning messages

```
% Interface <slot/port> does not exist
```

Related commands

circuit-id
description
encapsulation
filter
show interface bri
show interface dial
show interface serial

Example

The following example configures a serial WAN interface on port 1 of the card in slot 2.

```
CES# configure terminal
CES(config)# interface serial 2/1
CES(config-if)#
```

ppp authentication chap

Use this command to enable the Challenge Handshake Authentication Protocol (CHAP) for PPP sessions on a serial interface or on an ATM subinterface. Use the **no** form of the command to disable CHAP. After you enable CHAP, use the **ppp username** and the **ppp password** commands to set the CHAP user ID and password.

Note: This command is available on serial interfaces and ATM subinterfaces only.

Syntax

```
ppp authentication chap
no ppp authentication chap
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration (serial interface)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (serial interface)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

```
ppp authentication pap
ppp password
ppp username
show interface
```

Example

The following example enables CHAP authentication for PPP sessions on serial interface 2/1 and then sets the CHAP user ID and password.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp authentication chap
CES(config-if)# ppp username george13
CES(config-if)# ppp password eewG32L=73
CES(config-if)#
```

The following example disables CHAP authentication on the serial interface.

```
CES(config)# interface serial 2/1
CES(config-if)# no ppp authentication chap
CES(config-if)#
```

The following example enables CHAP authentication for PPP sessions on the subinterface on ATM interface 3/1.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# ppp authentication chap
CES(config-subif)#
```

ppp authentication pap

Use this command to enable the Password Authentication Protocol (PAP) for PPP sessions on a serial interface or on an ATM subinterface. Use the **no** form of the command to disable PAP. After you enable PAP, use the **ppp username** and the **ppp password** commands to set the PAP user ID and password.



Note: This command is available on serial interfaces and ATM subinterfaces only.

Syntax

```
ppp authentication pap
no ppp authentication pap
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration (serial interface)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (serial interface)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

```
ppp authentication chap
ppp password
ppp username
show interface
```

Example

The following example enables PAP authentication for PPP sessions on serial interface 2/1 and then sets the PAP user ID and password.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp authentication pap
CES(config-if)# ppp username george13
CES(config-if)# ppp password eewG32L=73
CES(config-if)#
```

The following example disables PAP authentication on the serial interface.

```
CES(config)# interface serial 2/1
CES(config-if)# no ppp authentication pap
CES(config-if)#
```

The following example enables PAP authentication for PPP sessions on the subinterface on ATM interface 3/1.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# ppp authentication pap
CES(config-subif)#
```

ppp ip default-route

Use this command to configure the default route to use the dynamically learned IP address for the subinterface and to update that address when it changes. Use this command only if the protocol configured on the subinterface is PPPoA or PPPoE.

Syntax

ppp ip default-route {**disabled** | **enabled**}

Parameters

None

Default

Enabled

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% this subinterface is not configured for PPP
```

Related commands

ppp ip local
ppp ip remote
show interface atm

Example

The following example configures the subinterface to accept a negotiated IP address for the remote PPP peer and enables the default route to use the dynamically learned IP address for the subinterface.

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# encapsulation pppoesnap
CES(config-subif)# ppp ip remote negotiated
CES(config-subif)# ppp ip default-route enabled
CES(config-subif)#
```

The following example configures the default route not to use the dynamically learned IP address for the subinterface.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# ppp ip default-route disabled
CES(config-subif)#
```

ppp ip local (ATM subinterfaces)

Use this command to configure a static IP address for the local PPP interface on the ATM subinterface, or to specify that the IP address be negotiated with the remote PPP peer. Use the **no** form of the command to delete the IP address for the local PPP interface on this ATM subinterface.

Syntax

ppp ip local {<*ip-address*> [**mask** <*subnet-mask*>] | **negotiated**}
no ppp ip local

Parameters

ip-address	Specifies in dotted-decimal notation the IP address of the local PPP interface.
subnet-mask	Specifies in dotted-decimal notation the subnet mask for the IP address of the local PPP interface.
negotiated	Specifies that the IP address for the local subinterface will be negotiated with the remote PPP peer.

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% this subinterface is not configured for PPP
```

Related commands

ppp ip remote
show interface

Example

The following example configures a static IP address and subnet mask on the subinterface on ATM interface 3/1.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# ppp ip local 10.10.10.1 mask 255.255.0.0
CES(config-subif)#
```

The following example configures the subinterface on ATM interface 1/1 to negotiate its IP address with the remote PPP peer.

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# ppp ip local negotiated
CES(config-subif)#
```

The following example deletes the configured IP address from the subinterface on ATM interface 2/1.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# no ppp ip local
CES(config-subif)#
```

ppp ip local (dial interfaces)

Use this command to configure a static IP address for the local PPP interface on a dial interface. The local IP address is the Nortel VPN Router address as seen from a public network. The ISP typically provides this IP address to you. You must configure a local IP address for IP traffic to pass over this PPP interface. Use the **no** form of the command to delete the IP address for the local PPP interface.

Syntax

ppp ip local {<*address*> [**mask** <*subnet_mask*>] | **negotiated**}
no ppp ip local

Parameters

address	Specifies in dotted-decimal notation the IP address of the local PPP interface.
subnet_mask	Specifies in dotted-decimal notation the subnet mask for the IP address of the local PPP interface.
negotiated	Specifies that the IP address for the local interface will be negotiated with the remote PPP peer.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp ip remote
show interface bri
show interface dial

Example

The following example configures a static IP address and subnet mask on ISDN BRI interface 4/1.

```
CES(config)# interface bri 4/1
CES(config-if)# ppp ip local 202.100.20.1 mask 255.255.0.0
CES(config-if)#
```

The following example configures ISDN BRI interface 1/1 to negotiate its IP address with the remote peer.

```
CES(config)# interface bri 1/1
CES(config-if)# ppp ip local negotiated
CES(config-if)#
```

The following example deletes the configured IP address from dial interface 7/1.

```
CES(config)# interface dial 7/1
CES(config-if)# no ppp ip local
CES(config-if)#
```

ppp ip local (serial interfaces)

Use this command to specify a static IP address for the local serial PPP interface. This IP address is the Nortel VPN Router IP address as seen from a public network. The ISP typically provides this IP address to you. You must configure a local IP address for IP traffic to pass over this PPP interface. Use the **no** form of the command to delete the local IP address.

Syntax

ppp ip local <*address*> [<*subnet_mask*>]
no ppp ip local

Parameters

address	Specifies in dotted-decimal notation the IP address of the local PPP interface.
subnet_mask	Specifies in dotted-decimal notation the subnet mask for the IP address of the local PPP interface.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp ip ospf
ppp ip remote
ppp ip rip
ppp public
show interface serial ppp

Example

The following example configures and enables PPP on serial interface 2/1 and assigns a static IP address and subnet mask to the interface.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# filter permit-all
CES(config-if)# ppp ip local 202.100.20.1 255.255.0.0
CES(config-if)#
```

ppp ip ospf

Use this command to enable and configure OSPF on the serial interface. Use the **no** form of the command to disable OSPF on this serial interface.

Note: You can configure OSPF on a serial interface with the same commands that you use to configure it on an Ethernet interface. For information about OSPF commands, see Chapter 23, “IP interface configuration commands,” on page 1159.

Syntax

```
ppp ip ospf
no ppp ip ospf
```

Parameters

None

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp ip local
ppp ip remote
ppp ip rip
ppp public
show interface serial ppp

Example

The following example configures OSPF on a local IP address for this PPP interface.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp ip local 202.100.20.1 255.255.0.0
CES(config-if)# ppp ip remote 202.100.20.2
CES(config-if)# ppp ip ospf
CES(config-if)#
```

ppp ip primary-dns-obtain enable

Use this command to enable the IP interface to obtain primary DNS server information from the remote PPP peer. When you execute this command, the IP interface, acting as a DNS proxy, forwards DNS name-resolution requests that it receives to a DNS server. Use the **no** form of the command to disable the function.

Note: This command is available on dial interfaces only.

Syntax

```
ppp ip primary-dns-obtain enable
no ppp ip primary-dns-obtain enable
```

Parameters

None

Default

Enabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp ip secondary-dns-obtain enable
show interface bri
show interface dial

Example

The following example enables dial interface 3/1 to forward DNS name-resolution requests to the remote PPP peer.

```
CES(config)# interface dial 3/1
CES(config-if)# ppp ip primary-dns-obtain enable
CES(config-if)#
```

The following example stops ISDN BRI interface 3/1 from forwarding DNS name-resolution requests to the remote PPP peer.

```
CES(config)# interface bri 3/1
CES(config-if)# no ppp ip primary-dns-obtain enable
CES(config-if)#
```

ppp ip remote (ATM subinterfaces)

Use this command to specify a remote IP address for the PPP peer of this ATM subinterface. You can allow this subinterface to accept a negotiated IP address, or you can specify a static IP address for the remote PPP peer. Use the **no** form of the command to delete the remote IP address.

Syntax

ppp ip remote {*<ip-address>* | **negotiated**}
no ppp ip remote

Parameters

ip-address	Specifies in dotted-decimal notation the statically assigned IP address for the remote PPP peer.
negotiated	Specifies that this subinterface will accept a negotiated IP address for its remote peer.

Default

Negotiated

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% this subinterface is not configured for PPP
```

Related commands

ppp ip default-route
ppp ip local
show interface

Example

The following example configures a static IP address for the remote PPP peer of the local subinterface on ATM interface 1/1.

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# ppp ip remote 10.10.10.2
CES(config-subif)#
```

The following example configures the subinterface on ATM interface 1/1 to accept a negotiated IP address for the remote PPP peer.

```
CES(config)# interface atm 1/1
CES(config-if)# subinterface 1
CES(config-subif)# ppp ip remote negotiated
CES(config-subif)#
```

The following example deletes the IP address for the remote PPP peer of the subinterface on ATM interface 2/1.

```
CES(config)# interface atm 2/1
CES(config-if)# subinterface 1
CES(config-subif)# no ppp ip remote
CES(config-subif)#
```

ppp ip remote (dial interfaces)

Use this command to specify a remote IP address for the PPP peer of this interface. You can allow this interface to accept a negotiated IP address, or you can specify a static IP address for the remote interface. Use the **no** form of the command to delete the remote IP address.

Syntax

ppp ip remote {**negotiated** | *<ip-address>*}
no ppp ip remote [**negotiated**]

Parameters

negotiated	Specifies that this interface will accept a negotiated IP address for its remote peer.
ip-address	Specifies the statically assigned IP address for the remote PPP peer.

Default

Negotiated

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp ip local
show interface bri
show interface dial

Example

The following example configures a static IP address for the remote peer of local ISDN interface 2/1.

```
CES(config)# interface bri 2/1
CES(config-if)# ppp ip remote 202.100.20.2
CES(config-if)#
```

The following example configures the local dial interface to accept a negotiated IP address for the remote peer.

```
CES(config)# interface dial 4/1
CES(config-if)# ppp ip remote negotiated
CES(config-if)#
```

The following example deletes the IP address for the remote peer of ISDN interface 4/1.

```
CES(config)# interface bri 4/1
CES(config-if)# no ppp ip remote
CES(config-if)#
```

ppp ip remote (serial interfaces)

Use this command to specify a remote IP address for the PPP peer of this interface. You can allow this interface to accept a negotiated IP address, or you can specify a static IP address for the remote interface. Use the **no** form of the command to delete the remote IP address.

Syntax

ppp ip remote {**negotiated** | <*ip-address*>}
no ppp ip remote [**negotiated**]

Parameters

negotiated	Specifies that this interface will accept a negotiated IP address for its remote peer.
ip-address	Specifies the statically assigned IP address for the remote PPP peer.

Default

Negotiated

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp ip local
ppp ip ospf
ppp ip rip
ppp public
show interface serial ppp

Example

The following example configures a local IP address for interface 2/1 and a remote IP address for the remote peer.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp ip local 202.100.20.1
CES(config-if)# ppp ip remote 202.100.20.2
CES(config-if)#
```

The following example configures the local PPP interface to accept a negotiated IP address for the remote peer.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp ip remote negotiated
CES(config-if)#
```

ppp ip rip

Use this command to enable RIP on the serial interface. Use the **no** form of the command to disable RIP.



Note: You can configure RIP on a serial interface with the same commands that you use to configure it on an Ethernet interface. For information about RIP commands, see Chapter 23, “IP interface configuration commands,” on page 1159.

Syntax

```
ppp ip rip
no ppp ip rip
```

Parameters

None

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp ip local
ppp ip ospf
ppp ip remote
ppp public
show interface serial ppp

Example

The following example configures RIP on the local IP address for this PPP interface.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp ip local 202.100.20.1
CES(config-if)# ppp ip remote 202.100.20.2
CES(config-if)# ppp ip rip
CES(config-if)#
```

ppp ip secondary-dns-obtain enable

Use this command to enable the IP interface to obtain secondary DNS server information from the remote PPP peer. When you execute this command, the IP interface, acting as a DNS proxy, forwards DNS name-resolution requests that it receives to a DNS server. Use the **no** form of the command to disable the function.

Note: This command is available on dial interfaces only.

Syntax

```
ppp ip secondary-dns-obtain enable
no ppp ip secondary-dns-obtain enable
```

Parameters

None

Default

Enabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp ip primary-dns-obtain enable
show interface bri
show interface dial

Example

The following example enables ISDN BRI interface 3/1 to forward DNS name-resolution requests to the remote PPP peer.

```
CES(config)# interface bri 3/1
CES(config-if)# ppp ip secondary-dns-obtain enable
CES(config-if)#
```

The following example stops dial interface 5/1 from forwarding DNS name-resolution requests to the remote PPP peer.

```
CES(config)# interface dial 5/1
CES(config-if)# no ppp ip secondary-dns-obtain enable
CES(config-if)#
```

ppp ipcp vj-connect-id-compression-negotiation

Use this command to enable or disable Van Jacobson (VJ) connection ID compression negotiation. In conjunction with VJ compression negotiation, VJ connection ID compression negotiation further reduces the TCP/IP packet header to increase packet transmission performance.

Syntax

ppp ipcp vj-connect-id-compression-negotiation {**disable** | **enable**}

Parameters

None

Default

Disabled

Command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

encapsulation
ppp ipcp vj-max-slots
ppp ipcp vj-negotiation
show interface

Example

The following example enables Van Jacobson compression negotiation and VJ connection ID compression negotiation on the PPP interface.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp ipcp vj-negotiation enable
CES(config-if)# ppp ipcp vj-connect-id-compression-
negotiation enable
CES(config-if)#
```

The following example enables Van Jacobson compression negotiation and VJ connection ID compression negotiation on the ATM subinterface.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# encapsulation pppoesnap
CES(config-subif)# ppp ipcp vj-negotiation enabled
CES(config-subif)# ppp ipcp vj-connect-id-compression-
negotiation enabled
CES(config-subif)#
```

The following example disables Van Jacobson connection ID compression negotiation on the dial interface.

```
CES(config)# interface dial 7/1
CES(config-if)# ppp ipcp vj-connect-id-compression-
negotiation disable
CES(config-if)#
```

ppp ipcp vj-max-slots

Use this command to specify the maximum number of concurrent Van Jacobson (VJ) compressed TCP/IP flows.

Syntax

ppp ipcp vj-max-slots <*value*>

Parameters

value	Specifies the maximum number of concurrent VJ-compressed TCP/IP flows. Enter an integer from 2–16.

Default

8

Command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

encapsulation
ppp ipcp vj-connect-id-compression-negotiation
ppp ipcp vj-negotiation
show interface

Example

The following example sets the maximum number of VJ-compressed flows to 4.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp ipcp vj-max-slots 4
CES(config-if)#
```

The following example sets the maximum number of VJ-compressed flows to 5.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# ppp ipcp vj-max-slots 5
CES(config-subif)#
```

ppp ipcp vj-negotiation

Use this command to enable or disable Van Jacobson (VJ) compression negotiation. VJ compression negotiation compresses the TCP/IP header fields on a per TCP/IP flow basis to reduce packet overhead.

Syntax

```
ppp ipcp vj-negotiation {disable | enable}
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

encapsulation
ppp ipcp vj-connect-id-compression-negotiation
ppp ipcp vj-max-slots
show interface

Example

The following example enables Van Jacobson compression negotiation on the subinterface on ATM interface 3/1.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# ppp ipcp vj-negotiation enabled
CES(config-subif)#
```

The following example enables Van Jacobson compression negotiation on the PPP interface.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp ipcp vj-negotiation enable
CES(config-if)#
```

The following example disables VJ compression negotiation on the PPP interface.

```
CES(config-if)# ppp ipcp vj-negotiation disable
CES(config-if)#
```

ppp lcp address-control-field-compression

Use this command to enable or disable LCP address control field compression. This option compresses the address control field in the packet header and reduces packet overhead by 1 byte.

Syntax

ppp lcp address-control-field-compression {**disable** | **enable**}

Parameters

None

Default

Disabled

Command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

ppp lcp echo-fault-threshold
ppp lcp echo-interval
ppp lcp protocol-field-compression
show interface

Example

The following example configures LCP address control field compression on PPP interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp lcp address-control-field-compression
enable
CES(config-if)#
```

The following example disables LCP address control field compression from the subinterface on ATM interface 3/1.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# encapsulation aal5snap
CES(config-subif)# ppp lcp address-control-field-compression
disable
CES(config-subif)#
```

ppp lcp echo-fault-threshold

Use this command to specify a value for the Link Control Protocol (LCP) echo fault threshold. The echo fault threshold is the number of consecutive unanswered echo requests that LCP sends before it disconnects the link.

Syntax

ppp lcp echo-fault-threshold <*value*>

Parameters

value	Specifies the number of consecutive unanswered echo requests the interface sends before it disconnects the link. Enter an integer from 0–255. The value 0 disables the threshold.

Default

2

Command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

ppp lcp address-control-field-compression
ppp lcp echo-interval
ppp lcp protocol-field-compression
show interface

Example

The following example sets the number of unanswered echo requests to 1.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp lcp echo-fault-threshold 1
CES(config-if)#
```

The following example sets the number of unanswered echo requests to 3.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# encapsulation pppoesnap
CES(config-subif)# ppp lcp echo-fault-threshold 3
CES(config-subif)#
```

ppp lcp echo-interval

Use this command to specify the number of seconds between echo requests. You can use this interval with the echo request threshold to determine whether the link has been disconnected.

Syntax

ppp lcp echo-interval <*seconds*>

Parameters

seconds	Specifies the number of seconds between LCP echo requests. Enter an integer from 0–255.

Default

10

Command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

ppp lcp address-control-field-compression
ppp lcp echo-fault-threshold
ppp lcp protocol-field-compression
show interface

Example

The following example sets the LCP echo interval to 2 seconds.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp lcp echo-interval 2
CES(config-if)#
```

The following example sets the LCP echo interval to 12 seconds.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# encapsulation aal5snap
CES(config-subif)# ppp lcp echo-interval 12
CES(config-subif)#
```

ppp lcp protocol-field-compression

Use this command to enable or disable LCP protocol field compression. This option compresses the protocol field in the packet header and reduces packet overhead by 1 byte.

Syntax

ppp lcp protocol-field-compression {**disable** | **enable**}

Parameters

None

Default

Disabled

Command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (serial and dial interfaces)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

ppp lcp address-control-field-compression
ppp lcp echo-fault-threshold
ppp lcp echo-interval
show interface

Example

The following example enables LCP protocol field compression on the subinterface of ATM interface 3/1.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# encapsulation aal5snap
CES(config-subif)# ppp lcp protocol-field-compression enable
CES(config-subif)#
```

The following example disables LCP protocol field compression on serial PPP interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp lcp protocol-field-compression disable
CES(config-if)#
```

ppp lcp-ncp interface-debug

Use this command to enable or disable interface debug mode. In interface debug mode, PPP control packets are sent to the event log.

Note: LCP-NCP interface debug mode is an internal customer support utility used to troubleshoot WAN interface problems. You should enable this utility only when directed by customer support personnel.

Syntax

```
ppp lcp-ncp interface-debug {enable | disable}
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp lcp address-control-field-compression
ppp lcp echo-fault-threshold
ppp lcp echo-interval
ppp lcp protocol-field-compression
show interface bri
show interface dial
show interface serial ppp

Example

The following example configures LCP-NCP debugging on serial interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp lcp-ncp interface-debug enable
CES(config-if)#
```

ppp local authentication chap

Use this command to enable the Challenge Handshake Authentication Protocol (CHAP) for PPP sessions on the local dial interface. After you enable CHAP, use the **ppp local username** and the **ppp local password** commands to set the CHAP user name and password. Use the **no** form of the command to disable CHAP.

Note: This command is available on dial interfaces only.

Syntax

```
ppp local authentication chap
no ppp local authentication chap
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

If you have not yet configured the CHAP user name and password, you see this warning message:

```
% Username and/or password not configured.
```

Related commands

ppp local authentication pap
ppp local password
ppp local username
show interface bri
show interface dial

Example

The following example enables CHAP for PPP sessions on ISDN interface 2/1 and then sets the CHAP user name and password.

```
CES(config)# interface bri 2/1
CES(config-if)# ppp local authentication chap
CES(config-if)# ppp local username george13
CES(config-if)# ppp local password eewG32L=73
CES(config-if)#
```

The following example removes CHAP from the interface.

```
CES(config)# interface bri 2/1
CES(config-if)# no ppp local authentication chap
CES(config-if)#
```

ppp local authentication pap

Use this command to enable the Password Authentication Protocol (PAP) for PPP sessions on the local dial interface. After you enable PAP, use the **ppp local username** and the **ppp local password** commands to set the PAP user name and password. Use the **no** form of the command to disable PAP.



Note: This command is available on dial interfaces only.

Syntax

```
ppp local authentication pap
no ppp local authentication pap
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

If you have not yet configured the PAP user name and password, you see this warning message:

```
% Username and/or password not configured.
```

Related commands

ppp local authentication chap
ppp local password
ppp local username
ppp remote authentication pap
show interface bri
show interface dial

Example

The following example enables PAP for PPP sessions on ISDN BRI interface 2/1 and then sets the PAP user name and password.

```
CES(config)# interface bri 2/1
CES(config-if)# ppp local authentication pap
CES(config-if)# ppp local username george13
CES(config-if)# ppp local password eewG32L=73
CES(config-if)#
```

The following example disables PAP on the interface.

```
CES(config)# interface bri 2/1
CES(config-if)# no ppp local authentication pap
CES(config-if)#
```

ppp local password

Use this command to configure a password for the local CHAP or PAP user name for PPP authentication. You must first execute the **ppp local username** command to configure the CHAP or PAP user name. Use the **no** form of the command to delete the password.

Note: This command is available on dial interfaces only.

Syntax

ppp local password <*password*>
no ppp local password

Parameters

password	Specifies the CHAP or PAP password for the local dial interface. Enter up to 127 characters.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp local authentication chap
ppp local authentication pap
ppp local username
show interface bri
show interface dial

Example

The following example enables CHAP for PPP sessions on dial interface 2/1 and then specifies a CHAP user name and password.

```
CES(config)# interface dial 2/1
CES(config-if)# ppp local authentication chap
CES(config-if)# ppp local username george13
CES(config-if)# ppp local password eewG32L=73
CES(config-if)#
```

The following example deletes the CHAP or PAP password from ISDN interface 3/1.

```
CES(config)# interface bri 3/1
CES(config-if)# no ppp local password
CES(config-if)#
```

ppp local username

Use this command to configure the CHAP or PAP user name for PPP authentication; then use the **ppp local password** command to configure a password for the CHAP or PAP user name. Use the **no** form of the command to delete the user name.

Note: This command is available on dial interfaces only.

Syntax

ppp local username <*username*>
no ppp local username

Parameters

username	Specifies the CHAP or PAP user name for the local dial interface. Enter up to 127 characters.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp local authentication chap
ppp local authentication pap
ppp local password
show interface bri
show interface dial

Example

The following example enables PAP for PPP sessions on ISDN interface 2/1 and then specifies a PAP user name and password.

```
CES(config)# interface bri 2/1
CES(config-if)# ppp local authentication pap
CES(config-if)# ppp local username george13
CES(config-if)# ppp local password eewG32L=73
CES(config-if)#
```

The following example deletes the CHAP or PAP user name from dial interface 3/1.

```
CES(config)# interface dial 3/1
CES(config-if)# no ppp local username
CES(config-if)#
```

ppp multilink high-threshold-duration

Use this command to set the number of seconds that bandwidth utilization of the first B-channel must exceed a configured percentage to trigger the addition of the second B-channel to the multilink bundle. (You set the percentage with the **ppp multilink high-threshold-percent** command.) Use the **no** form of the command to reset the duration to its default value, 5 seconds.



Note: This command is available on ISDN interfaces only.

Syntax

ppp multilink high-threshold-duration <*seconds*>
no ppp multilink high-threshold-duration

Parameters

seconds	Specifies the time in seconds that bandwidth utilization must exceed the high-threshold percentage to trigger the addition of the second B-channel to the circuit. Enter an integer from 5 through 60.

Default

5

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
isdn bandwidth-monitor enable
ppp multilink high-threshold-percent
ppp multilink outgoing enable
show interface bri
```

Example

The following example sets the high-threshold duration to 10 seconds:

```
CES(config)# interface bri 3/1
CES(config-if)# ppp multilink high-threshold-duration 10
CES(config-if)#
```

The following example resets the high-threshold duration to its default value (5 seconds).

```
CES(config)# interface bri 3/1
CES(config-if)# no ppp multilink high-threshold-duration
CES(config-if)#
```

ppp multilink high-threshold-percent

Use this command to set the percentage of bandwidth utilization of the first B-channel that must be exceeded for a configured duration to trigger the addition of the second B-channel to the multilink bundle. (You set the duration with the **ppp multilink high-threshold-duration** command.) Use the **no** form of the command to reset this value to its default value, 80 percent.



Note: This command is available on ISDN interfaces only.

Syntax

```
ppp multilink high-threshold-percent <percentage>
no ppp multilink high-threshold-percent
```

Parameters

percentage	Specifies the percentage of the first B-channel that must be continuously used for a configured number of seconds to trigger the addition of the second B-channel to the circuit. Enter an integer from 70 through 100.

Default

80

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
isdn bandwidth-monitor enable
ppp multilink high-threshold-duration
ppp multilink outgoing enable
show interface bri
```

Example

The following example sets the bandwidth utilization threshold that triggers the addition of the second B-channel on ISDN interface 3/1 to 90 percent.

```
CES(config)# interface bri 3/1
CES(config-if)# ppp multilink high-threshold-percent 90
CES(config-if)#
```

The following example resets the bandwidth utilization threshold for this ISDN interface to its default value, 80 percent.

```
CES(config)# interface bri 3/1
CES(config-if)# no ppp multilink high-threshold-percent
CES(config-if)#
```

ppp multilink incoming enable

Use this command to enable multilink for incoming calls. When you execute this command, incoming calls will be negotiated for multilink, if the peer is capable of multilink. Use the **no** form of the command to disable multilink for incoming calls.



Note: This command is available on ISDN interfaces only.

Syntax

```
ppp multilink incoming enable
no ppp multilink incoming enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp multilink outgoing enable
show interface bri

Example

The following example enables PPP multilink for incoming calls.

```
CES(config)# interface bri 3/1
CES(config-if)# ppp multilink incoming enable
CES(config-if)#
```

The following example disables PPP multilink for incoming calls.

```
CES(config-if)# no ppp multilink incoming enable
CES(config-if)#
```

ppp multilink low-minimum-duration

Use this command to configure the minimum number of seconds that the second B-channel must stay active before it can be dropped due to low-threshold criteria. This interval prevents the too-rapid tearing down of the second B-channel. Use the **no** form of the command to reset this interval to its default value, 180 seconds.



Note: This command is available on ISDN interfaces only.

Syntax

```
ppp multilink low-minimum-duration <seconds>
no ppp multilink low-minimum-duration
```

Parameters

seconds	Specifies the time in seconds that the gateway keeps the second B-channel active before it drops it due to low-threshold criteria. Enter an integer from 60 through 180.

Default

180

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
isdn bandwidth-monitor enable
ppp multilink low-threshold-duration
ppp multilink low-threshold-percent
ppp multilink outgoing enable
show interface bri
```

Example

The following example sets the minimum duration of the second B-channel to 90 seconds.

```
CES(config)# interface bri 3/1
CES(config-if)# ppp multilink low-minimum-duration 90
CES(config-if)#
```

The following example resets the minimum duration of the second B-channel to its default value, 180 seconds.

```
CES(config-if)# no ppp multilink low-minimum-duration
CES(config-if)#
```

ppp multilink low-threshold-duration

Use this command to set the number of seconds that bandwidth utilization of the second B-channel must stay below a configured percentage to trigger the removal of the second B-channel from the multilink bundle. (You set the percentage with the **ppp multilink low-threshold-percent** command.) Use the **no** form of the command to reset the duration to its default value, 60 seconds.



Note: This command is available on ISDN interfaces only.

Syntax

ppp multilink low-threshold-duration <*seconds*>
no ppp multilink low-threshold-duration

Parameters

seconds	Specifies the number of seconds that bandwidth utilization must stay below the low-threshold percentage to trigger the removal of the second B-channel from the circuit. Enter an integer from 30 through 90.

Default

60

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
isdn bandwidth-monitor enable
ppp multilink low-minimum-duration
ppp multilink low-threshold-percent
ppp multilink outgoing enable
show interface bri
```

Example

The following example sets the low-threshold duration to 40 seconds.

```
CES(config)# interface bri 4/1
CES(config-if)# ppp multilink low-threshold-duration 40
CES(config-if)#
```

The following example resets the low-threshold duration to its default value (60 seconds).

```
CES(config)# interface bri 3/1
CES(config-if)# no ppp multilink low-threshold-duration
CES(config-if)#
```

ppp multilink low-threshold-percent

Use this command to set the low-threshold percentage for bandwidth utilization of the second B-channel. If the B-channel uses less than this percentage of bandwidth for the number of seconds configured with the **ppp multilink low-threshold-duration** command, the second B-channel is removed from the multilink bundle. Use the **no** form of the command to reset the percentage to its default value, 20 percent.



Note: This command is available on ISDN interfaces only.

Syntax

```
ppp multilink low-threshold-percent <percentage>
no ppp multilink low-threshold-percent
```

Parameters

percentage	Specifies the low-threshold percentage for the second B-channel. If bandwidth utilization of the second B-channel falls below this percentage for a configured number of seconds, the link is dropped from the circuit. Enter an integer from 10 through 30.

Default

20

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
isdn bandwidth-monitor enable
ppp multilink low-minimum-duration
ppp multilink low-threshold-duration
ppp multilink outgoing enable
show interface bri
```

Example

The following example sets the low threshold for bandwidth utilization of the second B-channel to 10 percent.

```
CES(config)# interface bri 3/1
CES(config-if)# ppp multilink low-threshold-percent 10
CES(config-if)#
```

The following example resets the low threshold to the default value, 20 percent.

```
CES(config-if)# no ppp multilink low-threshold-percent
CES(config-if)#
```

ppp multilink minimum-links

Use this command to configure the minimum number of links to include in the multilink circuit, either 1 (the default) or 2. Use the **no** form of the command to reset the number to its default value, 1.



Note: This command is available on ISDN interfaces only.

Syntax

```
ppp multilink minimum-links {1 | 2}
no ppp multilink minimum-links
```

Parameters

1 or **2**	Specifies whether one or two B-channels will be included in the circuit.

Default

1

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
isdn bandwidth-monitor enable
ppp multilink outgoing enable
show interface bri
```

Example

The following example sets the minimum number of links to 2.

```
CES(config)# interface bri 3/1
CES(config-if)# ppp multilink minimum-links 2
CES(config-if)#
```

The following example resets the minimum number of links to its default value, 1.

```
CES(config)# interface bri 3/1
CES(config-if)# no ppp multilink minimum-links
CES(config-if)#
```

ppp multilink outgoing enable

Use this command to enable multilink for outgoing calls. When you execute this command, outgoing calls will be bundled as two B-channels into one 128 Kb/s pipe to provide higher bandwidth as needed. Use the **no** form of the command to disable multilink for outgoing calls.

Note: This command is available on ISDN interfaces only.

Syntax

```
ppp multilink outgoing enable
no ppp multilink outgoing enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

isdn bandwidth-monitor enable
ppp multilink incoming enable
ppp multilink minimum-links
show interface bri

Example

The following example enables multilink on outgoing calls.

```
CES(config)# interface bri 3/1
CES(config-if)# ppp multilink outgoing enable
CES(config-if)#
```

The following example disables multilink on outgoing calls.

```
CES(config-if)# no ppp multilink outgoing enable
CES(config-if)#
```

ppp password

Use this command to configure a password for the CHAP or PAP user ID for PPP authentication. You must first execute the **ppp username** command to configure the CHAP or PAP user ID.

Note: This command is available on serial interfaces and ATM subinterfaces only.

Syntax

ppp password <*password*>

Parameters

password	Specifies the CHAP or PAP user password. Enter up to 127 characters.

Default

None

Command mode

Interface Configuration (serial interface)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (serial interface)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

ppp authentication chap
ppp authentication pap
ppp username
show interface

Example

The following example enables CHAP on the serial PPP interface and then specifies a CHAP user name and password.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp authentication chap
CES(config-if)# ppp username george13
CES(config-if)# ppp password eewG32L=73
CES(config-if)#
```

The following example enables CHAP on the subinterface of ATM interface 3/1 and then specifies a CHAP user name and password.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# ppp authentication chap
CES(config-subif)# ppp username george13
CES(config-subif)# ppp password eewG32L=73
CES(config-subif)#
```

ppp public

Use this command to configure this PPP interface as a public interface. Use the **no** form of the command to reset the value to the default (private).



Note: This command is available on serial interfaces only.

Syntax

```
ppp public
no ppp public
```

Parameters

None

Default

Private

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
ppp ip local
ppp ip ospf
ppp ip remote
ppp ip rip
show interface serial ppp
```

Example

The following example configures PPP interface 2/1 as public.

```
CES(config)# interface serial 2/1
CES(config-if)# ppp public
CES(config-if)#
```

The following example configures PPP interface 2/1 as private.

```
CES(config)# interface serial 2/1
CES(config-if)# no ppp public
CES(config-if)#
```

ppp remote authentication pap

Use this command to enable the Password Authentication Protocol (PAP) for PPP sessions on the remote dial interface. After you enable PAP, use the **ppp remote username** and the **ppp remote password** commands to set the PAP user name and password. Use the **no** form of the command to disable PAP.

Note: This command is available on dial interfaces only.

Syntax

```
ppp remote authentication pap
no ppp remote authentication pap
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

If you have not yet configured the PAP user name and password, you see this warning message:

```
% Username and/or password not configured.
```

Related commands

ppp local authentication pap
ppp remote password
ppp remote username
show interface bri
show interface dial

Example

The following example enables PAP for PPP sessions on the remote end of ISDN BRI interface 2/1 and then sets the remote PAP user name and password.

```
CES(config)# interface bri 2/1
CES(config-if)# ppp remote authentication pap
CES(config-if)# ppp remote username george13
CES(config-if)# ppp remote password eewG32L=73
CES(config-if)#
```

The following example disables PAP on the remote interface.

```
CES(config)# interface bri 2/1
CES(config-if)# no ppp remote authentication pap
CES(config-if)#
```

ppp remote password

Use this command to configure a password for the remote PAP user name for PPP authentication. You must first execute the **ppp remote username** command to configure the remote PAP user name. Use the **no** form of the command to delete the PAP password.



Note: This command is available on dial interfaces only.

Syntax

ppp remote password *<password>*
no ppp remote password

Parameters

password	Specifies the remote PAP password. Enter up to 127 characters.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp remote authentication pap
ppp remote username
show interface bri
show interface dial

Example

The following example enables PAP for PPP sessions on the remote end of ISDN BRI interface 2/1 and then sets the remote PAP user name and password.

```
CES(config)# interface bri 2/1
CES(config-if)# ppp remote authentication pap
CES(config-if)# ppp remote username george13
CES(config-if)# ppp remote password eewG32L=73
CES(config-if)#
```

The following example deletes the remote PAP password.

```
CES(config)# interface bri 2/1
CES(config-if)# no ppp remote password
CES(config-if)#
```

ppp remote username

Use this command to configure the remote PAP user name for PPP authentication; then use the **ppp remote password** command to configure a password for the remote user name. Use the **no** form of the command to delete the user name.

Note: This command is available on dial interfaces only.

Syntax

ppp remote username <*username*>
no ppp remote username

Parameters

username	Specifies the PAP user name for this interface. Enter up to 127 characters.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ppp remote authentication pap
ppp remote password
show interface bri
show interface dial

Example

The following example enables PAP for PPP sessions on the remote end of ISDN BRI interface 2/1 and then sets the remote PAP user name and password.

```
CES(config)# interface bri 2/1
CES(config-if)# ppp remote authentication pap
CES(config-if)# ppp remote username george13
CES(config-if)# ppp remote password eewG32L=73
CES(config-if)#
```

The following example deletes the PAP user name.

```
CES(config)# interface bri 2/1
CES(config-if)# no ppp remote username
CES(config-if)#
```

ppp username

Use this command to configure the CHAP or PAP user ID for PPP authentication; then use the **ppp password** command to configure a password for the CHAP or PAP user ID.



Note: This command is available on serial interfaces and ATM subinterfaces only.

Syntax

ppp username <*username*>

Parameters

username	Specifies the CHAP or PAP user ID for this interface. Enter up to 127 characters.

Default

None

Command mode

Interface Configuration (serial interface)
Subinterface Configuration (ATM subinterface)

Next command mode

Interface Configuration (serial interface)
Subinterface Configuration (ATM subinterface)

Required privileges

System Management - Manage
User Management - None

Related commands

ppp authentication chap
ppp authentication pap
ppp password
show interface

Example

The following example enables PAP on the serial PPP interface and then specifies a PAP user name and password.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation ppp
CES(config-if)# ppp authentication pap
CES(config-if)# ppp username george13
CES(config-if)# ppp password eewG32L=73
CES(config-if)#
```

The following example enables CHAP on the subinterface of ATM interface 3/1 and then specifies a CHAP user name and password.

```
CES(config)# interface atm 3/1
CES(config-if)# subinterface 1
CES(config-subif)# ppp authentication chap
CES(config-subif)# ppp username george13
CES(config-subif)# ppp password eewG32L=73
CES(config-subif)#
```

show interface serial

Use this command to display serial interface configuration information.

Syntax

show interface serial <*slot*>/<*port*>

Parameters

slot	Specifies the slot of the serial interface.
port	Specifies the port of the serial interface.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

% Interface <*slot*>/<*port*> does not exist

Related commands

show interface bri
show interface dial
show interface serial statistics

Example

The following example shows the type of information displayed by the command.

```
CES# show int serial 3/1
  Interface: serial Slot 3 Port 1
    State: Enabled
    Circuit ID:
    Description:
    Data-Rate: 64
    Filter: deny all
    Invert Data: no
    Protocol Encapsulation: PPP
    Public/Private: Public
    MTU: 1500
    TCP-Maximum Segment Size Clamping: Disabled
    TCP-Maximum Segment Size [bytes]: 1460
CES#
```

show interface serial ppp

Use this command to display serial interface PPP configuration information.

Syntax

show interface serial <*slot*>/<*port*> **ppp**

Parameters

slot	Specifies the slot of the serial interface.
port	Specifies the port of the serial interface.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Interface <slot>/<port> does not exist
```

Related commands

show interface bri
show interface dial
show interface serial statistics

Example

The following example shows the type of information displayed by the command.

```
CES# show interface serial 2/1 ppp
  Interface: serial Slot 1 Port 1
    Type: private
    Authentication: CHAP
    IP local: 47.10.234.11
    IP remote: 47.10.234.12
    IPCP VJ Connect ID Compression Negotiation: enabled
    IPCP VJ Max Slots: 4
    IPCP VJ Negotiation: enabled
    LCP Address Control Field Compression: enabled
    LCP Protocol-field-compression: enabled
    LCP Echo Fault Threshold: 2
    LCP Echo Interval: 2
    LCP-NCP Interface Debug: enabled
    Username: administrator
CES#
```

show interface serial statistics

Use this command to display serial interface statistics information.

Syntax

show interface serial <*slot*>/<*port*> **statistics**

Parameters

slot	Specifies the slot of the serial interface that you want to display statistics for.
port	Specifies the port of the serial interface that you want to display statistics for.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

show interface bri statistics
show interface dial statistics
show interface serial ppp

Example

The following example displays statistics for serial interface 2/1 running PPP.

```
CES# show interface serial 2/1 statistics
Date 12/02/2002  Time 18:55:37
WAN Slot 2 Interface 1
        PHY: Down
        Administrative State: Enabled
        Link Protocol: PPP
        NCP:  IPCP


  Interface Packet Statistics
  ===========================
       InPackets =               0             OutPackets =               0
       InGood =                  0             OutGood =                  0
       InOctets =                0             OutOctets =                0
       InErrors =                0             OutErrors =                0
       InNoBuffErrs =            0             OutNoBuffErrs =            0
       InOverrunErrs =           0             OutUnderrunErrs =          0
        InCRCErrs =               0
        InGiantErrs =             0
        InFramingErrs =           0


  Hardware Information
  ====================
        PHY ID model:   0x4
        PHY ID rev:     0x3
        Interface: none
        Clocking: External

CES#
```

The following example displays statistics for serial interface 2/1 running frame relay.

```
CES# show interface serial 2/1 statistics
  WAN Slot 2 Interface 1
    PHY: Down
    Administrative State: Enabled
    Link Protocol: Frame Relay

    Interface Packet Statistics
    ===========================
    InPackets =                0      OutPackets =               0
    InGood =                   0      OutGood =                  0
    InOctets =                 0      OutOctets =                0
    InErrors =                 0      OutErrors =                0
    InNoBuffErrs =             0      OutNoBuffErrs =            0
    InOverrunErrs =            0      OutUnderrunErrs =          0
    InCRCErrs =                0
    InGiantErrs =              0
    InFramingErrs =            0

    Frame Relay Stack Packet Statistics
    ===================================
    BadCallRef =               0      BadProDis =                0
    BadFrame =                 0      BadReportType =            0
    BadFullStat =              0      BadSnglStat =              0
    BadIeLinkIntg =            0      BadStatEnq =               0
    BadIeReportType =          0      BufShortage =              0
    BadLinkInteg =             0      PeerNotResp =              0
    BadLockShift =             0      ShortFrame =               0
    BadMsgType =               0      ZeroSendSeqNo =            0
    BadEncapIn =               0      BadDecapIn =               0
    UnknownDlci =              0

    Hardware Information
    ====================
    PHY ID model:0x4
    PHY ID rev:0x0
    Interface: XOVER
    Clocking: External
    DSR:
    DTR: Deasserted
```

Chapter 30
T1 and E1 CSU/DSU commands

This chapter provides information about T1 and E1 CSU/DSU commands.

Command	Page
clock source	1464
controller	1466
framing	1468
invert data	1469
line-buildout	1471
linecode	1472
performance-report-message	1474
show controller	1476
timeslot	1478
tx-ringsize	1480

clock source

Use this command to set the CSU/DSU clock source. Use the **no** form of the command to reset the clock source to the default value (loop, that is, external). In general, you set the clock source to internal for test purposes only.

Syntax

```
clock source {internal | loop}
no clock source
```

Parameters

internal	Set the clock source to be internal to the interface card.
loop	Set the clock source to loop back to the transmission side of the interface card; that is, the timing is determined by the T1 service provider.

Default

loop

Command mode

Controller Configuration

Next command mode

Controller Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

controller
framing
invert data
line-buildout
linecode
performance-report-message
show controller
timeslot

Example

The following example sets the clock source of the T1 CSU/DSU to internal.

```
CES(config)# controller t1 1/1
CES(config-controller)# clock source internal
CES(config-controller)#
```

The following example sets the clock source of the T1 CSU/DSU to loop.

```
CES(config)# controller t1 1/1
CES(config-controller)# clock source loop
CES(config-controller)#
```

The following example resets the clock source of the E1 CSU/DSU to its default value, that is, loop.

```
CES(config)# controller e1 1/1
CES(config-controller)# no clock source
CES(config-controller)#
```

controller

Use this command to configure T1 or E1 controller parameters and to enter Controller Configuration mode.

Syntax

controller {**e1** | **t1**} <*slot*>/<*port*>

Parameters

e1	Set the line format to E1.
t1	Set the line format to T1.
slot	Specifies the slot containing the E1 or T1 interface card that you want to configure. Type an integer from 0 through 6.
port	Specifies the port on the E1 or T1 interface card that you want to configure. Type an integer from 1 through 4.

Default

T1

Command mode

Global Configuration

Next command mode

Controller Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

If you enter the **controller** command and specify an interface card that does not support E1 or T1, the following message is displayed:

```
% invalid card type for a controller
```

Related commands

clock source
framing
invert data
line-buildout
linecode
performance-report-message
show controller
timeslot

Example

The following example sets the line format for interface 1/1 to E1 and enters Controller Configuration mode.

```
CES# config terminal
CES(config)# controller e1 1/1
CES(config-controller)#
```

The following example sets the line format for interface 2/1 to T1 and enters Controller Configuration mode.

```
CES# config terminal
CES(config)# controller t1 2/1
CES(config-controller)#
```

framing

Use this command to set the frame format for the T1 data line. Framing determines how the data is encapsulated and handles the signaling for alarms and loopbacks. The T1 provider supplies the frame format to enter.



Note: This command applies to T1 interfaces only. For E1, only unframed format is supported.

Syntax

```
framing {esf | sf}
```

Parameters

esf	Set the T1 frame format to extended superframe.
sf	Set the T1 frame format to superframe.

Default

ESF (extended superframe)

Command mode

Controller Configuration

Next command mode

Controller Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

clock source
controller
invert data
line-buildout
linecode
performance-report-message
show controller
timeslot

Example

The following example sets the T1 frame format for the CSU/DSU to superframe.

```
CES(config)# controller t1 1/1
CES(config-controller)# framing sf
CES(config-controller)#
```

invert data

Use this command to set the HDLC signal polarity of HDLC data lines. Use the **no** form of this command to reset the signal polarity to its default value, normal.



Note: The HDLC signal polarity must be set to the same value—inverted or normal—on both the local and remote CSU/DSU.

Syntax

invert data
no invert data

Parameters

None

Default

normal

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

clock source
controller
framing
line-buildout
linecode
performance-report-message
show controller
timeslot

Example

The following example sets the HDLC signal polarity of the CSU/DSU to inverted.

```
CES(config)# interface serial 1/1
CES(config-if)# invert data
CES(config-if)#
```

The following example resets the HDLC signal polarity of the CSU/DSU to normal.

```
CES(config)# interface serial 1/1
CES(config-if)# no invert data
CES(config-if)#
```

line-buildout

Use this command to set the signal output levels of T1 with integrated CSU/DSU lines. The distance between the CSU/DSU and the T1 provider's gateway determines the value to specify.

Note: This command applies to T1 lines only. E1 lines always use the default buildout value, 0 dB.

Syntax

line-buildout {0 | -7.5 | -15 | -22.5}

Parameters

0, **-7.5**, **-15**, **-22.5**	Specify the signal output level in decibels (dB).

Default

0 dB

Command mode

Controller Configuration

Next command mode

Controller Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

clock source
controller
framing
invert data
linecode
performance-report-message
show controller
timeslot

Example

The following example sets the output level of the CSU/DSU to -7.5 dB.

```
CES(config)# controller t1 1/1
CES(config-controller)# line-buildout -7.5
CES(config-controller)#
```

linecode

Use this command to set the encoding of binary digits on the T1 lines. The T1 service provider supplies this value.

Note: This command applies to T1 lines only. E1 lines always use the default line code value for E1, HDB3 (high-density bipolar coding).

Syntax

linecode {**ami** | **b8zs**}

Parameters

ami	Set the line code type to alternate mark inversion (AMI).
b8zs	Set the line code type to bipolar with 8 zero substitution (B8ZS).

Default

B8ZS

Command mode

Controller Configuration

Next command mode

Controller Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

clock source
controller
framing
invert data
line-buildout
performance-report-message
show controller
timeslot

Example

The following example sets the T1 line coding to AMI.

```
CES(config)# controller t1 1/1
CES(config-controller)# linecode ami
CES(config-controller)#
```

The following example sets the T1 line coding to B8ZS.

```
CES(config)# controller t1 1/1
CES(config-controller)# linecode b8zs
CES(config-controller)#
```

performance-report-message

Use this command to set the performance report message format for T1 lines if the framing format is set to extended superframe (ESF). The T1 service provider supplies this value. Use the **no** form of the command to reset the parameter to its default value, ANSI.



Note: If the framing format is set to superframe (SF), you should set the performance report message format to none.

Syntax

```
performance-report-message {ansi | ds1-mib | none}
no performance-report-message
```

Parameters

ansi	Set the T1 performance reporting message to ANSI standard.
ds1-mib	Set the T1 performance reporting message to DS-1 MIB.
none	Specify that no T1 performance report will be generated.

Default

ANSI

Command mode

Controller Configuration

Next command mode

Controller Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

clock source
controller
framing
invert data
line-buildout
linecode
show controller
timeslot

Example

The following example sets the T1 performance report message to “none.”

```
CES(config)# controller t1 1/1
CES(config-controller)# performance-report-message none
CES(config-controller)#
```

The following example resets the T1 performance report message to the default value, ANSI.

```
CES(config)# controller t1 1/1
CES(config-controller)# no performance-report-message
CES(config-controller)#
```

show controller

Use this command to display T1 or E1 CSU/DSU attributes.

Syntax

show controller {**e1** | **t1**} <*slot*>/<*port*>

Parameters

e1	Display E1 controller information.
t1	Display T1 controller information.
slot	Specifies the slot containing the E1 or T1 interface card that you want to display information about. Type an integer from 0 through 6.
port	Specifies the port on the E1 or T1 interface card that you want to display information about. Type an integer from 1 through 4.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

If you enter the **`show controller t1`** command for an E1 controller or the reverse, the following message is displayed:

```
% incorrect controller specified
```

If you enter the **`show controller`** command and specify an interface card that does not support E1 or T1, the following message is displayed:

```
% invalid card type for a controller
```

Related commands

`clock source`
`controller`
`framing`
`line-buildout`
`linecode`
`performance-report-message`
`timeslot`

Example

The following example displays information about the T1 controller for interface 1/1.

```
CES# show controller t1 1/1
  Controller: Slot 1 Port 1
    Clock Source: Loop
    Build Out: 0 dB
    Line Code: AMI
    Framing: ESF
    Performance Report Message: DS1 MIB
    Fractional T1 Start Channel: 12
    Fractional T1 Bandwidth: 256 Kbps
CES#
```

The following example displays information about an E1 controller.

```
CES# show controller e1 2/1
  Controller: Slot 2 Port 1
    Clock Source: Loop
    Build Out: 0 dB
    Line Code: HDB3
    Framing: UF
    Performance Report Message: none
CES#
```

timeslot

Use this command to configure fractional T1. You can configure channel 0 for frame synchronization (“framed T1”) or for data transfer (“unframed T1”). Use the **no** form of the command to set “unframed” line framing operation.

Syntax

timeslot *<start_channel> <Kb_per_second>*
no timeslot

Parameters

start_channel	Specifies the first channel to be used for fractional T1. Enter an integer from 1 through 24.
Kb_per_second	Specifies the kilobits per second (Kb/s) to allocate to this connection. Enter a multiple of 64—that is, 64 multiplied by the number of channels you are allocating. Each channel represents bandwidth in the amount of 64 Kb/s. For example, to reserve 5 channels for fractional T1 service that begin with channel 1, enter **timeslot 1 320** (that is, 5*64 Kb/s).

Default

Start channel is 1; bandwidth allocation is 1536 Kb/s.

Command mode

Controller Configuration

Next command mode

Controller Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

clock source
controller
framing
invert data
line-buildout
linecode
performance-report-message
show controller

Example

The following example configures channels 7-14 for fractional T1 transmission with bandwidth of 512 Kb/s (64 * 8 channels).

```
CES(config)# controller t1 1/1
CES(config-controller)# timeslot 7 512
CES(config-controller)#
```

tx-ringsize

Use this command to set the size of the transmit ring.

Syntax

tx-ringsize
no tx-ringsize

Parameters

transmit ring size	Value must be a power of 2. Valid ring sizes are 1,2, 4, 8, 16, 32, 64, 128. <1-128>

Default

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

Example

```
CES(config-if)# tx-ringsize <transmit ring size>
CES(config-if)# no tx-ringsize
```

Chapter 31
Frame relay commands

This chapter provides information about frame relay configuration commands.

Command	Page
class	1484
cost	1485
description	1487
dlci	1489
encapsulation (interface)	1490
encapsulation (subinterface)	1492
fragment	1494
frame-relay bc	1495
frame-relay be	1496
frame-relay cir	1498
frame-relay connection-type	1499
“frame-relay debug	1501
“frame-relay lmi-n391dte	1503
“frame-relay lmi-t391dte	1504
“frame-relay lmi-type	1506
“frame-relay subinterface	1507
“interleave	1510
“interface	1511
“inverse-arp	1513
“ip local	1514
“ip ospf	1516

Command	Page
“ip remote	1518
“ip rip	1519
“map-class frame-relay	1521
“payload-compress frf9	1522
“priority	1524
“public	1526
“show frame-relay lmi	1527
“show frame-relay pvc	1529
“traffic-shape rate	1532

class

This command associates a subinterface with a previously created map class. Use the no form of the command to remove the association.

Syntax

class *map-class-name*
no class

Parameters

map-class-name text name of the associated map class

Default

none

Command mode

subinterface configuration (config-subif)

Next command mode

subinterface configuration (config-subif)

Prerequisites

The map class must exist.

Warnings

% map class does not exist

Required Privileges

System Management - Manage

User Management - None

Related Commands

map-class frame-relay map-class-name

Example

Example of configuring a subinterface with map class "gold".

```
CES(config)# interface serial 2/1
CES(config-if)# subinterface 1
CES(config-subif)# class gold
CES(config-subif)#
```

cost

Use this command to specify the routing cost for the local IP address on the subinterface. Use the **no** form of the command to return the cost to its default value, 1000.

Syntax

cost <*number*>
no cost

Parameters

number	Specifies the routing cost for the local IP address on the subinterface. You can enter any integer from 10 through 1000.

Default

1000

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

description
dlci
encapsulation MPoFR
frame-relay subinterface
public
traffic-shape rate
show frame-relay pvc

Example

The following example specifies a routing cost of 200 for the subinterface.

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# cost 200
CES(config-subif)#
```

The following example restores the default routing cost (1000) on this subinterface.

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# no cost
CES(config-subif)#
```

description

Use this command to set a text description for the subinterface. Use the **no** form of the command to delete this text.

The interface description appears in the result of the ifName MIB.

Syntax

description <*text*>
no description

Parameters

text	Specifies a text description of the subinterface. Enter up to 127 characters. If the text includes spaces, enclose it in quotation marks.

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

cost
dlci
encapsulation MPoFR
frame-relay subinterface
public
traffic-shape rate
show frame-relay pvc

Example

The following example creates a description for subinterface 2.

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay subinterface 2
CES(config-subif)# description “My local interface to CO”
CES(config-subif)#
```

dlci

Use this command to specify the data link connection identifier (DLCI) for a subinterface. Use the **no** form of this command to delete the DLCI.

Syntax

dlci <*number*>
no dlci

Parameters

number	Specifies the DLCI for the local subinterface. Type an integer from 16-991.

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

cost
description
encapsulation MPoFR
frame-relay subinterface
public
traffic-shape rate
show frame-relay pvc

Example

The following example configures the DLCI for subinterface 1.

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# dlci 5
CES(config-subif)#
```

encapsulation (interface)

Use this command to select the next encapsulation protocol for the serial interface. Use the **no** form of this command to return the encapsulation to its default value (PPP).

Syntax

encapsulation {**ppp** | **frame-relay**}
no encapsulation

Parameters

ppp	Specifies that the next encapsulation protocol on this interface is PPP.
frame-relay	Specifies that the next encapsulation protocol on this interface is frame relay.

Default

PPP

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

frame-relay connection-type
frame-relay lmi-n391dte
frame-relay lmi-t391dte
frame-relay lmi-type
show frame-relay lmi

Example

The following example configures serial interface 2/1 for the frame relay protocol.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation frame-relay
CES(config-if)#
```

encapsulation (subinterface)

Use this command to set encapsulation for a subinterface. Use the **no** form of this command to delete the encapsulation identifier.

Syntax

encapsulation MPoFR
encapsulation PPPoFR {ip|ipcp |lcp| lcp-ncp |password| username}
no encapsulation

Parameters

MPoFR	Specifies multiprotocol over frame relay (RFC 1490) encapsulation on this subinterface.
PPPoFR	Specifies PPP over frame relay encapsulation on this subinterface. To configure PPP, use the following parameters: • authentication—Enables PPP authentication • ip— Configures PPP IP parameters • ipcp— Configures IPCP parameters • lcp— Configures LCP parameters • lcp-ncp— Configures LCP/NCP parameters • password— Chap/Pap password • username — User ID

Default

MPoFR

PPPoFR

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

cost
description
dlci
frame-relay subinterface
public
traffic-shape rate
show frame-relay pvc

Example

The following example configures MPoFR (RFC 1490) on subinterface 1.

```
CES(config)# interface serial 1/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# encapsulation MPoFR
CES(config-subif)#
```

fragment

This command configures the virtual circuit to use ETE fragmentation and sets the fragment size to a specified value. If no fragment size is specified than this will take the previous value, and this value will also be printed. The no form disable this feature.

Syntax

```
no fragment
fragment [fragmentSize]
```

Parameters

fragmentSize— integer specifying the size of a fragment - with a value between 40 and 800.

Default

80

Command mode

Subinterface Configuration

Next Command Mode

Sub-interface configuration

Related commands

interleave

Example

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# interleave 200
CES(config-subif)#
```

frame-relay bc

This command configures the frame relay traffic shaping Committed Burst Size (Bc) parameter for a frame relay map class.

Syntax

frame-relay bc *bc*

Parameters

bc—committed burst size, in bits

min 0, max line rate

Default

0

Command mode

map class configuration (config-map-class)

Next command mode

map class configuration (config-map-class)

Prerequisites

Map class must be created

Warnings

% bc out of range

Required privileges

System Management - Manage

User Management - None

Related commands

```
[no] class
[no] map-class frame-relay map-class-name
traffic-shape rate { cir [ bc [ be ]]}
```

Example

Example of configuring the frame relay map class "gold" with a Bc of 64,000 bits.

```
CES(config)# map-class frame-relay gold
CES(config-map-class)# frame-relay bc 64000
CES(config-map-class)#
```

frame-relay be

This command configures the frame relay traffic shaping Excess Burst Size (Be) parameter for a frame relay map class.

Syntax

```
frame-relay be be
```

Parameters

excess burst size, in bits

min 0, max line rate

Default

0

Command mode

map class configuration (config-map-class)

Next command mode

map class configuration (config-map-class)

Prerequisites

Map class must be created

Warnings

% be out of range

Required privileges

System Management - Manage

User Management - None

Related commands

[no] class
[no] map-class frame-relay map-class-name
traffic-shape rate { cir [bc [be]]}

Example

Example of configuring the frame relay map class "gold" with a Be of 192,000 bits.

```
CES(config)# map-class frame-relay gold
CES(config-map-class)# frame-relay be 192000
CES(config-map-class)#
```

frame-relay cir

This command configures the frame relay traffic shaping Committed Information Rate (CIR) parameter for a frame relay map class.

Syntax

frame-relay cir cir

Parameters

cir—committed information rate, in bits per second

min 0, max line rate

Default

None

Command mode

map class configuration (config-map-class)

Next command mode

map class configuration (config-map-class)

Prerequisites

Map class must be created

Warnings

% cir out of range

Required privileges

System Management - Manage

User Management - None

Related commands

[no] class
[no] map-class frame-relay map-class-name
traffic-shape rate { cir [bc [be]]}

Example

Example of configuring the frame relay map class "gold" with a CIR of 64,000 bits per second.

```
CES(config)# map-class frame-relay gold
CES(config-map-class)# frame-relay cir 64000
CES(config-map-class)#
```

frame-relay connection-type

Use this command to select the connection type. Use the **no** form of this command to return to the default connection type.

Syntax

```
frame-relay connection-type {direct | switched}
no frame-relay connection-type
```

Parameters

direct	Indicates that there is a direct connection between two frame relay devices. Use this setting if you want to connect two Nortel VPN Router devices back to back.
switched	Indicates that there is a switched connection between two frame relay devices, that is, the gateway is configured as a DTE device connected to a frame relay switch.

Default

Switched

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

encapsulation
frame-relay debug
frame-relay lmi-n391dte
frame-relay lmi-t391dte
frame-relay lmi-type
show frame-relay lmi

Example

The following example sets the frame relay interface connection type.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation frame-relay
CES(config-if)# frame-relay connection-type direct
CES(config-if)#
```

frame-relay debug

Use this command to enable debug mode on a frame relay interface. In debug mode, frame relay packets are logged in the event log. Use the **no** form of this command to disable debug mode.

Syntax

frame-relay <*slot*>/<*port*> **debug**
no frame-relay <*slot*>/<*port*> **debug**

Parameters

slot	Specifies the slot number that the card is installed in.
port	Specifies the port number on the installed card.

Default

Debug mode is disabled.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

frame-relay connection-type
frame-relay subinterface debug

Example

The following example enables frame relay debug mode on port 1 of the card in slot 2.

```
CES(config)# frame-relay 2/1 debug
CES(config)#
```

The following example disables frame relay debug mode on port 1 of the card in slot 2.

```
CES(config)# no frame-relay 2/1 debug
CES(config)#
```

frame-relay lmi-n391dte

Use this command to set a full status polling counter for the LMI. Use the **no** form of the command to return the counter to its default value, 6.

Syntax

frame-relay lmi-n391dte <*keepalive-exchanges*>
no frame-relay lmi-n391dte

Parameters

keepalive-exchanges	Specifies the number of keepalive exchanges that must transpire before requesting a full status message. You can set this value to any integer from 1 through 255.

Default

6 keepalive exchanges

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

encapsulation
frame-relay connection-type
frame-relay lmi-t391dte
frame-relay lmi-type
show frame-relay lmi

Example

The following example configures the Nortel VPN Router to request a full status response from the gateway after every fourth status inquiry. The other three status inquiries will request keepalive exchanges only.

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay lmi-n391dte 4
CES(config-if)#
```

frame-relay lmi-t391dte

Use this command to set a full status polling interval for the LMI. Use the **no** form of the command to return the interval to its default value, 10.

Syntax

frame-relay lmi-t391dte <*seconds*>
no frame-relay lmi-t391dte

Parameters

seconds	Specifies the number of seconds between keepalive exchanges when requesting a full status message. You can enter any integer from 5 through 30.

Default

10 seconds

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

encapsulation
frame-relay connection-type
frame-relay lmi-n391dte
frame-relay lmi-type
show frame-relay lmi

Example

The following example configures a 30-second interval between inquiries when generating a full status response from the gateway.

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay lmi-t391dte 30
CES(config-if)#
```

frame-relay lmi-type

Use this command to specify the Local Management Interface (LMI) type. Use the **no** form of the command to reset the LMI type to its default value.

Syntax

```
frame-relay lmi-type {ansi | ilmi | none | q933a}
no frame-relay lmi-type
```

Parameters

ansi	Sets the LMI type to Annex D (defined by ANSI standard T1.617).
ilmi	Sets the LMI type to Interim Local Management Interface (ILMI).
none	Sets the LMI type to “none” (no LMI type).
q933a	Sets the LMI type to ITU-T Q.933 Annex A.

Default

Q.933 Annex A

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

encapsulation
frame-relay connection-type
frame-relay lmi-n391dte
frame-relay lmi-t391dte
show frame-relay lmi

Example

The following example sets the LMI type on the interface to ANSI Annex D.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation frame-relay
CES(config-if)# frame-relay lmi-type ansi
CES(config-if)#
```

frame-relay subinterface

Use this command to create a subinterface or to enable a configured one. The **no** form of this command deletes a frame relay subinterface or disables it. Used with the **debug** option, this command puts the subinterface into debug mode. The **no** form of the **frame-relay subinterface debug** command exits debug mode.

Syntax

frame-relay subinterface <*subinterface*> [{**enable** | **debug**}]
no frame-relay subinterface <*subinterface*> [{**enable** | **debug**}]

Parameters

subinterface	Specifies the subinterface (PVC) that you are configuring. Type an integer from 1 through 10.
enable	Enables the specified PVC.
debug	Places the specified subinterface into debug mode. In debug mode, packets are parsed and displayed in the event log. This mode adversely affects performance, so disable debug mode during normal operation.

Default

When you create a subinterface, it is enabled.

Command mode

Interface Configuration

Next command mode

Subinterface Configuration (when subinterface is created)
Interface Configuration (when subinterface is enabled or set to debug mode)

Required privileges

System Management - Manage
User Management - None

Related commands

description
dlci
encapsulation MPoFR
frame-relay subinterface
public
traffic-shape rate
show frame-relay pvc

Example

The following example creates subinterface 3 on port 1 of the card in slot 2 and then disables it.

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay subinterface 3
CES(config-subif)# exit
CES(config-if)# no frame-relay subinterface 3 enable
CES(config-if)#
```

The following example reenables subinterface 3 on port 1 of the card in slot 2.

```
CES(config-if)# frame-relay subinterface 3 enable
CES(config-if)#
```

The following example deletes subinterface 3 on port 1 of the card in slot 2.

```
CES(config)# interface serial 2/1
CES(config-if)# no frame-relay subinterface 3
CES(config-if)#
```

The following example places subinterface 3 into debug mode.

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay subinterface 3 debug
CES(config-if)#
```

The following example exits debug mode on subinterface 3 on port 1 of the card in slot 2.

```
CES(config)# interface serial 2/1
CES(config-if)# no frame-relay subinterface 3 debug
CES(config-if)#
```

interleave

This command enables interleaving of packets on this interface. The no form disables this feature.

Syntax

```
no frame-relay interleave
frame-relay interleave
```

Parameters

None

Default

None

Command mode

Interface configuration

Next Command Mode

Interface configuration

Related commands

fragment

Example

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay interleave
CES(config-if)#
```

interface

This command is used to begin configuration of a serial interface.

Syntax

interface type slot/port

Parameters

type—Specifies interface type. For Frame Relay interface must be serial.

slot—Interface slot number. Permitted values are [1-6].

port—Interface port number. Permitted values are [1-4]. Please note the change from the previous values [0-1] to [1-4].

Default

None

Command mode

Global Configuration

Next command mode

Interface Configuration

Prerequisites

There must be a serial System WAN interface card on this slot. Permitted cards are: Multi-port V.35 (WANic400), single-port HSSI (WANic700), and Multi-port T1 support (LMC150x).

Warnings

% interface 2/3 does not exist

% serial card does not exist

Required privileges

System Management - Manage

User Management - None

Related commands

None

Example

Example of a successful help for the interface command:

```
CES(config)# interface serial ?
slot Specifies slot of the interface card [1-6]
port Specifies port of the interface card [1-4]
CES(config)#
```

Example of a successful start of configuring of an serial interface on System WAN card in slot 2 port 3:

```
CES(config)# interface serial 2/3
CES(config-if)#
```

inverse-arp

This command re-enables Inverse ARP on a specified interface or subinterface. Use the no form of this command to disable this feature.

To enable or disable IARP for all DLCIs on the specified interface or subinterface, omit the DLCI number.

This implementation of IARP is based on RFC1293. It allows CES running Frame Relay to discover the protocol address of a device associated with the virtual circuit.

The show frame-relay map command displays the word "dynamic" to flag virtual circuits that are created dynamically by IARP.

Syntax

```
inverse-arp ip
no inverse-arp ip
```

Parameters

protocol—specifies protocol. Currently supported protocol is ip only.

Default

Enabled

Command mode

Sub-interface configuration

Next command mode

Sub-interface configuration

Required privileges

System Management - Manage

User Management - None

Related commands

```
clear frame-relay-inarp ?
show frame-relay map
```

Example

In the following example, the serial interface already has a basic configuration. Below you may see how to set IARP on sub-interface 1:

```
CES(config)# interface serial 1/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# inverse-arp ip
```

This is an example of successful disabling of IARP on sub-interface 1:

```
CES(config)# interface serial 1/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# no inverse-arp ip
```

ip local

Use this command to assign an IP address to the local subinterface. Use the **no** form of this command to delete the IP address.

Syntax

```
ip local <address> [mask]
no ip local
```

Parameters

address	Specifies the IP address associated with the local PVC.
mask	Specifies the subnet mask for the IP address configured on the local PVC. Configure a mask only if this subinterface is private.

Default

Subnet mask: 255.255.255.255

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

frame-relay subinterface
ip ospf
ip remote
ip rip
show frame-relay pvc

Example

The following example configures a local IP address on frame relay PVC 1.

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# ip local 10.10.10.1
CES(config-subif)#
```

The following example configures a local IP address and mask for frame relay PVC 1.

```
CES(config)# interface serial 2/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# no public
CES(config-subif)# ip local 10.10.10.1 255.255.255.0
CES(config-subif)#
```

ip ospf

Use this command to enable OSPF on the subinterface. Use the **no** form of this command to disable OSPF.

Note: You can configure OSPF on a frame relay subinterface with the same commands that you use to configure it on a LAN interface. For information about OSPF commands, see Chapter 23, “IP interface configuration commands,” on page 1159.

Syntax

```
ip ospf
no ip ospf
```

Parameters

None

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% OSPF is only available when the sub-interface is Private
```

Related commands

frame-relay subinterface
ip local
ip remote
ip rip
show frame-relay pvc

Example

The following example enables OSPF on subinterface 3.

```
CES(config)# interface serial 1/1
CES(config-if)# frame-relay subinterface 3
CES(config-subif)# ip ospf
CES(config-subif)#
```

ip remote

Use this command to assign an IP address to the remote side of this virtual circuit. Use the **no** form of this command to delete this IP address.

Syntax

```
ip remote <address>
ip remote <negotiated>
no ip remote
```

Parameters

address	Specifies the IP address associated with the remote PVC.
negotiated	Specifies that this subinterface will accept a negotiated IP address for its remote peer.

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
frame-relay subinterface
ip local
ip ospf
ip rip
show frame-relay pvc
```

Example

The following example configures a remote IP address for frame relay PVC 1.

```
CES(config)# interface serial 1/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# ip remote 10.10.10.2
CES(config-subif)#
```

ip rip

Use this command to enable RIP on the subinterface. Use the **no** form of this command to disable RIP.



Note: You can configure RIP on a frame relay subinterface with the same commands that you use to configure it on a LAN interface. For information about RIP commands, see Chapter 23, “IP interface configuration commands,” on page 1159.

Syntax

```
ip rip
no ip rip
```

Parameters

None

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% RIP is only available when the sub-interface is Private
```

Related commands

frame-relay subinterface
ip local
ip ospf
ip remote
show frame-relay pvc

Example

The following example enables RIP on subinterface 2.

```
CES(config)# interface serial 1/1
CES(config-if)# frame-relay subinterface 2
CES(config-subif)# ip rip
CES(config-subif)#
```

map-class frame-relay

This command creates and/or modifies a map-class name to define quality of service (QoS) values for a virtual circuit. Use the no form of this command to delete the map class.

This command first appeared in CES Release Fenway

Syntax

[no] map-class frame-relay map-class-name

Parameters

map-class-name—name of this map class.

Default

None

Command mode

Global configuration

Next command mode

Map Class Configuration - creation, modification

Global Configuration - deletion

Required privileges

System Management - Manage

User Management - None

Related commands

```
[no] class
frame-relay bc
frame-relay be
frame-relay cir
```

Example

Example of creating a frame relay map-class named "gold".

```
CES(config)# map-class frame-relay gold
CES(config-map-class)# exit
CES(config)#
```

Example of deleting a frame relay map-class named "gold".

```
CES(config)# no map-class frame-relay gold
CES(config)#
```

payload-compress frf9

This command is used to enable LZS payload compression on a specified sub-interface. This algorithm is supported by both the CES s/w and CES h/w accelerator. If FRF9 compression is enabled, then the CES will attempt to negotiate a compression algorithm (currently, there will be LZS only). If the remote end does not support FRF9 or if it supports FRF9 but does not support LZS compression, then data compression will not be performed on the VC.

Use the no form of this command to disable payload compression on a specified subinterface.

This command first appeared in CES Release Coolidge.

Syntax

```
payload-compress frf9
no payload-compress frf9
```

Parameters

None

Default

Disabled

Command mode

Sub-interface configuration

Next command mode

Sub-interface configuration

Required privileges

System Management - Manage

User Management - None

Related commands

Example

Example of enabling of FRF9 compression on sub-interface 1.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation frame-relay
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# payload-compress frf9

CES(config-subif)#
```

Example of disabling of FRF9 compression on sub-interface 1.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation frame-relay
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# no payload-compress
CES(config-subif)#
```

priority

This command specifies a a queue number for the virtual circuit. Use the no form of this command to return to the default value.

Syntax

```
priority number
no priority
```

Parameters

number—Priority queue number. Permitted values are:

0 - None

1 - Low

2 - Medium

3 - High

4 - Highest

Default

None

Command mode

Subinterface configuration

Next command mode

Subinterface configuration

Required privileges

System Management - Manage

User Management - None

Related commands

None

Example

Example of specifying high priority (queue 3) for traffic on sub-interface 100.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation frame-relay
CES(config-if)# frame-relay subinterface 100
CES(config-subif)# priority 3
CES(config-subif)#
```

Example of specifying the default no priority (queue 0) for traffic on sub-interface 100.

```
CES(config)# interface serial 2/1
CES(config-if)# encapsulation frame-relay
CES(config-if)# frame-relay subinterface 100
CES(config-subif)# no priority
```

public

On the Nortel VPN Router device, a subinterface is defined either as public or private. Use this command to configure a subinterface as a public (untrusted) subinterface. Use the **no** form of this command to reset the value to the default (private).

Syntax

```
public
no public
```

Parameters

None

Default

Private

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

cost
description
dlci
encapsulation MPoFR
frame-relay subinterface
traffic-shape rate
show frame-relay pvc

Example

The following example configures subinterface 1 as public.

```
CES(config)# interface serial 1/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# public
CES(config-subif)#
```

The following example configures subinterface 1 as private.

```
CES(config)# interface serial 1/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# no public
CES(config-subif)#
```

show frame-relay lmi

Use this command to display frame relay LMI statistics.

Syntax

frame-relay lmi-type
show frame-relay lmi

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

frame-relay connection-type
frame-relay lmi-n391dte
frame-relay lmi-t391dte
frame-relay lmi-type
show frame-relay pvc

Example

The following example displays frame relay LMI statistics.

```
CES# show frame-relay lmi
  Interface: serial Slot 1 Port 1
    Connection-type: Switched
    LMI N391dte: 10 times
    LMI T391dte: 15 seconds
    LMI Type: ansi
    LMI Statistics
      Invalid Unnumbered Info: 0
      Invalid Prot Disc: 0
      Invalid Dummy Call Ref: 0
      Invalid Message Type: 0
      Invalid Status Enquiry: 0
      Invalid Lock Shift: 0
      Num Buffer Shortages: 0
      Invalid Report Type IE: 0
      Invalid Report Type: 0
      Invalid Link Integrity IE: 0
      Invalid Full Stat: 0
      Invalid Link Integrity Type: 0
      Num Status Timeout: 0
      Invalid Signaling Status: 0
      Invalid Encapsulation In: 0
      Invalid Decapsulation In: 0
      Num Short Frames: 0
      Invalid Send Seq Num: 0
      Num Unknown DLCI: 0
CES#
```

show frame-relay pvc

Use this command to display frame relay PVC (subinterface) statistics.

Syntax

show frame-relay pvc

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

description
dlci
encapsulation MPoFR
frame-relay subinterface
public
traffic-shape rate
show frame-relay lmi

Example

The following example displays frame relay statistics for all configured VCs.

```
CES# show frame-relay pvc
  Interface: serial Slot 1 Port 1

    Subinterface: 1
      Description: branch 1001
      Type: private
      DLCI: 1111
      Encapsulation: mpofr
      IP local: 47.12.45.21
      IP remote: 47.105.15.45
      Traffic-shape
        in BECN pkts: 0       out BECN pkts: 0
        in FECN pkts: 0       out FECN pkts: 0
             in pkts: 0            out pkts: 0
            in bytes: 0           out bytes: 0
          in DE pkts: 0         out DE pkts: 0
        CIR: 56000 bps
        BC: 150000 bits
        BE: 100000 bits

      Subinterface: 2
        Description: branch 1002
        Type: private
        DLCI: 2222
        Encapsulation: mpofr
        IP local: 47.12.45.22
        IP remote: 47.105.25.55
      Traffic-shape
        in BECN pkts: 0       out BECN pkts: 0
        in FECN pkts: 0       out FECN pkts: 0
             in pkts: 0            out pkts: 0
            in bytes: 0           out bytes: 0
          in DE pkts: 0         out DE pkts: 0
        CIR: 56000 bps
        BC: 150000 bits
        BE: 100000 bits
CES#
```

traffic-shape rate

Use this command to set the following traffic shaping parameters for an individual subinterface. Use the **no** form of this command to reset the parameters to their default values.

- Committed information rate (CIR)
- Committed burst size (B_c)
- Excess burst size (B_e).

Syntax

```
traffic-shape rate <cir> [<bc> [<be>]]
no traffic-shape rate
```

Parameters

cir	Specifies the committed information rate in bits/second. • For the single V.35/X.21 WAN interface card, enter an integer from 0-1536000. • For the T1 CSU/DSU WAN interface card, enter an integer from 0-2048000.
bc	Specifies the committed burst size in bits. • For the single V.35/X.21 WAN interface card, enter an integer from 0-1536000. • For the T1 CSU/DSU WAN interface card, enter an integer from 0-2048000.
be	Specifies the excess burst size in bits. • For the single V.35/X.21 WAN interface card, enter an integer from 0-1536000. • For the T1 CSU/DSU WAN interface card, enter an integer from 0-2048000.

Default

None

Command mode

Subinterface Configuration

Next command mode

Subinterface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

cost
description
dlci
encapsulation MPoFR
frame-relay subinterface
public
show frame-relay pvc

Example

The following example specifies frame relay traffic shaping parameters for subinterface 1.

```
CES(config)# interface serial 1/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# traffic-shape rate 1500000 11000 10000
CES(config-subif)#
```

The following example resets the traffic shaping parameters to their default values.

```
CES(config)# interface serial 1/1
CES(config-if)# frame-relay subinterface 1
CES(config-subif)# no traffic-shape rate
CES(config-subif)#
```

Chapter 32
Demand Services configuration commands

This chapter describes Demand Services configuration commands. Demand Services replaces the Backup Interface Services (Bis) feature and functionality. All of the existing Bis functionality has been incorporated into Demand Services.

Under this design, a Demand interface is configured that is associated with a physical (usually dial) interface. The Demand interface defines the trigger event as well as the dialing parameters to be used.

Command	Page
dial	1536
demand	1538
demand add	1539
demand delay	1540
demand enable	1541
exit	1542
hours name	1543
interface	1546
interface-group	1548
ping	1549
priority	1551
redial	1553
remote-network	1555
route-unreachable	1557
show demand	1558

Command	Page
timeout	1560
trigger	1561
wait	1564

dial

Use this to configure a dial-on-demand on an interface. no dial removes dial-on-demand from the interface

Syntax

```
dial [primary | secondary | tertiary] <phone number> user
<user> password <password>

no dial
```

Parameters

`<name>`	Specifies a selection of an demand interface
`primary secondary tertiary`	Allows phone numbers to be provided from the specified demand interface. T
`<phone number>`	Type the phone numbers of
`<user>`	Type the name of the user.
`<password>`	Type the password

Default

Command mode

Demand Configuration

Next command mode

Demand Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

```
show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger
wait
no dial
remote-network
```

Example

```
CES(config-demand)# dial primary 555-555-5555 John pass
CES(config-demand)# no dial 555-555-5555 John pass
```

demand

Use this to edit an existing demand interface.

Syntax

demand <*demandinterface*>
no demand <*demandinterface*>

Parameters

<demandinterface>	Specifies a selection of a demand interface

Default

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

demand add
demand <demandinterface> **enable**
demand delay
exit
show demand

Example

```
CES(config)# demand <demandinterface>
CES(config)# no demand <demandinterface>
```

demand add

Use this to add a new demand interface.

Syntax

demand add <*demandinterface*>

Parameters

<demandinterface>	Specifies a selection of an interface

Default

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

demand
demand add
demand <demandinterface> **enable**
demand delay
exit
show demand

Example

CES(config)# **demand add** <*demandinterface*>

demand delay

Use this to set start up delay for a demand interface.

Syntax

demand delay <*numseconds*>

Parameters

<numseconds>	Specify a number of seconds of delay. Numseconds can be a value from 0 to 600 seconds.

Default

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

demand
demand add
demand <demandinterface> **enable**
exit
show demand

Example

```
CES(config)# demand delay 12
```

demand enable

Use this to enable a dial on demand interface.

Syntax

demand <demandinterface> **enable**
no demand <demandinterface> **enable**

Parameters

Default

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

demand
demand add
demand delay
exit
show demand

Example

```
CES(config)# demand <demandinterface> enable
CES(config)# no demand <demandinterface> enable
```

exit

Use this to exit a demand interface.

Syntax

exit

Parameters

None

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

demand
demand add
demand delay
show demand

Example

```
CES(config)# exit
```

hours name

Use this command to specify the days and hours that a Demand profile can be activated. T



Note: To configure a time specification, execute the **access-hours** command in Global Configuration mode, or go to the Profiles > Hours screen.

Syntax

hours name {**Anytime** | **Weekdays** | **Weekends**}

Parameters

None

Default

anytime (24 hours a day, 7 days a week)

Command mode

Demand Configuration

Next command mode

Demand Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger
wait
no dial
remote-network

Example

```
CES(config-demand)# hours name Weekdays
```

interface

Use this command to specify the physical interface.

Syntax

interface <*slot#interface#*>

Parameters

slot # interface #	Specifies the name of an existing interface.

Default

None

Command mode

Demand Configuration

Next command mode

Demand Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger
wait
no dial
remote-network

Example

```
CES(config-demand)# interface 3/7
```

interface-group

Use this command to specify the interface group.

Syntax

interface-group <*interface-group-name*>

Parameters

interface-group-name	Specifies the name of an existing interface group.

Default

None

Command mode

Demand Configuration

Next command mode

Demand Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger
wait
no dial
remote-network
```

Example

```
CES(config-demand)# interface-group LAN2
```

ping

Use this command to configure a Demand profile to activate the demand interface when a specific connection fails (the ping monitors this connection).

To ensure the "test" button on a ping trigger demand interface has a successful test, the ping destination must be unreachable during the test. This may be accomplished by using a temporary fake ping destination address while performing the test.

Syntax

ping <*dest_IP*> **source** <*slot*>/<*port*> [**retry** <*number*>] [**wait** <*seconds*>]

Parameters

dest_IP	Specifies in dotted-decimal notation the IP address of the system to ping. This connection is the entity that will be backed up.
slot/port	Specifies the interface on this Nortel VPN Router that is the source of the ping.
number	Specifies the maximum number of ping retries allowed before the gateway assumes that the connection has failed and triggers the backup interface. Enter an integer from 1 through 6. The default value is 3.
seconds	Specifies the maximum number of seconds that the gateway waits to receive an ICMP reply before it assumes that the connection has failed and triggers the backup interface. Enter an integer from 1 through 900. The default value is 5.

Default

Number of retries: 3
Number of seconds: 5

Command mode

Demand Configuration

Next command mode

Demand Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger
wait
no dial
remote-network
```

Example

```
CES(config-demand)# ping 192.222.222.22 0/3
```

priority

This command specifies a a queue number for the demand interface.

Syntax

priority <number>

Parameters

1-99

Default

None

Command mode

Demand configuration

Next command mode

Demand configuration

Required privileges

System Management - Manage

User Management - None

Related commands

```
show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger
wait
no dial
remote-network
```

Example

```
CES(config-demand)# priority 33
```

redial

Use this command to set the number of redial attempts for the Demand profile. The redial value specifies how many times the demand interface redials a telephone number before the connection is declared unreachable.

Syntax

redial <*number*>

Parameters

number	Specifies the number of redial attempts that the demand interface makes before it considers the called number unreachable. Enter a value from 1 through 255. The default value is 3.

Default

3

Command mode

Demand Configuration

Next command mode

Demand Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger
wait
no dial
remote-network
```

Example

```
CES(config/demand)# redial 10
CES(config/demand)#
```

remote-network

This command allows you to add, edit, or delete a remote network.

Syntax

remote-network add <*ipAddr*> **mask** <*maskIp*> **cost** <*cost*> **gateway** <*gateway*>

no remote-network <*ipAddr*> **mask** <*maskIp*>

remote-network <*ipAddr*> **mask** <*maskIp*> **enable**

no remote-network <*ipAddr*> **mask** <*maskIp*> **enable**

Parameters

no	Disable or delete remote network. **No** <remote-network> deletes an existing remote-network. **No** <remote-network> **Enable** disables a remote-network.
mask	Keyword for indicating mask to specify a network.
cost	Keyword for indicating cost of a network.
Gateway	Keyword for indicating a gateway of a network. For LANs only, the valid options for cost are 1 to 200
ipAddr	The IP address for the network.
maskIp	The IP address for the mask of a network.
cost	The cost for the network (1 through 10000).
enable	Enable a network.

Default

None

Command mode

Demand Configuration

Next command mode

Demand Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

```
show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger
wait
no dial
remote-network
```

Example

```
CES(config-demand)# remote-network 11.11.11.11 mask
255.255.0.0 cost 12
```

route-unreachable

Use this command to configure a Demand profile to activate the demand interface when a specific route times out in the routing table. This type of trigger requires that your IP network use RIP or OSPF with redundant routes between end points. If the connection is completely lost, the route times out in the routing table and triggers Demand.



Note: To configure a route, execute the **`network`** command in Global Configuration mode, or go to the Profiles > Networks screen.

Syntax

`route-unreachable` <*`route-name`*>

Parameters

route-name	Specifies the name of the network. If this network becomes unreachable, the Demand profile triggers the demand interface.

Default

None

Command mode

Demand Configuration

Next command mode

Demand Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger
wait
no dial
remote-network
```

Example

```
CES(config-demand)# route-unreachable Network1
```

show demand

Use this command to display the list of configured demand interfaces or the configuration of a specified interface.

Syntax

show demand <*name*>

Parameters

`name`	Specifies a selection of a demand interface

Default

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

demand
demand add
demand <demandinterface> **enable**
demand delay
exit

Example

```
CES(config)# show demand <name>
CES(config)# no show demand <name>
```

timeout

Use this to configures the time (seconds) to wait until traffic trigger on a demand interfaces.

Syntax

timeout <*number*>

Parameters

1 to 86400 seconds

Default

None

Command mode

Demand Configuration

Next command mode

Demand Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

```
show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger traffic
wait
no dial
remote-network
```

Example

```
CES(config-demand)# timeout 24
```

trigger

Use this command to specify the trigger mode for the demand profile that you are configuring. The trigger can be either event-based (for example, the failure of an interface group) or time-based (hours of operation). Use the **no** form of the command to reset the trigger mode to its default, that is, interface group.

Syntax

trigger {**traffic** | **hours** | **interface-group** | **ping** | **route-unreachable**}

no trigger traffic

Parameters

traffic	Specifies this demand interface will be activated by traffic
hours	Specifies that a specific time of day will trigger the activation of the interface.
interface-group	Specifies that the failure of an interface group will trigger the activation of the interface.
ping	Specifies that the failure of a ping to a specific destination will trigger the activation of the interface.
route-unreachable	Specifies that the timing out of a specific route in the route table will trigger the activation of the interface.

Default

None

Command mode

Demand Configuration

Next command mode

Demand Configuration

Related commands

show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger traffic
wait
no dial
remote-network

Example

```
CES(config-demand)# trigger traffic
```

wait

Use this command to set the number of seconds between redial attempts for the demand interface. When this interval expires, the connection is declared unreachable.

Syntax

wait <*seconds*>

Parameters

60 to 255

Default

60

Command mode

Demand Configuration

Next command mode

Demand Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show
dial
hours name
interface
interface-group
ping
priority
redial
route-unreachable
timeout
trigger traffic
wait
no dial
remote-network

Example

```
CES(config-demand)# wait 33
```

Chapter 33
Router RIP configuration commands

This chapter describes the router RIP configuration commands.

Command	Page
distribute-list	1567
network	1570
redistribute	1571
router rip	1573
show ip rip	1574
show ip rip database	1575
show ip rip interface	1576
show ip rip redistribution	1578
timers basic	1579
RIP configuration example	1580

distribute-list

Use this command to configure a RIP policy for incoming or outgoing routes and to enable or disable the policy. Use the **no** form of this command to delete the policy.

Syntax

```
distribute-list <access-list> {in | out} {<ip-address> |
bo-conn <tunnel_name> <group_name>} [enable | disable]
no distribute-list <access-list> {in | out} {<ip-address> |
bo-conn <tunnel_name> <group_name>}
```

Parameters

access-list	Specifies the name of the access list to use for this policy.
ip-address	Specifies the IP address of the interface that the policy applies to. This IP address can be a physical interface or a virtual (tunnel) interface. To apply the policy to a tunnel, specify the IP address of the tunnel end point. If you enter the IP address 0.0.0.0, the policy applies to all interfaces.
tunnel-name	Specifies the name of the asynchronous branch office tunnel (ABOT) that the policy applies to.
group-name	Specifies the group name for the asynchronous branch office tunnel (ABOT) that the policy applies to.
enable **disable**	Specifies whether the policy is enabled or disabled. By default, a policy is enabled when you create it.

Default

None

Command mode

Router RIP Configuration

Next command mode

Router RIP Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Specifying an access list name, which was never created.

% Applying a distribute-list <name1> in on an interface,
which already has a distribute-list <name2> in specified,
will over-ride the existing one.

% Applying a distribute-list <name1> out on an interface,
which already has a distribute-list <name2> out specified,
will over-ride the existing one.
```

Related commands

access-list

Example

The following example creates an accept policy for incoming packets on interface 10.254.52.1.

```
CES(config)# router rip
CES(config-rip)# distribute-list deny_10.254.1.x_network in
10.254.52.1
CES(config-rip)#
```

The following example creates an announce policy for packets exiting asynchronous branch office tunnel “local101” for group /Base/Chicago.

```
CES(config)# router rip
CES(config-rip)# distribute-list drop_ftp out local101
/Base/Chicago
CES(config-rip)#
```

The following example disables an announce policy for asynchronous branch office tunnel “local101” for group /Base/Chicago.

```
CES(config)# router rip
CES(config-rip)# distribute-list drop_ftp out local101
/Base/Chicago disable
CES(config-rip)#
```

The following example removes an accept policy from interface 10.254.52.3.

```
CES(config-rip)# no distribute-list deny_10.254.1.x in
10.254.52.3
CES(config-rip)#
```

network

This command configures RIP on an interface; the **no** form deletes RIP from the interface. This command is specific to the Nortel VPN Router.

Syntax

network *<address> <mask>*
no network *<address> <mask>*

Parameters

address	Address of interface on which to configure RIP routing.
mask	Mask associated with the interface.

Default

Enabled

Command mode

Router RIP Configuration

Next command mode

Router RIP Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This command should be specified in the context of the RIP routing process. Also, the IP interface should have been created prior to enabling RIP on that interface.

Warning messages

```
% The interface does not exist.
```

Example

In the following example, the IP address and the mask should match the IP address of the interface.

```
CES(config-rip)# network 10.11.0.12 255.255.0.0
CES(config-rip)# no network 10.11.0.12 255.255.0.0
```

redistribute

Use this command to redistribute routes from one routing domain into another routing domain. Use the **no** form of the command to disable redistribution. Also, a new protocol type called generic-client is added for redistributing the non-local client routes.

Syntax

```
redistribute {bgp | clip | direct | hosts | ospf | static |
utunnel| mgmt| nat}
no redistribute {bgp | clip | direct | hosts | ospf | static
| utunnel| mgmt| nat}
```

Parameters

bgp	Distribute routes authored by BGP
clip	Distribute clip routes
direct	Distribute direct routes
hosts	Distribute routes from directly connected hosts.
ospf	Distribute routes authored by OSPF
static	Distribute static routes.
utunnel	Distribute routes from non-local clients.
mgmt	Distribute management virtual address routes
nat	Distribute nat routes

Default

Redistribution of direct and static is enabled for RIP. No redistribution is enabled for OSPF.

Command mode

Router RIP Configuration

Next command mode

Router RIP Configuration

Required privileges

System Management – Manage
User Management – None

Example

The following example configures the gateway to redistribute BGP and NAT routes into the RIP domain.

```
CES(config)# router rip
CES(config-rip)# redistribute bgp
CES(config-rip)# redistribute nat
```

router rip

This command globally enables or disables the RIP routing process. All global configuration commands are entered from the terminal.

Syntax

```
router rip
no router rip
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Router RIP Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config)# router rip
CES(config)# no router rip
```

show ip rip

This command displays general information about RIP routing, the state of the RIP routing process and status.

Syntax

```
show ip rip
```

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Related commands

show ip rip interface
show ip rip database

Example

This example shows the state of RIP and the associated status information.

```
CES> show ip rip
Global Rip Status: Enabled
Trusted Neighbor: Disabled, Rip Domain: 0
Triggered Update: Off, RouteChange: 0x0, Query: 0x0
Local [Net: 0x00000000, Mask: 0x00000000, ClassMask:
0x00000000]
LocalCircuit: 1

Node Wide Stats:
rn_rtid: 0x00000000
rn_tics: 0, rn_num_circ: 0, rn_routes: 0
rn_udpInDatagrams: 0, rn_udpOutDatagrams: 1
rn_udpInErrors: 0, rn_udpNoPorts: 0
```

show ip rip database

Use this command to display information about the RIP database on the gateway, that is, routes owned and imported by RIP.

Syntax

show ip rip database

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Related commands

show ip rip
show ip rip interface

Example

This example shows routes in the RIP database.

```
CES> show ip rip database
Circuit Address     Mask            Owner Cost Metric Gw
================================================================
1       192.32.0.0  255.255.0.0      RIP    5    5  10.0.234.230
1       192.168.0.0 255.255.0.0      RIP    5    5  10.0.234.230
1       9.1.10.18   255.255.255.255  RIP    3    3  10.0.234.191
```

show ip rip interface

This command displays information about RIP interfaces that are configured for RIP routing.

Syntax

show ip rip interface

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Related commands

show ip rip
show ip rip database

Example

This example shows the state of the configured interface.

```
CES> show ip rip interface
Cid[1] Enabled, State: UP, Auth: None,Type: ETH
Cid[1] Ip: 10.0.4.41,Subnet: 255.255.0.0
Cid[1] Talk: ON, Listen: ON, RxMode: V2, TxMode: V2,
PoisonRev: Enabled
Cid[1] ImpDRoute: Dis, ExpTSMetric: 1 ExpSMetric: 0,
ExpDMetric: 0
Cid[1] RxUpdates: 5, TxUpdates 20, TxTrigUpd 2, RxBadPkts:
0, RxBadRoutes: 0
```

show ip rip redistribution

This command displays the routing protocols that are redistributed into RIP.

Syntax

```
show ip rip redistribution
```

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management – Manage
User Management – None

Example

The following example shows that static routes, routes from directly connected networks, and OSPF routes are redistributed into RIP.

```
CES> show ip rip redistribution
Redistribution Table for Rip:
Static: Enabled  Direct Nets: Enabled
Direct Hosts: Disabled  Ospf: Enabled   UTunnel: Enabled
```

timers basic

This command adjusts RIP routing protocol update timers. The no form restores it to the default timer values.



Caution: The RIP timers on all devices in the network must be set to the same values.

Syntax

timers basic *<update>*
no timers basic

Parameters

update	Sets timer in seconds. The **no** form resets it to 30 seconds.

Default

30 seconds

Command mode

Router RIP Configuration

Next command mode

Router RIP Configuration

Required privileges

System Management – Manage
User Management – None

Example

The following example sets the timers to 40 seconds and then resets them to the default value, 30 seconds.

```
CES(config-rip)# timers basic 40
CES(config-rip)# no timers basic
```

RIP configuration example

The following example shows how to configure RIP as follows:

- Enable RIP globally on the gateway.
- Configure RIP to redistribute direct routes.
- Configure interface 0/0 as a fast Ethernet interface.
- Enable RIP on interface 0/0.

```
CES# configure terminal
Enter configuration commands, one per line. End with Ctrl-z.
CES(config)# router rip
CES(config-rip)# network 10.1.1.1 255.255.0.0
CES(config-rip)# redistribute connected
CES(config-rip)# exit
CES(config)# interface fastethernet 0/0
CES(config-if)# ip rip
CES(config-if)# exit
```

Chapter 34
Router VRRP configuration commands

This chapter describes the VRRP configuration commands.

Command	Page
activate	1581
critical-interface-group	1584
interface group	1586
network	1588
respond-icmp	1589
router vrrp	1590
show critical-interface	1591
show interface groups	1592
show ip vrrp	1594

activate

This command creates and configures VRRP on an interface to run as a virtual router.

Syntax

```
activate <ip_address> vrid <vrid> [advertise <interval>]
[authentication {none | simple <text>}] [master-delay {none
| delay <delay> | time-of-day <delay_time>}][preempt-mode]

no activate <ip_address>
```

Parameters

ip_address	Interface address to be configured as a virtual router.
vrid	Virtual router ID. The range is 1-254.
interval	Advertisement interval in seconds (optional).
text	Authentication text if authentication mode is configured as simple**.**
delay	Delay delta time in *hh:mm:sec* format if the master delay mode is configured as delay.
delay_time	The delay time in *hh:mm:ss* format if the master delay mode is configured as time-of-day.
preempt-mode	Activate or disable the preempt-mode. The Preempt-mode allows a higher priority backup router to preempt a lower priority master router, even if the higher priority router is not the address owner.

Default

The default values for the parameters are as follows:

Advertisement interval: 1 second
Authentication mode: none
Master delay mode: none

Command mode

Router VRRP Configuration

Next command mode

Router VRRP Configuration

Example

The command syntax applies differently when you first create the VRRP interface and when you change the configuration after the initial configuration. The following examples illustrate all possible commands for creating VRRP on the interface as a virtual router.

This command creates VRRP on interface 10.254.1.42 with a virtual router ID of 1. All other configuration parameters take their default values.

```
CES(config-vrrp)# activate 10.254.1.42 vrid 1
```

This command creates VRRP on interface 11.254.1.43 with a virtual router ID of 1 and an advertise interval of 5 seconds. All other configuration parameters take their default values.

```
CES(config-vrrp)# activate 11.254.1.43 vrid 1 advertise 5
```

This command creates VRRP on interface 12.254.1.43 with a virtual router ID of 1, an advertise interval of 5 seconds, and a text authentication type with the string *abcd*.

```
CES(config-vrrp)# activate 12.254.1.43 vrid 1 advertise 5
authentication simple abcd
```

This command creates VRRP on interface 13.254.1.43 with a virtual router ID of 1, an advertise interval of 5 seconds, a simple authentication type with the text string, and a delay mode for master delay with a delay delta time of 5 seconds.

```
CES(config-vrrp)# activate 13.254.1.43 vrid 1 advertise 5
authentication simple abcd master-delay delay 00:00:04
```

The following examples illustrate all possible commands for configuring the virtual router after you create it.

This command changes the VRID to 2, assuming it has been already created. Otherwise, it creates VRRP with a VRID of 2 on interface 10.254.1.42.

```
CES(config-vrrp)# activate 10.254.1.42 vrid 2
```

This command changes the advertisement interval to 10 seconds and the VRID to 1, assuming it has already been created. Otherwise it creates VRRP with a VRID of 1 on interface 11.254.1.43 with an advertisement interval of 10 seconds.

```
CES(config-vrrp)# activate 11.254.1.43 vrid 1 advertise 10
```

This command changes the authentication type to none and the VRID to 1, assuming it has already been created.

```
CES(config-vrrp)# activate 11.254.1.43 vrid 1 authentication
none
```

This command changes the master delay to time-of-day mode with a delta delay time of 35 seconds and a delay time of 12 hours, assuming it has already been created.

```
CES(config-vrrp)# activate 11.254.1.43 vrid 1 master-delay
time-of-day 00:00:35 12:00:00
```

critical-interface-group

This command creates a new critical interface group and enables or disables a configured critical interface group. You can configure from one through three critical interface groups. Use the **no** form of the command to delete a group.



Note: Before you can create a critical interface group, you must execute the **ip vrrp master** command to designate one interface as the master.

Syntax

```
critical-interface-group <master_ip_address> {1 | 2 | 3}
<group_name> {enabled | disabled}
critical-interface-group <master_ip_address> {1 | 2 | 3}
{enabled | disabled}
no critical-interface-group <master_ip_address> {1 | 2 | 3}
```

Parameters

master_ip_address	Configured VRRP master interface.
group_name	Name of the interface group to be associated with the master interface.

Default

The default name for all critical interface groups is “None.”

Command mode

Router VRRP Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Address <xxx> is not configured
% Group <xxx> does not exist
% Group <xxx> already exists
% No Interface Group assigned yet
```

Related commands

show critical-interface-group

Example

The following example configures and enables critical interface group 1 for VRRP master interface 192.33.2.3 and names the group “Jamaica.”

```
CES(config)# router vrrp
CES(config-vrrp)# critical-interface-group 192.33.2.3
1 Jamaica enabled
```

The following example disables a configured interface group.

```
CES(config-vrrp)# critical-interface-group 192.33.2.3 1
disabled
```

The following example deletes critical interface group 1.

```
CES(config-vrrp)# no critical-interface-group 192.33.2.3 1
```

interface group

Use this command to create an interface group and associate interfaces with the group. You also use this command to enable or disable any interface in the group or the group as a whole. You can create multiple groups on a gateway, and each interface can be associated with more than one group.

Use the **no** form of the command to delete one or more interfaces from the group or to delete the entire group.

Syntax

interface group <*group_name*> [**ip** <*IP_address*> | **enabled** | **disabled**]

no interface group <*group_name*> [**ip** <*IP_address*>]

Parameters

group <*group_name*>	Name of an existing interface group to modify or delete or the name of the new interface group to create. The name is case sensitive.
ip <*IP_address*>	IP address to add to the interface group or to delete from the interface group.

Default

None

Command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Cannot add IP address: Interface <xxx> does not exist
% Interface group <xxx> does not exist
% Interface group <xxx> already exists
```

Related commands

critical interface-group
show interface groups

Example

The following commands create a new interface group called “Jamaica,” add an IP address to the group, enable the group, and then disable it.

```
CES(config)# interface group jamaica
CES(config)# interface group jamaica ip 10.0.15.201
CES(config)# interface group jamaica enabled
CES(config)# interface group jamaica disabled
```

The following commands delete an IP interface from the interface group Jamaica and then delete the group itself.

```
CES(config)# no interface group jamaica ip 10.0.15.201
CES(config)# no interface group jamaica
```

network

This command creates VRRP on the network interface specified. The **no** version of this command deletes VRRP from the network interface. The Nortel VPN Router CLI uses the **network** command to create the protocol interface. After you create the protocol interface, you must enable the protocol on this interface in Interface Configuration mode.

Syntax

network <*ip_address*>
no network <*ip_address*>

Parameters

ip_address	The private network interface on which to enable VRRP.

Default

None

Command mode

Router VRRP Configuration

Next command mode

Router VRRP Configuration

Example

```
CES(config)# router vrrp
CES(router-vrrp)# network 10.0.3.191
CES(router-vrrp)# no network 10.0.3.191
```

respond-icmp

This command enables VRRP to respond to icmp packets whenever VRRP becomes master for an IP address that it backs up.

Syntax

```
respond-icmp enable
no respond-icmp enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Router VRRP Configuration

Required privileges

System Management – Manage
User Management – None

Example

This example enables the respond-icmp for VRRP.

```
CES(config)# router vrrp
CES(config-vrrp)# respond-icmp enable
CES(config)# no respond-icmp enable
```

router vrrp

This command configures VRRP globally and navigates to Router VRRP Configuration mode. In this command mode, you can configure all global router configuration commands specific to VRRP. The **no** version of this command disables VRRP on the router.

Syntax

```
router vrrp
no router vrrp
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Router VRRP Configuration

Required privileges

System Management – Manage
User Management – None

Example

```
CES(config)# router vrrp
CES(config-vrrp)# exit
CES(config)# no router vrrp
```

show critical-interface

This command displays the critical interface group administrative and operational states and the interface group name for each master virtual router configured on the gateway.

Syntax

```
show critical-interface
```

Parameters

None

Default

None

Command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

critical-interface-group

Example

```
CES> show critical-interface
Critical interface: 192.33.5.6
 Operational State: MASTER    VRID: 1
 Group 1: Jamaica Op State: UP   Admin State: ENABLED
 Group 2: Rialto  Op State: UP   Admin State: ENABLED
 Group 3: (None)  Op State: UP   Admin State: DISABLED
CES>
```

show interface groups

This command displays information about the interface groups configured on the gateway.

Syntax

show interface groups [**ip** | *<group_name>*]

Parameters

ip	Display a list of IP addresses that can be included in interface groups.
group_name	Display the interfaces in the specified interface group.

Default

None

Command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

interface group
show critical-interface

Example

```
CES> show interface groups
Current Interface groups:
  Jamaica
  Rialto
CES> show interface groups Jamaica
Current Interfaces in the Group:
  47.17.248.50
  192.33.5.6
  192.33.5.12
CES> show interface groups ip
Available Interfaces:
  47.17.248.50
  192.33.5.6
  10.0.16.48 (Chester_1)
CES>
```

show ip vrrp

This command displays information about VRRP status.

Syntax

show ip vrrp [**interface**]

Parameters

interface	Display detailed information about VRRP on each interface where it is configured.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Example

This example displays the interfaces configured for VRRP and the more detailed output available with the optional **`interface`** parameter.

```
CES> show ip vrrp
Slot Intf VRID Prio State  Address
  0    1    1    255  Master 10.0.20.186
  1    1    2    100  Backup 10.0.21.186
CES> show ip vrrp interface
  Slot 0 Interface 1
    Virtual router 1
      Current state is Master, priority 255, may not preempt
      Advertisement interval 1
      IP Address 10.0.20.186
      Became master 1 times, sent 0 Zero prio pkts, recv'd 0
      Sent 436 advertisements, recv'd 0
      No errors
    Virtual router 2
      Current state is Backup, priority 100, may not preempt
      Advertisement interval 1
      IP Address 10.0.21.186
      Became master 1 times, sent 0 Zero prio pkts, recv'd 0
      Sent 7 advertisements, recv'd 426
      No errors
```

show run routing vrrp

This command displays information about VRRP priority.

Syntax

```
show run routing vrrp
```

Parameters

None

Default

None

Command mode

Router VRRP Configuration

Next command mode

Router VRRP Configuration

Example

This example displays the priorities configured for VRRP.

```
CES#show run routing vrrp
! Routing VRRP Configuration
router vrrp
network 10.250.5.228
exit
! Interface Configuration
interface FastEthernet 4/1
! RIP Interface Configuration
ip rip
ip rip send version 2
ip rip receive version 2
no ip rip authentication mode
ip rip cost 1
ip rip poison-reverse
no ip rip import-default
no ip rip export-default-metric
ip rip export-static-metric 1
no ip rip export-ospf-metric
ip rip export-bo-static-metric 1
! Vrrp Interface Configuration
ip vrrp
no ip vrrp master
exit
interface FastEthernet 0/1
! RIP Interface Configuration
ip rip
ip rip send version 2
ip rip receive version 2
no ip rip authentication mode
ip rip cost 1
ip rip poison-reverse
no ip rip import-default
no ip rip export-default-metric
ip rip export-static-metric 1
no ip rip export-ospf-metric
ip rip export-bo-static-metric 1
! Vrrp Interface Configuration
exit
! Interface Group Configuration
```

```
! Routing VRRP Configuration
router vrrp
activate 10.250.5.229 vrid 2 advertise 1
activate 10.250.5.229 vrid 2 authentication none
activate 10.250.5.229 vrid 2 master-delay none
exit
CES#
```

Chapter 35
Router OSPF configuration commands

This chapter describes the router OSPF configuration commands.

Command	Page
area	1600
asbr	1602
auto-vlink	1604
compat-3-6	1605
distribute-list	1607
external-metric	1609
network	1610
redistribute	1612
router-id	1613
router ospf	1615
show ip ospf	1616
show ip ospf border-routers	1618
show ip ospf database	1619
show ip ospf interface	1620
show ip ospf neighbor	1621
show ip ospf virtual-links	1623

area

Use this command to create OSPF areas, including stub areas. You can also use this command to specify the cost of the default summary route used for the stub area and to configure summary advertisements for border routers. The **no** form of the command deletes an area, changes a stub area to a non-stub area, or removes the default cost or configured range.

Syntax

```
area <area-id> [[stub] | [default-cost <cost>] |
[range <ip-address> <mask>]]
no area <area-id> [[stub] | [default-cost] |
[range <ip-address> <mask>]]
```

Parameters

area-id	Specifies the OSPF area ID in the form of an IP address.
stub	Defines an area to be a stub area.
default-cost	Specifies the cost for the default summary route generated by ABR into the stub or NSSA area. The default cost is 1. You can specify a cost from 1 through 255.
range	If this gateway is a border router, specifies that routes in the address range that you enter should be summarized in advertisements.

Default

Summary route is used for the stub area.

Command mode

Router OSPF Configuration

Next command mode

Router OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

You can only execute the **`area stub`** and **`area default-cost`** commands if the area specified by *`area-id`* already exists. Also, you cannot use these commands on the backbone area 0.0.0.0

Warning messages

When an area is deleted using the **`no`** form of the command, a warning appears if any physical interfaces or tunnels already exist in the area.

```
% Move interface <interface-id> to a different area before
deleting <area-id>.
```

```
% Tunnel <tunnel name> exists on <area_id>. Move tunnel to a
different area first.
```

A warning is displayed if an attempt is made to delete an area range that does not exist.

```
% Range: Addr <net_id> Mask <net_mask> doesn't exist within
area <areaid>
```

Example

The following example creates the area 11.254.1.20:

```
CES(config-ospf)# area 11.254.1.20
```

The following example creates the summary route 140.191.0.0 with a mask of 255.255.0.0:

```
CES(config-ospf)# area 11.254.1.20 range 140.191.0.0
255.255.0.0
```

The following example deletes the summary route 140.191.0.0 with a mask of 255.255.0.0:

```
CES(config-ospf)# no area 11.254.1.20 range 140.191.0.0
255.0.0.0
```

The following example configures the area 11.254.1.20 to be a stub area:

```
CES(config-ospf)# area 11.254.1.20 stub
```

The following example sets the default cost in area 11.254.1.20 to 40:

```
CES(config-ospf)# area 11.254.1.20 default-cost 40
```

The following example sets the default cost in area 11.254.1.20 to the default, 10:

```
CES(config-ospf)# no area 11.254.1.20 default-cost
```

This example configures the area 11.254.1.20 to be a non-stub area:

```
CES(config-ospf)# no area 11.254.1.20 stub
```

The following example deletes area 11.254.1.20:

```
CES(config-ospf)# no area 11.254.1.20
```

asbr

This command enables the gateway as an autonomous system boundary router. This command is specific to the Nortel VPN Router. This should be specified in the context of the OSPF routing process.

Syntax

```
asbr
no asbr
```

Parameters

None

Default

False

Command mode

Router OSPF Configuration

Next command mode

Router OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Example

The following example configures this router as an ASBR:

```
CES(config-ospf)# asbr
```

The following example removes ASBR from this router:

```
CES(config-ospf)# no asbr
```

auto-vlink

Use this command to enable the automatic creation of virtual links for OSPF area border routers. The **no** form of the command disables the automatic creation of virtual links.

Syntax

```
auto-vlink
no auto-vlink
```

Parameters

None

Default

Not enabled

Command mode

Router OSPF Configuration

Next command mode

Router OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

compat-3-6

Example

The following example enables automatic virtual links.

```
CES(config-ospf)# auto-vlink
```

The following example disables automatic virtual links.

```
CES(config-ospf)# no auto-vlink
```

compat-3-6

Nortel VPN Router software versions earlier than Version 4.0 do not support OSPF virtual links. If your network has Nortel VPN Routers running Version 4.0 or later *and* gateways running software earlier than Version 4.0, use this command to avoid compatibility issues that may arise with automatic virtual links over tunnels.

- If all Nortel VPN Router in the network are running Version 4.0 or later software, disable the **compat-3-6** option on all the gateways (the default setting is disabled).
- If one or more Nortel VPN Router in the network are running software earlier than Version 4.0, enable the **compat-3-6** option on all the gateways.

When you enable the **compat-3-6** option, virtual links cannot be formed even by gateways running Version 4.0 or later. Use the **no** form of the command to disable this flag.

Syntax

```
compat-3-6 enable
no compat-3-6 enable
```

Parameters

None

Default

Disabled

Command mode

Router OSPF Configuration

Next command mode

Router OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

auto-vlink

Example

The following example enables the **compat-3-6** option.

```
CES(config-ospf)# compat-3-6 enable
```

The following example disables the **compat-3-6** option.

```
CES(config-ospf)# no compat-3-6 enable
```

distribute-list

Use this command to configure an OSPF policy for incoming or outgoing routes and to enable or disable the policy. Use the **no** form of this command to delete the policy.

Syntax

```
distribute-list <access-list> {in | out} {<ip-address> |
bo-conn <tunnel_name> <group_name>} [enable | disable]
no distribute-list <access-list> {in | out} {<ip-address> |
bo-conn <tunnel_name> <group_name>}
```

Parameters

access-list	Specifies the name of the access list to use for this policy.
ip-address	Specifies the IP address of the interface that the policy applies to. This IP address can be a physical interface or a virtual (tunnel) interface. To apply the policy to a tunnel, specify the IP address of the tunnel end point. If you enter the IP address 0.0.0.0, the policy applies to all interfaces.
tunnel-name	Specifies the name of the asynchronous branch office tunnel (ABOT) that the policy applies to.
group-name	Specifies the group name for the asynchronous branch office tunnel (ABOT) that the policy applies to.
enable **disable**	Specifies whether the policy is enabled or disabled. By default, a policy is enabled when you create it.

Default

None

Command mode

Router OSPF Configuration

Next command mode

Router OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Specifying an access list name, which was never created.

% Applying a distribute-list <name1> in on an interface,
which already has a distribute-list <name2> in specified,
will over-ride the existing one.

% Applying a distribute-list <name1> out on an interface,
which already has a distribute-list <name2> out specified,
will over-ride the existing one.
```

Related commands

access-list

Example

The following example creates an accept policy for incoming packets on interface 10.254.52.1.

```
CES(config)# router ospf
CES(config-ospf)# distribute-list deny_10.254.1.x_network in
10.254.52.1
CES(config-ospf)#
```

The following example creates an announce policy for packets exiting asynchronous branch office tunnel “local101” for group /Base/Chicago.

```
CES(config)# router ospf
CES(config-ospf)# distribute-list drop_ftp out local101
/Base/Chicago
CES(config-ospf)#
```

The following example disables an announce policy for asynchronous branch office tunnel “local101” for group /Base/Chicago.

```
CES(config)# router ospf
CES(config-ospf)# distribute-list drop_ftp out local101
/Base/Chicago disable
CES(config-ospf)#
```

The following example removes an accept policy from interface 10.254.52.3.

```
CES(config-ospf)# no distribute-list deny_10.254.1.x in
10.254.52.3
CES(config-ospf)#
```

external-metric

This command sets the external metric type to type 1 or type 2.

Syntax

external-metric type <*value*>

Parameters

type	Metric type.
value	Value of the external metric type. Enter 1 or 2.

Command mode

Router OSPF Configuration

Next command mode

Router OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Example

This example sets the external metric type to type 2.

```
CES(config-ospf)# external-metric-type 2
```

network

This command configures OSPF on interfaces and assigns an area ID to it. The **no** form deletes OSPF from the interfaces. The *area-id* is valid only in the context of OSPF. The creation and deletion of OSPF is specific to the Nortel VPN Router. If the area does not already exist, it is created. This command works only for private interfaces. This should be specified in the context of the OSPF routing process.

Syntax

```
network <address> <wildcardmask> area <area-id>
no network <address> <wildcardmask>
```

Parameters

address	IP address of the physical interface on which to enable routing.
wildcardmask	Wildcard mask (inverse mask format).
area-id	IP address for the area ID.

Default

None

Command mode

Router OSPF Configuration

Next command mode

Router OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

An interface can belong to only one area. If the area specified by *area-id* does not exist, then one is created automatically. A warning displays if the creation fails.

```
% OSPF interface creation failure.
```

Related commands

The **`ip ospf`** command enables IP on an interface. The interface is enabled by default on creation.

Example

This example specifies that all physical interfaces falling within the above wildcard mask are put in area 1.254.1.20 and enabled.

```
CES(config-ospf)# network 10.11.0.12 0.0.0.255 area
1.254.1.20
```

This example specifies that all physical interfaces falling within the above wildcard mask are deleted.

```
CES(config-ospf)# no network 10.11.0.12 0.0.0.255 area
1.254.1.20
```

redistribute

This command redistributes routes from one routing domain into another routing domain. The **no** form disables redistribution. This deviates from the Nortel VPN Router UI management representation of direct instead of connected**.** Also, a new protocol type called generic-client is added for redistributing the non-local client routes. This should be specified in the context of the RIP or OSPF routing process.

Syntax

```
redistribute { clip | direct | hosts | mgmt| nat | bgp|rip |
static | utunnel}
no redistribute { clip | direct | hosts | mgmt| nat | bgp|rip
| static | utunnel}
```

Parameters

clip	Distribute clip routes
direct	Distribute direct routes
hosts	Distribute routes from directly connected hosts.
mgmt	Distribute management virtual address routes
nat	Distribute nat routes

bgp	Distribute routes authored by BGP
rip	Distribute routes authored byRIP
static	Distribute static routes.
utunnel	Distribute routes from non-local clients.

Default

Redistribution of static is enabled for RIP. No redistribution is enabled for OSPF.

Command mode

Router OSPF Configuration

Next command mode

Router OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Example

These examples show that BGP and NAT routes are to be redistributed into RIP domain.

```
CES(config-rip)# redistribute bgp
CES(config-rip)# redistribute nat
```

router-id

Use this command to change the OSPF router ID. This command is specific to the Nortel VPN Router.

Syntax

router-id <*value*>

Parameters

value	Router ID as an IP address.

Default

Lowest of all the IP addresses configured in the CES.

Command mode

Router OSPF Configuration

Next command mode

Router OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This should be specified in the context of the OSPF routing process.

Warning messages

A warning is displayed if there is an error in setting the router ID:

```
% Error setting router ID.
```

Example

This example changes the router ID to 1.1.1.1.

```
CES(config-ospf)# router-id 1.1.1.1
```

router ospf

This command globally enables or disables the OSPF routing process. All global configuration commands are entered from the terminal. This differs from the NNCLI standard, which specifies the process ID when it is enabled.

Syntax

```
router ospf
no router ospf
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Router OSPF Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

A warning is displayed if the enabling is not successful.

```
% This feature is not enabled. Contact your sales
representative to purchase this key. The key can then be
entered on the ADMIN->INSTALL KEYS page.
```

Example

This example enables OSPF.

```
CES(config)# router ospf
```

This example disables OSPF.

```
CES(config)# no router ospf
```

show ip ospf

This command displays general information about the OSPF routing process.

Syntax

```
show ip ospf
```

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Example

```
CES> show ip ospf

Routing Process "ospf 201" with ID 192.42.110.200
Supports only single TOS (TOS0) route.
It is an area border and autonomous system boundary router.
Redistributing External Routes from,igrp 200 with metric
mapped to 2, includes subnets in redistribution rip with
metric mapped to 2.
igrp 2 with metric mapped to 100
igrp 32 with metric mapped to 1
Number of areas in this router is 3
Area 192.42.110.0
Number of interfaces in this area is 1
Area has simple password authentication
SPF algorithm executed 6 times
```

show ip ospf border-routers

This command displays the internal OSPF routing table entries to area border routers (ABRs) and autonomous system boundary routers (ASBRs).

Syntax

```
show ip ospf border-routers
```

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management – View
User Management – None

Example

```
CES> show ip ospf border-routers
OSPF Internal Routing Table

Destination        Next Hop        Cost   Type     Rte Type   Area SPF
No

160.89.97.53     144.144.1.53    10     ABR      INTRA    0.0.0.3        3
160.89.103.51    160.89.96.51    10     ABR      INTRA    0.0.0.3        3
160.89.103.52    160.89.96.51    20     ASBR     INTER    0.0.0.3        3
160.89.103.52    144.144.1.53    22     ASBR     INTER    0.0.0.3        3
```

show ip ospf database

This command displays lists of information related to the OSPF database.

Syntax

show ip ospf [<*area-id*>] **database**
show ip ospf [<*area-id*>] **database router** [<*link-state-id*>]
show ip ospf [<*area-id*>] **database network** [<*link-state-id*]>
show ip ospf [<*area-id*>] **database summary**
show ip ospf [<*area-id*>] **database asb-summary**
[<*link-state-id*>]
show ip ospf [<*area-id*>] **database database-summary**
show ip ospf database external [<*link-state-id*>]

Parameters

area-id	Specifies an area ID in the form of an IP address.
link-state-id	Specifies a link state ID (optional).

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management – View
User Management – None

Example

```
CES> show ip ospf database
```

show ip ospf interface

This command displays information related to OSPF interfaces.

Syntax

show ip ospf interface {**ethernet** <*value*> | **ptpt** <*value*>}

Parameters

ethernet	Valid values are 0 through 64.
ptpt	Valid values are 65 through 65536.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management – View
User Management – None

Example

```
CES> show ip ospf interface ethernet 0
Ethernet 0 is up, line protocol is up
Internet Address 131.119.254.202, Mask 255.255.255.0, Area 0.0.0.0
AS 201, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State OTHER, Priority 1
Designated Router id 131.119.254.10, Interface address 131.119.254.10
Backup Designated router id 131.119.254.28, Interface addr
131.119.254.28
Timer intervals configured, Hello 10, Dead 60, Wait 40, Retransmit 5
Hello due in 0:00:05
Neighbor Count is 8, Adjacent neighbor count is 2
  Adjacent with neighbor 131.119.254.28 (Backup Designated Router)
  Adjacent with neighbor 131.119.254.10 (Designated Router)
```

show ip ospf neighbor

This command displays OSPF neighbor information on a per-interface basis.

Syntax

show ip ospf neighbor [<*neighbor-id*>] **detail**

Parameters

neighbor-id	IP address of the neighbor.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management – View
User Management – None

Example

```
CES> show ip ospf neighbor
Neighbor 199.199.199.137, interface address 160.89.80.37
    In the area 0.0.0.0 via interface Ethernet0
    Neighbor priority is 1, State is FULL
    Options 2
    Dead timer due in 0:00:32
    Link State retransmission due in 0:00:04
 Neighbor 199.199.199.137, interface address 192.31.48.189
    In the area 0.0.0.0 via interface Fddi0
    Neighbor priority is 5, State is FULL
    Options 2
    Dead timer due in 0:00:32
    Link State retransmission due in 0:00:03
```

show ip ospf virtual-links

This command displays information about the current state of OSPF virtual links.

Syntax

show ip ospf virtual-links

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management – View
User Management – None

Example

This example displays the current state of the OSPF virtual links.

```
CES> show ip ospf virtual-links
```

Chapter 36
IPX configuration commands

This chapter describes the IPX configuration commands.

Command	Page
disable	1625
enable	1626
ipx public-network-address	1628
ipx interface	1630
network	1632

disable

Use this command to disable the private IPX interface.

Syntax

disable

Parameters

None

Default

Enabled

Command mode

IPX Interface Configuration

Next command mode

IPX Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

enable
ipx interface
network

Example

The following example configures an IPX interface on port 1 of the network card in slot 2 and then disables the IPX interface.

```
CES(config)# ipx interface 2/1
CES(config-ipx)# network 4F1A3BC2 encapsulation sap
CES(config-ipx)# disable
CES(config-ipx)# exit
CES(config)#
```

enable

Use this command to enable the private IPX interface.

Syntax

enable

Parameters

None

Default

Enabled

Command mode

IPX Interface Configuration

Next command mode

IPX Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

disable
ipx interface
network

Example

The following example configures an IPX interface on port 1 of the network card in slot 2, disables the IPX interface, and then reenables it.

```
CES(config)# ipx interface 2/1
CES(config-ipx)# network 4F1A3BC2 encapsulation sap
CES(config-ipx)# disable
CES(config-ipx)# enable
```

ipx public-network-address

Use this command to configure an IPX public interface on the gateway. All public interfaces on the gateway are treated as a single IPX network segment and use the same IPX public network address. The gateway assigns this public network address to tunneled clients. To delete IPX from the public interface, use the **no** form of this command.

Syntax

ipx public-network-address <*address*> {**default-nearest-server** <*server*> | **maximum-sap-entries** <*saps*> | **maximum-route-entries** <*routes*>}

no ipx public-network-address <*address*>

Parameters

public-network-address <*address*>	Specifies the IPX public network address that the gateway assigns to tunneled clients. All public interfaces on the gateway are treated as a single network segment and use the same IPX public network address. An IPX public network address is a 4-byte hexadecimal number that must be unique. A sample public network address is 4F1A3BC2. After you configure or change the public network address, you must restart the gateway.
default-nearest-server <*server*>	Specifies the name of the server that you want to be the default nearest server. The default nearest server name can consists of up to 48 ASCII characters. When a remote system establishes an IPX connection with the gateway, the system sends a get nearest server (GNS) packet to the gateway. In response to a GNS request, the gateway returns the name and IPX address of the server specified using this parameter. If that server is not available, the gateway returns the name and IPX address of the server that is topologically closest to the requesting system.

maximum-sap-entries <*saps*>	Specifies the largest number of Service Advertising Protocol (SAP) entries that the gateway handles concurrently. SAP is a Novell protocol that provides a means for servers to advertise their services to routers, gateways, and other servers. You can specify from 10 through 10,000 SAP entries. Each entry requires approximately 100 bytes of memory, so 10,000 entries require approximately 1 MB of memory. Therefore, you should set the maximum number of entries to a value that is slightly greater than the number of servers that you support to allow for future growth.
maximum-route-entries <*routes*>	Specifies the largest number of IPX route entries that the gateway handles concurrently. A route entry is required for each reachable IPX network that is learned through the IPX RIP protocol. You can specify from 10 through 10,000 route entries. Each entry requires approximately 100 bytes of memory, so 10,000 entries require approximately 1 MB of memory. Therefore, you should set the maximum number of entries to a value that is slightly greater than the number of routes that you support to allow for future growth.

Default

The default value for both the maximum number of SAP entries and the maximum number of route entries is 1024.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ipx interface
show running-config system ipx

Example

The following example configures the IPX public interface and changes the default values for the maximum number of SAP entries and the maximum number of IPX routes handled by the gateway.

```
CES(config)# ipx public-network-address 4F1A3BC2
default-nearest-server Boston-server
CES(config)# ipx public-network-address 4F1A3BC2
maximum-sap-entries 512
CES(config)# ipx public-network-address 4F1A3BC2
maximum-route-entries 2048
CES(config)#
```

The following example deletes the IPX public interface from the gateway.

```
CES(config)# no ipx public-network-address 4F1A3BC2
CES(config)#
```

ipx interface

Use this command to configure a private interface as an IPX interface. To disable IPX routing, use the **no** form of this command.



Note: After you configure IPX on an interface, you must also enable IPX for each specific group that will use it.

Syntax

ipx interface {**LAN** | <*slot/port*>}
no ipx interface {**LAN** | <*slot/port*>}

Parameters

interface	Specifies the private interface on which you are enabling IPX. The value “LAN” indicates the Ethernet interface on the system board installed in every Nortel VPN Router. The value *<slot/port>* represents an optional LAN card in the specified expansion slot.

Default

None

Command mode

Global Configuration

Next command mode

IPX Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ipx public-network-address
network

Example

The following example configures an IPX interface on port 1 of the network card in slot 2, configures the IPX network number and the encapsulation type for the interface, and enables IPX for group /Base/test.

```
CES(config)# ipx interface 2/1
CES(config-ipx)# network 4F1A3BC2 encapsulation sap
CES(config-ipx)# exit
CES(config)#
```

The following example disables the IPX interface on port 2/1.

```
CES(config-ipx)# disable
CES(config-ipx)#
```

The following example deletes the IPX interface from port 2/1.

```
CES(config-ipx)# exit
CES(config)# no ipx interface 2/1
CES(config)#
```

network

Use this command to specify the network address and the encapsulation method for this IPX interface. The IPX network address and the encapsulation method (the IPX frame type) must match those of the LAN.

For the network address, enter an eight-digit hexadecimal number that uniquely identifies the network segment. You do not need to specify leading zeros in the network address. For example, for the network number 000000AA you can enter AA. Valid values are from 1 through FFFFFFFD.

Syntax

network <*number*> **encapsulation** {**arpa** | **novell-ether** | **sap** | **snap**}

Parameters

novell-ether	Specifies Novell Ethernet 802.3 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. This encapsulation is the default type used by NetWare Version 3.11.
sap	Specifies Novell Ethernet 802.2 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 LLC header. This encapsulation is the default type used by NetWare Version 4.0.
snap	Specifies Novell Ethernet SNAP (Subnetwork Access Protocol) encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 SNAP LLC header.
arpa	Specifies Novell Ethernet II encapsulation. Recommended for networks that handle both TCP/IP and IPX traffic.

Default

Default encapsulation is Novell Ethernet 802.3 (novell-ether).

Command mode

IPX Interface Configuration

Next command mode

IPX Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

ipx interface
ipx public-network-address

Example

The following example configures an IPX interface on port 1 of the network card in slot 2, configures the IPX network number and the encapsulation type for the interface, and enables IPX for group /Base/test.

```
CES(config)# ipx interface 2/1
CES(config-ipx)# network 4F1A3BC2 encapsulation sap
CES(config-ipx)# exit
CES(config)# group conn "/Base/test"
CES(config-group/con)# ipx
CES(config-group/con)#
```

The following example disables the IPX interface on port 2/1.

```
CES(config-ipx)# disable
CES(config-ipx)#
```

Chapter 37
Routing table configuration commands

This chapter describes the routing table configuration commands.

Command	Page
copy ip ospf-lsdb-table	1635
copy ip route-table	1636
show ip route	1638

copy ip ospf-lsdb-table

Use this command to copy the contents of the OSPF link state database table to a file.

Syntax

copy ip ospf-lsdb-table *<file_name>*

Parameters

file_name	Name of the file where the LSDB will be copied.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management – Manage
User Management – None

Example

The following example copies the contents of the link state database to the file lsdb.dat. The new file is copied to /ide0/system/routing.

```
CES# copy ip ospf-lsdb-table lsdb.dat
CES#
```

copy ip route-table

Use this command to copy the contents of the route table to the specified file.

Syntax

copy ip route-table <*file_name*> [**all**]

Parameters

file_name	Name of the file where the route table contents will be copied.
all	Copy all routes to all destinations in the routing table. The default copies only the best routes for all destinations.

Default

The best routes to all destinations are copied.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management – Manage
User Management – None

Example

The following example copies only the best routes to all destinations to the file rtbl.dat. The location of the file is /ide0/system/routing.

```
CES# copy ip route-table rtbl.dat
CES#
```

The following example copies all routes to all destinations.

```
CES# copy ip route-table rtbl.dat all
CES#
```

show ip route

Use this command to display routes from the routing table.

Syntax

show ip route [<*dest_ip_address*> <*mask*> [**exact**]] [**interface** <*phys_ip_address*>] [**all** | **direct** | **ospf** | **rip** | **static** | **utunnel**]

show ip route [**all** | **clip** | **direct** | **nat** | **ospf** | **rip** | **static** | **utunnel**]

show ip route summary

Parameters

dest_ip_address	Specifies the IP address of a network or host.
mask	Specifies the mask of the network or host address (type 255.255.255.255 for a host).
exact	Display routes to the specific network only.
interface	Display routes that match the specified source interface.
phys_ip_address	Specifies the IP address of the source physical interface.
all	Display all routes in the routing table or all routes that match the search criteria (destination IP address, source gateway interface, or both).
clip, **direct**, **nat**, **ospf**, **rip**, **static**, or **utunnel**	Display routes that were injected into the route table by the specified protocol or service (**utunnel** means “user tunnel client”). If no source is specified, display all routes.
summary	Display summary information about the entries in the routing table.

Default

This command lists the best routes in the routing table.

Command mode

User EXEC

Next command mode

User EXEC

Warning messages

```
% No physical interface is associated with this IP address
```

Example

The following example displays a summary of the routes in the route table.

```
CES> show ip route summary

IP routing table summary
Maximum ECMP Paths = 1
Total routes = 3
Best routes = 3
Static routes = 1
Direct routes = 2
RIP routes = 0
OSPF routes = 0
CLIP routes = 1
NAT routes = 0

CES>
```

The following example displays all routes in the routing table.

```
CES> show ip route
Protocol IP Address      Mask            Cost Next Hop        Interface
-------------------------------------------------------------------------
STATIC   0.0.0.0         0.0.0.0        [10] 47.17.66.177    47.17.66.188
RIP      3.3.0.0         255.255.0.0    [2]  10.123.198.1    10.123.196.1
RIP      5.5.0.0          255.255.0.0     [3]  16.16.0.162     16.16.0.196
RIP      6.6.0.0          255.255.0.0     [3]  16.16.0.162     16.16.0.196
DIRECT    7.7.0.0          255.255.0.0     [0]  7.7.0.196       7.7.0.196
DIRECT    7.7.0.196        255.255.255.255 [0]  127.0.0.1       127.0.0.1
RIP      10.3.0.0         255.255.0.0     [3]  16.16.0.162     16.16.0.196
RIP      10.123.0.0       255.255.240.0   [3]  16.16.0.162     16.16.0.196
RIP      10.123.16.0      255.255.240.0   [4]  16.16.0.162     16.16.0.196
RIP      10.123.21.1      255.255.255.255 [4]  16.16.0.162     16.16.0.196
RIP      10.123.21.10     255.255.255.255 [4]  16.16.0.162     16.16.0.196
RIP      10.123.80.0      255.255.240.0   [4]  16.16.0.162     16.16.0.196
RIP      10.123.160.0     255.255.240.0   [2]  16.16.0.162     16.16.0.196
RIP      10.123.176.0     255.255.240.0   [3]  16.16.0.162     16.16.0.196
DIRECT   10.123.192.0     255.255.240.0   [0]  10.123.196.1    10.123.196.1
DIRECT    10.123.196.1     255.255.255.255 [0]  127.0.0.1       127.0.0.1
DIRECT   16.16.0.0        255.255.255.0   [0]  16.16.0.196     16.16.0.196
DIRECT    16.16.0.196      255.255.255.255 [0]  127.0.0.1       127.0.0.1
RIP      20.123.1.45      255.255.255.255 [4]  16.16.0.162     16.16.0.196
RIP      20.123.2.45      255.255.255.255 [4]  16.16.0.162     16.16.0.196
RIP      20.123.4.45      255.255.255.255 [4]  16.16.0.162     16.16.0.196
Total route(s) 21
CES>
```

The following example displays all routes that have 47.17.248.66 as their source interface.

```
CES> show ip route interface 47.17.248.66
Protocol IP Address      Mask            Cost Next Hop        Interface
-------------------------------------------------------------------------
STATIC   0.0.0.0         0.0.0.0        [10] 47.17.248.1     47.17.248.66
DIRECT    47.17.248.0      255.255.248.0   [0]  47.17.248.66  47.17.248.66
CES>
```

The following example displays all direct routes in the routing table.

```
CES> show ip route direct

Protocol IP Address      Mask            Cost Next Hop        Interface
-------------------------------------------------------------------------
DIRECT   47.17.248.0     255.255.248.0   [0]  47.17.248.52 47.17.248.52
DIRECT   47.17.248.52    255.255.255.255 [0]  127.0.0.1       127.0.0.1
```

The following example displays all RIP routes in the routing table.

```
CES> show ip route rip
Protocol IP Address      Mask            Cost Next Hop        Interface
-------------------------------------------------------------------------
RIP      3.3.0.0         255.255.0.0     [2]  10.123.198.1    10.123.196.1
RIP      5.5.0.0         255.255.0.0     [3]  16.16.0.162     16.16.0.196
RIP      6.6.0.0         255.255.0.0     [3]  16.16.0.162     16.16.0.196
RIP      10.3.0.0        255.255.0.0     [3]  16.16.0.162     16.16.0.196
RIP      10.123.0.0      255.255.240.0   [3]  16.16.0.162     16.16.0.196
RIP      10.123.16.0     255.255.240.0   [4]  16.16.0.162     16.16.0.196
RIP      10.123.21.1     255.255.255.255 [4]  16.16.0.162     16.16.0.196
RIP      10.123.21.10    255.255.255.255 [4]  16.16.0.162     16.16.0.196
RIP      10.123.80.0     255.255.240.0   [4]  16.16.0.162     16.16.0.196
RIP      10.123.160.0    255.255.240.0   [2]  16.16.0.162     16.16.0.196
RIP      10.123.176.0    255.255.240.0   [3]  16.16.0.162     16.16.0.196
RIP      20.123.1.45     255.255.255.255 [4]  16.16.0.162     16.16.0.196
RIP      20.123.2.45     255.255.255.255 [4]  16.16.0.162     16.16.0.196
RIP      20.123.4.45     255.255.255.255 [4]  16.16.0.162     16.16.0.196
Total route(s) 14
CES>
```

The following example displays all circuitless IP routes in the routing table.

```
CES> show ip route clip
Protocol IP Address      Mask            Cost Next Hop        Interface
-------------------------------------------------------------------------
CLIP     192.168.10.0    Directly connected
Total route(s) 1
CES>
```

The following example displays all routes to destination network 10.123.0.0 with a mask of 255.255.240.0.

```
CES> show ip route 10.123.0.0
Protocol IP Address      Mask            Cost Next Hop        Interface
-------------------------------------------------------------------------
RIP      10.123.0.0      255.255.240.0   [3]  16.16.0.162     16.16.0.196
RIP      10.123.16.0     255.255.240.0   [4]  16.16.0.162     16.16.0.196
RIP      10.123.80.0     255.255.240.0   [4]  16.16.0.162     16.16.0.196
RIP      10.123.160.0    255.255.240.0   [2]  16.16.0.162     16.16.0.196
RIP      10.123.176.0    255.255.240.0   [3]  16.16.0.162     16.16.0.196
DIRECT   10.123.192.0    255.255.240.0   [0]  10.123.196.1    10.123.196.1
CES>
```

Chapter 38
CAR configuration commands

This chapter describes client address resolution (CAR) configuration commands.

Command	Page
aggregation	1644
router car	1646
show router car	1647
threshold	1649

aggregation

Use this command to specify whether client address redistribution (CAR) will be enabled on the gateway and if it is enabled, what type of aggregation will be used.

Syntax

aggregation {**dynamic** |**host** | **static**}

Parameters

dynamic	Enables CAR and specifies that the client host addresses are added to the forwarding table only. The subnet of the user address pool, from which the client address was assigned, is added to the routing table. RIP and OSPF will advertise only the subnet of the address pool, not the client host addresses. When the last client using this user address pool disconnects, the subnet route will be removed from the routing table. RIP and OSPF will propagate the route deletion to surrounding networks.
host	Enables CAR and specifies that redistribution of client routes is limited to host routes only. Host routes are added to both the forwarding table and the routing table. RIP and OSPF advertise the host routes of the VPN clients to their peers.
static	Enables CAR and specifies that the client host addresses are added to the forwarding table only. The subnet of the user address pool, from which the client address was assigned, is added to the routing table. RIP and OSPF will advertise only the subnet of the address pool, not the client host addresses. When the last client using this user address pool disconnects, the subnet route will not be removed from the routing table. The subnet of the user address pool will remain in the routing table as long as the user address pool remains valid. The subnet for the user address pool will be deleted from the routing table only when you delete the user address pool itself.

Default

Disabled

Command mode

Router CAR Configuration

Next command mode

Router CAR Configuration

Required privileges

Services Management - Manage
User Management - None

Related commands

router car
show router car
threshold

Example

The following example enables CAR on the gateway and sets the aggregation mode to dynamic. In dynamic aggregation mode, the subnet of the user address pool is removed from the routing table after the last host address drawn from this address pool is removed from the forwarding table.

```
CES(config)# router car
CES(config-car)# aggregation dynamic
CES(config-car)#
```

The following example sets the aggregation mode to static. In static aggregation mode, after the subnet of the user address pool is added to the routing table, it remains in the routing table until the user address pool is deleted.

```
CES(config-car)# aggregation static
CES(config-car)#
```

router car

Use this command to enable client address redistribution (CAR) on the gateway and to navigate to Router CAR Configuration mode. Use the **no** form of the command to globally disable CAR.

Syntax

```
router car [enable]
no router car [enable]
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Router CAR Configuration (if you enter **router car**)
Global Configuration (if you enter **router car enable** or **no router car**)

Required privileges

System Management – Manage
User Management – None

Related commands

aggregation
show router car
threshold

Example

The following example enables CAR globally.

```
CES(config)# router car enable
CES(config)#
```

The following example navigates to Router CAR Configuration mode.

```
CES(config)# router car
CES(config-car)#
```

The following example disables CAR globally.

```
CES(config)# no router car
CES(config)#
```

show router car

Use this command to display the status of CAR and the type of aggregation that is configured for it.

Syntax

show router car

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

Services Management - Manage
User Management - None

Related commands

aggregation
router car
threshold

Example

The following example displays the CAR configuration.

```
CES# show router car
Client Address Redistribution Configuration
  CAR: enabled
  CAR Aggregation Mode: static
  Max Number of Client Host Routes: 200
CES#
```

threshold

Use this command to set the maximum number of user tunnel host routes that the gateway can advertise.

Syntax

threshold <*count*>

Parameters

count	Specifies the maximum number of user tunnel host routes that the gateway advertises. Type an integer from 0 through 10000.

Default

200 user tunnel host routes

Command mode

Router CAR Configuration

Next command mode

Router CAR Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

aggregation
router car
show router car

Example

The following example resets the maximum number of user tunnel host routes that the gateway advertises to 300.

```
CES(config)# router car
CES(config-car)# threshold 300
CES(config-car)#
```

Chapter 39
Equal-cost multipath configuration commands

This chapter describes the equal-cost multipath configuration commands.

Command	Page
ip load-sharing	1651
maximum-paths	1653
ospf maximum-paths	1654
rip maximum-paths	1654
show ecmp	1657

ip load-sharing

This command selects the forwarding algorithms.

Syntax

```
ip load-sharing {per-packet | per-destination | per-source}
```

Parameters

per-packet	Round robin forwarding algorithm.
per-destination	Source destination forwarding algorithm
per-source	Source forwarding algorithm.

Default

per-packet

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This should be specified in the context of the ECMP routing process.

Example

This example selects round robin for per-packet forwarding.

```
CES(config)# ip load-sharing per-packet
```

This example selects round robin for per-source forwarding.

```
CES(config)# ip load-sharing per-source
```

maximum-paths

This commands set the maximum number of equal-cost paths to calculate across the system. The **no** form of this command sets it to the default value of 1.

Syntax

```
maximum-paths <n>
no maximum-paths
```

Parameters

n	The maximum number of equal-cost paths; the range is from 1 through 8.

Default

1

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This should be specified in the context of the ECMP routing process.

Example

This example sets the maximum number of equal-cost paths to 4.

```
CES(config)# maximum-paths 4
```

ospf maximum-paths

This command sets the maximum number of equal-cost paths to calculate within OSPF. The **no** form of this command sets it to the default value of 1.

Syntax

ospf maximum-paths <*n*>
no ospf maximum-paths

Parameters

n	The maximum number of equal-cost paths within OSPF; the range is from 1 through 4.

Default

1

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This should be specified in the context of the OSPF routing process.

Example

This example sets the number of maximum equal-cost paths within OSPF to 2.

```
CES(config)# ospf maximum-paths 2
```

rip maximum-paths

This command sets the maximum number of equal-cost paths to calculate within RIP. The **no** form of this command sets it to the default value of 1.

Syntax

```
rip maximum-paths <n>
no rip maximum-paths
```

Parameters

n	The maximum number of equal-cost paths within RIP; the range is from 1 through 4.

Default

1

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Prerequisites

This should be specified in the context of the RIP routing process.

Example

This example sets the number of maximum equal-cost paths within RIP to 2.

```
CES(config)# rip maximum-paths 2
```

show ecmp

This command shows the configuration of ECMP.

Syntax

show ecmp

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Example

```
CES# show ecmp

Maximum Paths = 1
Maximum OSPF Paths = 1
Maximum RIP Paths = 1
Ip Load Sharing Algo = Per Destination
```

Chapter 40
DHCP relay configuration commands

This chapter describes the DHCP relay configuration commands.

Command	Page
ip dhcp-relay	1659
ip forward-protocol dhcp-relay	1661
ip helper-address	1662
show dhcp-relay config	1663
show dhcp-relay config interface	1664
show dhcp-relay config statistics	1665

ip dhcp-relay

Use this command to set the private interface to act as a dhcp relay.

Syntax

ip dhcp-relay <*A.B.C.D.*> {**enable** | **disable**}

Parameters

<A.B.C.D.>	Configure the IP A.B.C.D (multinet address) with dhcp relay.
Enable	Enables the IP to act as dhcp relay.
Disable	Disables the IP to act as dhcp relay.

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

The following example enables and then disables DHCP relay on the gateway.

```
CES(config)# ip dhcp-relay <A.B.C.D.> enable
CES(config)# no ip dhcp-relay <A.B.C.D.> disable
CES(config)#
```

ip forward-protocol dhcp-relay

Use this command to globally enable DHCP relay. Use the **no** form of the command to globally disable DHCP relay.

Syntax

```
ip forward-protocol dhcp-relay
no ip forward-protocol dhcp-relay
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

The following example enables and then disables DHCP relay on the gateway.

```
CES(config)# ip forward-protocol dhcp-relay
CES(config)# no ip forward-protocol dhcp-relay
CES(config)#
```

ip helper-address

This command sets the DHCP-relay server IP address and enables or disables the server IP address for an interface.

Syntax

ip helper-address <*ipaddr1*> **server** {**1** | **2** | **3**} <*dest_addr*>
no ip helper-address <*ipaddr1*> **server** {**1** | **2** | **3**}

Parameters

ipaddr1	Specifies the interface address.
dest_addr	Specifies the destination host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.
1, 2, or 3	Specifies the DHCP server index number (1, 2, or 3).

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

The following examples add and remove a DHCP server for the relay agent:

```
CES(config)# ip helper-address 10.0.179.12 server 1 10.0.0.1
CES(config)# no ip helper-address 10.0.179.12 server 1
```

show dhcp-relay config

Use this command to display the Dynamic Host Configuration Protocol (DHCP) configuration settings.

Syntax

show dhcp-relay config

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Example

```
CES> show dhcp-relay config

DHCP Relay OFF
```

Physical/Tunnel Interface	State	DHCP Servers
10.0.0.21	Enabled	Any DHCP Server
BurlingtonToBoston	Disabled	1.2.3.4, 2.3.4.5, 3.4.5.6

show dhcp-relay config interface

This command displays the DHCP physical/tunnel interface configuration setting.

Syntax

show dhcp-relay config interface {<*ip_address*> | <*hostname*>}

Parameters

ip_address	IP address of the physical interface.
name	Name of the branch office tunnel.

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Example

The following example shows the DHCP physical interface configuration.

```
CES> show dhcp-relay interface 10.0.0.21
```

Physical/Tunnel Interface	State	DHCP Servers
10.0.0.21	Enabled	Any DHCP Server

The following example shows the DHCP tunnel interface configuration.

```
CES> show dhcp-relay interface BurlingtonToBoston
```

Physical/Tunnel Interface	State	DHCP Servers
BurlingtonToBoston	Enabled	Any DHCP Server

show dhcp-relay config statistics

This command displays the DHCP relay statistics.

Syntax

```
show dhcp-relay config statistics
```

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Example

The following example shows the DHCP statistics.

```
CES> show dhcp-relay statistics
```

DHCP Relay Packets	Number of Packets
In	100
Out	250
Discarded	0

Chapter 41
Multicast relay configuration commands

This chapter describes the multicast relay configuration commands.

Command	Page
multicast-boundary interface	1668
multicast-relay congestion-threshold	1670
multicast-relay enable	1672
show multicast-relay	1673
show multicast-relay status interfaces	1675
show multicast-relay status statistics	1676

multicast-boundary interface

Use this command to add an interface or tunnel to the multicast boundary list or to enable an interface or tunnel on the list. The multicast relay boundary keeps multicast packets from being forwarded indiscriminately. Use the **no** form of the command to disable the interface or tunnel or to delete the interface or tunnel from the multicast boundary list.

Syntax

multicast-boundary interface {<*ip-address*> | **global**} **list** <*list-name*>

multicast-boundary interface {<*ip-address*> | **global**} **enable**

no multicast-boundary interface {<*ip-address*> | **global**}

no multicast-boundary interface {<*ip-address*> | **global**} **enable**

Parameters

ip-address	Specifies the IP address to include in the boundary list. The IP address can be for a physical interface or a virtual interface (tunnel). Type the IP address of the physical interface or of the tunnel end point. To include all interfaces, type **global**.
list-name	Specifies the name of the access list to apply to the interface or tunnel that you are adding to the multicast relay boundary list.

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Warning - This entry already exists
% Error - Multicast relay already configured on this
interface
```

Related commands

multicast-relay congestion-threshold
multicast-relay enable
show multicast-relay
show multicast-relay status interfaces
show multicast-relay status statistics

Example

The following example adds the interface 111.22.33.44 to the multicast boundary list and applies the access list “deny_239.0.0.0” to it.

```
CES# configure terminal
CES(config)# multicast-boundary interface 111.22.33.44 list
deny_239.0.0.0
CES(config)#
```

The following example enables interface 111.22.33.44 for the multicast boundary list.

```
CES(config)# multicast-boundary interface 111.22.33.44
enable
CES(config)#
```

The following example disables interface 111.22.33.44 for the multicast boundary list.

```
CES(config)# no multicast-boundary interface 111.22.33.44
enable
CES(config)#
```

The following example deletes interface 111.22.33.44 from the multicast boundary list.

```
CES(config)# no multicast-boundary interface 111.22.33.44
CES(config)#
```

multicast-relay congestion-threshold

Use this command to specify the multicast relay congestion threshold. The congestion threshold relates to the number of network processing memory buffers available to process multicast traffic. If forwarding performance for unicast traffic decreases because of the amount of multicast traffic, decrease the value of this parameter. Use the **no** form of the command to reset the threshold to its default value, 3000.

Syntax

multicast-relay congestion-threshold <*value*>
no multicast-relay congestion-threshold

Parameters

value	Specifies the congestion threshold for the gateway. Type an integer from 0 through 3000 (the default value).

Default

3000

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

multicast-boundary interface
multicast-relay enable
show multicast-relay
show multicast-relay status interfaces
show multicast-relay status statistics

Example

The following example changes the congestion threshold value to 2000.

```
CES(config)# multicast-relay congestion-threshold 2000
CES(config)#
```

The following example resets the congestion threshold value to its default value (3000).

```
CES(config)# no multicast-relay congestion-threshold
CES(config)#
```

multicast-relay enable

Use this command to enable multicast relay globally on the Nortel VPN Router. Use the **no** form of the command to disable multicast relay.

Syntax

```
multicast-relay enable
no multicast-relay enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

multicast-boundary interface
multicast-relay congestion-threshold
show multicast-relay
show multicast-relay status interfaces
show multicast-relay status statistics

Example

The following example enables multicast relay on the gateway.

```
CES# configure terminal
CES(config)# multicast-relay enable
CES(config)#
```

The following example disables multicast relay.

```
CES(config)# no multicast-relay enable
CES(config)#
```

show multicast-relay

Use this command to display the configuration parameters for multicast relay.

Syntax

show multicast-relay

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

multicast-boundary interface
multicast-relay congestion-control
multicast-relay enable
show multicast-relay status interfaces
show multicast-relay status statistics

Example

The following example shows multicast relay configuration values.

```
CES# show multicast-relay

Multicast Relay       :    ENABLED
Congestion Threshold  :    2000

Interface:           47.17.248.53
Access Name/Number:  myaccesslist
State:               DISABLED

CES#
```

show multicast-relay status interfaces

Use this command to display information about enabled multicast relay interfaces.

Syntax

```
show multicast-relay status interfaces
```

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

```
multicast-boundary interface
multicast-relay congestion-threshold
multicast-relay enable
show multicast-relay
show multicast-relay status statistics
```

Example

The following example displays information about the interfaces configured for multicast relay.

```
CES# show multicast-relay status interfaces

  11/19/2003   16:01:26
  Interface        Access-list
  ---------------- -----------
  47.17.248.56     myaccesslist

CES#
```

show multicast-relay status statistics

Use this command to display multicast relay statistics.

Syntax

show multicast-relay status statistics

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

multicast-boundary interface
multicast-relay congestion-threshold
multicast-relay enable
show multicast-relay
show multicast-relay status interfaces

Example

The following example displays multicast relay status and statistics.

```
CES# show multicast-relay status statistics
  11/19/2003   15:58:26
  Global Multicast Relay Status: Disabled
  Configured Threshold value: 3000
  Total number of packets queued: 0
  Total number of packets dropped: 0


  Multicast Relay Input/Output Statistics
  ---------------------------------------
  Interface        Cid PktsRcvd PktsSent PktsDropped
  ---------------- --- -------- -------- -----------
  0.0.0.0           1     0         0         0

CES#
```

Chapter 42
IGMP configuration commands

This chapter describes the IGMP configuration commands.

Command	Page
access-filter	1680
clear ip igmp statistics	1683
ip igmp proxy-type	1685
ip igmp enable	1687
last-member-query-int	1690
query-interval	1693
query-max-resp	1696
query-timeout	1699
robustval	1702
show ip igmp groups	1705
show ip igmp groups interface	1707
show ip igmp interface	1709
show ip igmp statistics	1711
show ip igmp statistics interface	1713
show running-config for igmp routing	1715
snmp-server mib igmp	1717
static members	1720
unsolicited-report-interval	1722

access-filter

Use this command to specify the access filter for:

- Ethernet, VLAN, and serial interfaces (Interface Mode)
- subinterfaces (Interface mode)
- branch offices (Branch Office Connection mode)
- groups (Group IGMP Configuration mode)

Syntax

Use the following command to configure the access filter on branch offices and groups.

access-filter *<name>*

Use the following command to configure the access filter on interfaces:

ip igmp access-filter *<name> [<A.B.C.D>]*

Use the following command to configure the access filter on serial interfaces:

ppp ip igmp access-filter *<name>*

Parameters

A.B.C.D	Specifies the IP address of the interface.
name	Specifies the name of the access filter.

Default

Disabled

Command mode

Branch Office Group IGMP Configuration
Group IGMP Configuration
Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

ip igmp proxy-type
last-member-query-int
query-interval
query-max-resp
query-timeout
robustval
unsolicited-report-interval

Example

The following example configures AF1 for /Group 1.

```
CES#
CES#configure terminal
CES(config)#bo-group igmp /Group 1
CES(config-bo_group/igmp)#access-filter AF1
CES(config-bo_group/igmp)#
```

The following example configures AF2 for FastEthernet 1/1.

```
CES#
CES#configure terminal
CES(config)#interface fastEthernet 1/1
CES(config-if)#ip igmp access-filter AF2
CES(config-if)#
```

clear ip igmp statistics

Use this command to clear IGMP statistics.

Syntax

clear ip igmp statistics

Parameters

None

Default

Disabled

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

list of related commands

Example

The following example clears IGMP statistics:

```
CES#
CES#clear ip igmp statistics
CES#
```

ip igmp proxy-type

Use this command to specify the IGMP proxy type (upstream or downstream) for:

- Ethernet, VLAN, and serial interfaces (Interface Mode)
- subinterfaces (Interface mode)
- branch offices (Branch Office Connection mode)

Syntax

Use the following command to specify the IGMP proxy type for branch offices:

proxy-type {upstream | downstream}

Use the following command to configure the last member query interval on interfaces:

ip igmp proxy-type {upstream | downstream}*[<A.B.C.D>]*

Use the following command to configure the last member query interval on serial interfaces:

ppp ip igmp proxy-type {upstream | downstream}

Parameters

A.B.C.D	Specifies the secondary address of an ethernet interface

Default

Disabled

Command mode

Branch Office Group IGMP Configuration
Group IGMP Configuration
Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

last-member-query-int
query-interval
query-max-resp
query-timeout
robustval
unsolicited-report-interval

Example

The following example configures the upstream proxy on FastEthernet 0/1.

```
CES(config)#
CES(config)#interface fastEthernet 0/1
CES(config-if)#ip igmp proxy-type upstream
CES(config-if)#
```

ip igmp enable

Use this command to globally enable and configure IGMP. You can also enable IGMP on:

- Ethernet, VLAN, and serial interfaces (Interface Mode)
- subinterfaces (Interface mode)
- branch offices (Branch Office Connection mode)
- groups (Group Connectivity configuration mode)

Use the **no** form of the command to disable IGMP.

Syntax

Use the following syntax to globally enable and configure IGMP.

```
ip igmp {enable | membership-group-limit <10-512> | version
{1 |2 |3} }
```

Use the following syntax to enable IGMP on interfaces.

ip igmp enable *[<A.B.C.D>]*

Use the following syntax to enable IGMP on serial interfaces.

ppp ip igmp enable

Use the following syntax to enable IGMP on branch offices or groups.

igmp enable

Parameters

membership-group-limit	Configures membership group limit.
version	Configures the IGMP version to be either IGMPv1, IGMPv2, or IGMPv3.
A.B.C.D	Specifies the secondary address of an ethernet interface. This parameter applies only when in Interface Configuration mode.

Default

Disabled

Command mode

Global Configuration
Interface Configuration
Branch Office Connection
Group IGMP Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% This feature is not enabled. Contact you sales
representative to purchase a key to enable this feature. The
key can then be entered using the 'license install' command
from Global Configuration mode.
% No IGMP Upstream interface configured.
```

Related commands

None

Example

The following example globally enables IGMP, sets a membership group limit of 512, and specifies the IGMP version as IGMPv3.

```
CES# configure terminal
CES(config)# ip igmp enable
CES(config)# ip igmp membership-group-limit 512
CES(config)# ip igmp version 3
CES(config)#
```

The following example disables IGMP.

```
CES(config)# no ip igmp enable
CES(config)#
```

The following example globally enables IGMP on Fast Ethernet interface 0/1.

```
CES#
CES#configure terminal
CES(config)#interface fastEthernet 0/1
CES(config-if)#eip igmp enable
CES(config-if)#
```

last-member-query-int

Use this command to configure the last member query interval for:

- Ethernet, VLAN, and serial interfaces (Interface Mode)
- subinterfaces (Interface mode)
- branch offices (Branch Office IGMP group mode)
- groups (Group IGMP Configuration mode)

Syntax

Use the following command to configure the last member query interval on branch offices:

last-member-query-int <10-250>

Use the following command to configure the last member query interval on interfaces:

ip igmp last-member-query-int <10-250> *[<A.B.C.D>]*

Use the following command to configure the last member query interval on serial interfaces:

ppp ip igmp last-member-query-int *<10-250>*

Parameters

A.B.C.D	Specifies the secondary address of an ethernet interface. This parameter applies only when in Interface Configuration mode.

Default

Disabled

Command mode

Branch Office Group IGMP
Group IGMP Configuration
Interface Configuration

Next command mode

Branch Office Group IGMP
Group IGMP Configuration
Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

access-filter
ip igmp proxy-type
query-interval
query-max-resp
query-timeout
robustval
unsolicited-report-interval

Example

The following example configures last member query interval for /Group 1.

```
CES#
CES#configure terminal
CES(config)#bo-group igmp /Group 1
CES(config-bo_group/igmp)#last-member-query-int 250
CES(config-bo_group/igmp)#
```

The following example configures last member query interval for /Group 2.

```
CES#
CES#configure terminal
CES(config)#group igmp /Group 2
CES(config-group/igmp)#last-member-query-int 250
CES(config-group/igmp)#
```

query-interval

Use this command to configure the query interval on:

- Ethernet, VLAN, and serial interfaces (Interface Mode)
- subinterfaces (Interface mode)
- branch offices (Branch Office IGMP group mode)
- groups (Group IGMP Configuration mode)

Syntax

Use the following command to configure the query interval on branch offices:

query-interval <1-512>

Use the following command to configure the query interval on interfaces:

ip igmp query-interval <1-512> [<*A.B.C.D*>**]**

Use the following command to configure the query interval on serial interfaces:

ppp ip igmp query-interval <1-512>

Parameters

A.B.C.D	Specifies the secondary address of an ethernet interface. This parameter applies only when in Interface Configuration mode.

Default

Disabled

Command mode

Branch Office Group IGMP
Group IGMP Configuration
Interface Configuration

Next command mode

Branch Office Group IGMP
Group IGMP Configuration
Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

access-filter
ip igmp proxy-type
last-member-query-int
query-max-resp
query-timeout
robustval
unsolicited-report-interval

Example

The following example configures the query interval for a branch office group.

```
CES#
CES#configure terminal
CES(config)#bo-group igmp /Group 1
CES(config-bo_group/igmp)#query-interval 512
CES(config-bo_group/igmp)#
```

The following example configures the query interval for a group.

```
CES#
CES#configure terminal
CES(config)#group igmp /Group 2
CES(config-group/igmp)#query-interval 512
CES(config-group/igmp)#
```

query-max-resp

Use this command to configure the query maximum response on:

- Ethernet, VLAN, and serial interfaces (Interface Mode)
- subinterfaces (Interface mode)
- branch offices (Branch Office IGMP group mode)
- groups (Group IGMP Configuration mode)

Syntax

Use the following command to configure the query maximum response on branch offices:

query-max-resp <10-250>

Use the following command to configure the query maximum response on interfaces:

ip igmp query-max-resp <10-250> [<*A.B.C.D*>**]**

Use the following command to configure the query maximum response on serial interfaces:

ppp igmp query-max-resp <10-250>

Parameters

A.B.C.D	Specifies the secondary address of an ethernet interface. This parameter applies only when in Interface Configuration mode.

Default

Disabled

Command mode

Branch Office Group IGMP
Group IGMP Configuration
Interface Configuration

Next command mode

Branch Office Group IGMP
Group IGMP Configuration
Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

access-filter
ip igmp proxy-type
last-member-query-int
query-interval
query-timeout
robustval
unsolicited-report-interval

Example

The following example configures the maximum query interval for a branch office group.

```
CES#
CES#configure terminal
CES(config)#bo-group igmp /Group 1
CES(config-bo_group/igmp)#query-max-resp 250
CES(config-bo_group/igmp)#
```

The following example configures the maximum query interval for a group.

```
CES#
CES#configure terminal
CES(config)#group igmp /Group 2
CES(config-group/igmp)#query-max-resp 250
CES(config-group/igmp)#
```

query-timeout

Use this command to configure the query timeout on:

- Ethernet, VLAN, and serial interfaces (Interface Mode)
- subinterfaces (Interface mode)
- branch offices (Branch Office IGMP group mode)
- groups (Group IGMP Configuration mode)

Syntax

Use the following command to configure the query timeout on branch offices:

query-timeout <10-1024>

Use the following command to configure the query timeout on interfaces:

ip igmp query-timeout <10-1024> *[<A.B.C.D>]*

Use the following command to configure the query timeout on branch offices and serial interfaces:

ppp ip igmp query-timeout <10-1024>

Parameters

A.B.C.D	Specifies the secondary address of an ethernet interface. This parameter applies only when in Interface Configuration mode.

Default

Disabled

Command mode

Branch Office Group IGMP
Group IGMP Configuration
Interface Configuration

Next command mode

Branch Office Group IGMP
Group IGMP Configuration
Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

access-filter
ip igmp proxy-type
last-member-query-int
query-interval
query-max-resp
robustval
unsolicited-report-interval

Example

The following example configures the query timeout for a branch office group.

```
CES#
CES#configure terminal
CES(config)#bo-group igmp /Group 1
CES(config-bo_group/igmp)#query-timeout 1024
CES(config-bo_group/igmp)#
```

The following example configures the query timeout for a group.

```
CES#
CES#configure terminal
CES(config)#group igmp /Group 2
CES(config-group/igmp)#query-timeout 1024
CES(config-group/igmp)#
```

robustval

Use this command to configure the robust value on:

- Ethernet, VLAN, and serial interfaces (Interface Mode)
- subinterfaces (Interface mode)
- branch offices (Branch Office IGMP group mode)
- groups (Group IGMP Configuration mode)

Syntax

Use the following command to configure the robust value on branch offices:

robustval <2-64>

Use the following command to configure the robust value on interfaces:

ip igmp robustval <2-64> [<*A.B.C.D*>**]**

Use the following command to configure the robust value on serial interfaces:

ppp ip igmp robustval <2-64>

Parameters

A.B.C.D	Specifies the secondary address of an ethernet interface. This parameter applies only when in Interface Configuration mode.

Default

Disabled

Command mode

Branch Office Group IGMP
Group IGMP Configuration
Interface Configuration

Next command mode

Branch Office Group IGMP
Group IGMP Configuration
Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

access-filter
ip igmp proxy-type
last-member-query-int
query-interval
query-max-resp
query-timeout
unsolicited-report-interval

Example

The following example configures the robust value for a branch office group.

```
CES#
CES#configure terminal
CES(config)#bo-group igmp /Group 1
CES(config-bo_group/igmp)#robustval 64
CES(config-bo_group/igmp)#
```

The following example configures the robust value for a group.

```
CES#
CES#configure terminal
CES(config)#group igmp /Group 2
CES(config-group/igmp)#robustval 64
CES(config-group/igmp)#
```

show ip igmp groups

Use this command to view IGMP group information.

Syntax

show ip igmp groups {count |detail |group <a.b.c.d.>}

Parameters

count	Displays how many multicast groups are passing IGMP traffic through the Nortel VPN Router.
detail	Displays multicast group details.
group	Displays information about the specified group.
<a.b.c.d.>	Specifies the IP address of the group,

Default

Disabled

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

list of related commands

Example

The following example shows how many groups the IGMP:

```
CES#
CES# show ip igmp groups count

Current Group Count: 2
CES(config)#
```

show ip igmp groups interface

Use this command to view IGMP group interface information.

Syntax

show ip igmp groups interface {atm <*slot*>/<*port*>**| branch office** <*word*>**| bri** <*slot*>/<*port*> **|fastEthernet** <*slot*>/<*port*> **| gigabitethernet** <*slot*>/<*port*> **| serial** <*slot*>/<*port*> **| utunnel** <*a.b.c.d.*>**}**

Parameters

ATM	Displays information about the ADSL/ATM interface.
branch office	Displays information about the branch office interface.
bri	Displays information about the SDN BRI interface.
fastEthernet	Displays information about the Fast Ethernet interface.
gigabitethernet	Displays information about the Gigabit Ethernet interface.
serial	Displays information about the serial interface.
utunnel	Displays information about the user tunnel interface.
word	Specifies the name of the branch office interface.
slot	For interface objects, specifies the slot of the interface card.
port	For interface objects, specifies the slot of the interface card.
a.b.c.d.	Specifies the IP address of the user tunnel,

Default

Disabled

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

list of related commands

Example

The following example shows how many groups the IGMP:

```
CES#
CES#show ip igmp groups interface fastEthernet 0/1

Interface 172.16.120.18
No group present on this interface
CES#
```

show ip igmp interface

Use this command to view IGMP interface information.

Syntax

show ip igmp interface

Parameters

None

Default

Disabled

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

list of related commands

Example

The following example shows IGMP interface information:

```
CES#
CES#show ip igmp interface
IGMP Interface  1.2.3.4
   Enabled              =  ENABLED
   Query Interval       =  125
   Query Max Resp Time  =  100 (1/10 sec)
   Last Mber Query Intvl=  10  (1/10 sec)
   DR Timeout           =  255
   Robustness Value     =  2
   ProxyType            =  Downstream
   Access Name          =  Not configured
IGMP Interface 1.2.3.4 Static Groups:
 No static group configured

IGMP Interface  172.16.120.18
   Enabled              =  ENABLED
Robustness Value =  2
ProxyType            =  Upstream
   Unsolicited Rep Intvl=  10
CES#
```

show ip igmp statistics

Use this command to view IGMP statistics.

Syntax

show ip igmp statistics

Parameters

None

Default

Disabled

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

list of related commands

Example

The following example shows IGMP statistics:

```
CES#
CES#show ip igmp statistics

IGMP Statistics:
  In Queries            : 0
  In Reports            : 0
  In Leaves             : 0
  In Unknown Type       : 0
  Out Queries           : 0
  Out Reports           : 0
  Out Leaves            : 0
  Dropped               : 0
  Bad                   : 0
  Wrong Version Queries : 0
CES#
```

show ip igmp statistics interface

Use this command to view IGMP statistics for each interface.

Syntax

show ip igmp statistics interface

Parameters

None

Default

Disabled

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

list of related commands

Example

The following example shows IGMP interface information:

```
CES#
CES#show ip igmp statistics interface

                                                Queries      Reports
Interface       Upstream  Groups  DR        Out   In  Out   In
172.16.120.18   YES       0       0.0.0.0   0     0   0     0

CES#
```

show running-config for igmp routing

Use this command to view the running-config information for IGMP routing.

Syntax

```
show ip igmp running-config {[file-url <word>] |
[user-friendly]} routing igmp
```

Parameters

file-url	Displays output filename in /system/runconf for Running Configuration
user-friendly	Displays the information in a user-friendly format.
word	Specifies the output filename to store the running-config file,

Default

Disabled

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

list of related commands

Example

The following example shows IGMP interface information:

```
CES#
CES#show running-config user-friendly routing igmp
! [IGMP Configuration]
ip igmp enable
! [IGMP Configuration (END)]
CES#
```

snmp-server mib igmp

Use this command to enable SNMP MIBs for the IGMP protocol.

Syntax

snmp-server mib igmp

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

snmp-server enable traps service igmp

Example

The following example shows IGMP interface information:

```
CES#
CES#configure terminal
Enter configuration commands, one per line. End with Ctrl/z.
CES#snmp-server mib igmp
CES#
```

snmp-server enable traps service igmp

Use this command to enable SNMP traps service for the IGMP protocol.

Syntax

snmp-server enable traps service igmp

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

snmp-server mib igmp

Example

The following example shows IGMP interface information:

```
CES#
CES#configure terminal
CES#snmp-server enable traps service igmp
CES#
```

static members

Use this command to configure static members on interfaces.

Syntax

Use the following command to configure the static members on interfaces:

ip igmp static-members *[<A.B.C.D>]*

Use the following command to configure the static members on serial interfaces:

ppp ip igmp static-members *[<A.B.C.D>]*

Parameters

A.B.C.D	Specifies the multicast group address.

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

access-filter
ip igmp proxy-type
last-member-query-int
query-interval
query-max-resp
query-timeout
robustval

Example

The following example configures the static members.

```
CES#
CES#configure terminal
CES(config)#interface fastEthernet 0/4
CES(config-if)#ip igmp static-member 225.0.0.0
CES(config-group/igmp)#
```

unsolicited-report-interval

Use this command to configure the unsolicited report interval on:

- Ethernet, VLAN, and serial interfaces (Interface Mode)
- subinterfaces (Interface mode)
- branch offices (Branch Office Group IGMP mode)

Syntax

Use the following command to configure the unsolicited report interval on branch offices:

unsolicited-report-interval <1-25>

Use the following command to configure the unsolicited report interval on interfaces:

ig igmp unsolicited-report-interval <1-25> [<*A.B.C.D*>**]**

Use the following command to configure the unsolicited report interval on serial interfaces:

ppp ig igmp unsolicited-report-interval <1-25>

Parameters

A.B.C.D	Specifies the IP address of the interface. This parameter applies only when in Interface Configuration mode.

Default

Disabled

Command mode

Branch Office Connection
Interface Configuration

Next command mode

Branch Office Connection
Interface Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

access-filter
ip igmp proxy-type
last-member-query-int
query-interval
query-max-resp
query-timeout
robustval

Example

The following example configures the unsolicited report interval value for a branch office group.

```
CES#
CES#configure terminal
CES(config)#bo-group igmp /Group 1
CES(config-bo_group/igmp)#unsolicited-report-interval 25
CES(config-bo_group/igmp)#
```

The following example configures the unsolicited report interval value for a group.

```
CES#
CES#configure terminal
CES(config)#group igmp /Group 2
CES(config-group/igmp)#unsolicited-report-interval 25
CES(config-group/igmp)#
```

Chapter 43
Static routing configuration commands

This chapter describes the static routing configuration commands.

Command	Page
ip default-network	1726
ip default-route-preference	1727
ip route	1729
router static	1731
show ip default-route-preference	1732
show ip static	1734

ip default-network

Use this command to define a default network (also known as a default route). Use the **no** form of the command to delete the default network.

Syntax

```
ip default-network <gateway> {public | private} [<cost>]
[enabled | disabled]
no ip default-network <gateway> {public | private}
```

Parameters

gateway	Specifies the IP address of the gateway router to the default network.
public **private**	Specifies the type of interface on the Nortel VPN Router device.
cost	Specifies the cost for the route (from 1 through 255). The default cost is 10.
enabled **disabled**	Specifies the administrative state of the default network.

Default

Cost is set at 10.
Administrative state is enabled.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ip default-route-preference
ip route
show ip default-route-preference
show ip static

Example

The following example adds a public default route with gateway 10.0.0.10 to the routing table with a cost of 30 and enables the default route.

```
CES(config)# ip default-network 10.0.0.10 public cost 30
enable
CES(config)#
```

This example deletes a public default route with gateway 10.0.0.10.

```
CES(config)# no ip default-network 10.0.0.10 public
CES(config)#
```

ip default-route-preference

Use this command to specify the preferred default route for non-tunneled packets that arrive on private interfaces. With this command, you can route packets that do not go across a tunnel to a defined remote network in one of two ways:

- If you set the default route preference to **public** (the default value), these packets go out the public interface using the public default gateway.
- If you set the default route preference to **private**, these packets go out over the branch office tunnel instead.

Syntax

```
ip default-route-preference private {private | public}
```

Parameters

private	Specifies that non-tunneled packets should go out over the branch office tunnel.
public	Specifies that non-tunneled packets should go out the public default route.

Default

Public

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

```
ip default-network
ip route
show ip default-route-preference
show ip static
```

Example

The following example sets the preferred default route for private interfaces to "private."

```
CES(config)# ip default-route-preference private private
CES(config)#
```

The following example sets the preferred default route for private interfaces to "public."

```
CES(config)# ip default-route-preference private public
CES(config)#
```

ip route

Use this command to create a static route. You can also use this command to enable or disable the static route and to change the cost of the route. Use the **no** form of the command to delete the static route.

Syntax

```
ip route <ip_address> <mask> <gateway> [<cost>]
[enabled | disabled]
no ip route <ip_address> <mask> <gateway>
```

Parameters

ip_address	Specifies the IP address at the other end of the static route.
mask	Specifies the associated subnet mask for the IP address.
gateway	Specifies the IP address of the gateway or of the outgoing WAN interface.
cost	Specifies the cost associated with the route. Enter a value from 1 through 65535.
enabled **disabled**	Specifies the administrative state of the static route.

Default

Cost is set at 10.
Administrative state is enabled.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ip default-network
router static
show ip static

Example

The following example adds a new static route with an IP address and network mask of 10.254.0.0 and 255.255.0.0. This new static route has 10.254.1.1 as a gateway and a cost metric of 2.

```
CES(config)# ip route 10.254.0.0 255.255.0.0 10.254.1.1 2
```

This example changes the cost of the configured static route to 20.

```
CES(config)# ip route 10.254.0.0 255.255.0.0 10.254.1.1 20
```

This command disables the static route. (It is not deleted from the configuration.)

```
CES(config)# ip route 10.254.0.0 255.255.0.0 10.254.1.1
disabled
```

This command reenables the static route.

```
CES(config)# ip route 10.254.0.0 255.255.0.0 10.254.1.1
enabled
```

This example removes the static route with an IP address of 10.254.0.0 from the configuration.

```
CES(config)# no ip route 10.254.0.0 255.255.0.0 10.254.1.1
```

router static

Use this command to enable static routing globally on the system. Use the **no** form of the command to disable the static routing process globally.

Syntax

```
router static
no router static
```

Parameters

None

Default

Enabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

ip route
show ip static

Example

The following example globally enables static routes. It does not enable individual static routes. Enabled static routes are added to the route table.

```
CES(config)# router static
```

The following example globally disables static routes. Static route entries are not removed from the configuration. Disabled static routes are removed from the route table.

```
CES(config)# no router static
```

show ip default-route-preference

Use this command to display the preferred default route for non-tunneled packets that arrive on private interfaces.

Syntax

show ip default-route-preference

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

ip default-route-preference

Example

The following example shows the preferred default route for non-tunneled packets arriving on private interfaces.

```
CES> show ip default-route-preference
IP Default Route Preference
  Incoming Route Type: private
  Outgoing Route Preference Type: public
CES>
```

show ip static

Use this command to display the static routes configured on the gateway.

Syntax

```
show ip static
```

Parameters

None

Default

None

Command mode

User EXEC

Next command mode

User EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

```
ip route
router static
```

Example

The following example displays all static routes configured on the gateway.

```
CES> show ip static
show ip static                          Aug 25, 2003   12:11:22 (GMT)

Network         Mask              Cost   Gateway          Admin State
=================================================================
0.0.0.0         0.0.0.0           1      47.17.68.241     enabled
4.4.4.4         255.255.255.252   1      7.7.7.2          disabled
4.4.4.4         255.255.255.252   1      7.7.7.7          enabled
5.5.5.4         255.255.255.252   1      7.7.7.2          enabled
9.9.9.0         255.255.255.0     1      7.7.7.2          enabled
9.9.9.0         255.255.255.0     10     3.3.3.6          disabled
47.16.1.50      255.255.255.0     1      47.17.68.241     enabled
47.16.2.50      255.255.255.0     1      47.17.68.241     enabled
47.16.38.34     255.255.255.0     1      47.17.68.241     enabled
192.168.1.0     255.255.255.0     1      192.168.2.10     enabled
192.168.3.0     255.255.255.0     1      192.168.2.10     enabled
CES>
```

Chapter 44
Access list/route policy configuration commands

This chapter describes the access list/route policy configuration commands.

Command	Page
access-list permit/deny	1737
route-policy enable/disable	1739

access-list permit/deny

These commands are used to create and delete access lists. The first two commands create an access list. The third command deletes an access list.

Syntax

```
access-list <name> {permit | deny} <ip_address> <mask>
[exact | range]
access-list <name> {permit | deny} [any]
no access-list <name>
access-list <name> list | move rule <number> rule <number>
```

Parameters

name	Name of the standard IP access list.
ip_address	IP address of the host or network to permit or deny.
mask	Mask of the host or network to permit or deny.
permit	Enables packet rejection.
deny	Enables packet forwarding.
list	Lists the current rules under the access list.
move	Puts rule 1 in front of rule 2.

Default

No access lists are created by default.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Warning messages

```
% Deletion of a non-existent access list.
```

Example

This command creates an access list to deny the network 10.254.1.0 and permit others.

```
CES(config)# access-list deny_10.254.1.x_network deny
10.254.1.0 255.255.255.0 range
```

The following command is required if the intent is to only deny the 10.254.1.0 network and permit the rest, because an implicit deny-all is present at the end of all the rules in an access list. The access list rules are applied in the order they were entered.

```
CES(config)# access-list deny_10.254.1.x_network permit any
```

```
CES(config)# no access-list deny_10.254.1.x_network
```

route-policy enable/disable

This command enables and disables the route policy feature globally.

Syntax

```
route-policy
no route-policy
```

Parameters

None

Default

Route policy is enabled by default.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Example

This example disables the route policy feature, globally. Any distribute list or redistribute filters configured will be ignored.

```
CES(config)# no route-policy
```

Chapter 45
Packet capture (PCAP) commands

Packet capture (PCAP) is a tool that allows you to troubleshoot a Nortel VPN Router and the network remotely. This chapter describes packet capture commands.

Command	Page
buffersize	1742
capture	1743
capture add	1745
capture-all	1745
capture enable	1748
capture save	1751
capture start	1752
capture stop	1754
clear capture	1756
direction	1757
filepath	1759
filesize	1761
filter	1762
length	1765
maxfiles	1766
persistent	1768
promiscuous	1770
remoteip	1771
show capture	1773
trigger	1777

Command	Page
type	1779
userid	1782
wrapping	1784

buffersize

Use this command to set the size of the RAM buffer.

Syntax

buffersize <size>

Parameters

size	Specifies the size the of the RAM buffer.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

capture
capture enable
show capture
maxfiles
filepath
filesize

Example

```
CES(capture-ethernet)#buffersize 1048576
```

capture

Use this command to enter capture mode for an existing capture object. Use the **no** form of the command to delete the specified capture object.

Syntax

capture <*name*>
no capture <*name*>

Parameters

name	Specifies the name of an existing capture object.

Default

None

Command mode

Privileged EXEC

Next command mode

Capture Configuration (**`capture`** command)
Privileged EXEC (**`no capture`** command)

Required privileges

System Management - Manage
User Management - None

Prerequisites

To delete a capture object, you must first stop packet capture.

Warning messages

```
% Capture must be stopped first
% Capture object name does not exist
```

Related commands

`capture add`
`capture enable`
`show capture`

Example

The following example navigates to capture mode for the object “test.”

```
CES# capture test
CES(capture-ethernet)#
```

The following example deletes the capture object “test.”

```
CES# no capture test
CES#
```

capture add

Use this command to create a new capture object and to specify the size of the capture buffer for it (the default buffer size is 1 MB).

Syntax

capture add <*name*> {**atm** | **bri** | **dial** | **fastethernet** | **gigabitethernet** | **serial**} <*slot*>/<*port*> [**size** <*octets*>]

capture add <*name*> {**global** | **tunnel**} [**size** <*octets*>]

Parameters

name	Specifies the name of the capture object to be created. This name must be unique on the gateway.
atm	Create a capture object for an ADSL/ATM interface.
bri	Create a capture object for an ISDN BRI interface.
dial	Create a capture object for a dial interface.
fastethernet	Create a capture object for a Fast Ethernet interface.
gigabitethernet	Create a capture object for a Gigabit Ethernet interface.
serial	Create a capture object for a serial interface.
slot	For interface objects, specifies the slot of the interface card.
port	For interface objects, specifies the port on the interface card.
global	Create a capture object for all IP traffic traversing any physical interface or tunnel on the gateway.
tunnel	Create a capture object for a tunnel.
size	Specify the size of the capture buffer (default is 1 MB).
octets	Specifies the number of octets to allocate to the capture buffer. You can enter a value from 32768 through 268435456. The default value is 1 MB.

Default

Buffer size is 1 MB.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% add is not a valid name for capture object
% enable is not a valid name for capture object
% Capture object name already exists
% Console is not in PPP Async mode
% Interface x/y is not a dial interface
% Interface x/y is not a Fast Ethernet interface
% Interface x/y is not a Gigabit Ethernet interface
% Interface x/y is not an ISDN BRI interface
% Interface x/y is not a Serial interface
```

Related commands

capture
capture enable
show capture

Example

The following example creates a capture object named “test1” for Fast Ethernet interface 1/1 and allocates 128,000 octets to the capture buffer.

```
CES# capture add test1 fastethernet 1/1 size 128000
CES#
```

The following example creates a capture object named “test2” for a tunnel session.

```
CES# capture add test2 tunnel
CES#
```

The following example creates a capture object named “test3” to capture all IP traffic going through the gateway.

```
CES# capture add test3 global
CES#
```

capture-all

Use this command to set PCAP Loss and No Loss mode.

Syntax

```
Capture-all
No capture-all
```

Parameters

Not applicable

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

capture
capture enable
show capture

Example

The following example sets this capture to capture all packets (no loss).

```
CES(capture-ethernet)#capture-all
```

capture enable

Use this command from the console port of the gateway to globally enable packet capture on the Nortel VPN Router . When you execute this command, you must enter a password to be used only by packet capture. This password must have at least eight characters and include at least one number.



Note: You must execute this command from the console port of the gateway before you can execute other packet capture commands from the command line interface.

Use the **no** form of the command to disable packet capture globally.

Syntax

capture enable
no capture enable

Parameters

None

Default

Disabled

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Prerequisites

You must change the administrator password from its default value before you execute the **`capture enable`** command.

Warning messages

```
% Administrator password must be changed first.
% Capture already enabled.
% Error reading password!
% Packet capture must be enabled from the console port.
% Passwords do not match!
% Weak password! Please try again.
```

Related commands

capture add
capture start
capture stop
show capture

Example

The following example enables packet capture globally. The password must have at least eight characters and include at least one number.

```
CES# capture enable
Please specify password for encrypting capture files.
Password: ********
Reenter password: ********
CES#
```

The following example disables packet capture globally.

```
CES# no capture enable
CES#
```

capture save

Use this command to save captured network traffic to the specified file on the Nortel VPN Router system disk. The file is saved in encrypted form, along with the password you entered with the **`capture enable`** command.

Syntax

`capture` *<name>* **`save`** *<file-name>*

Parameters

name	Specifies the name of an existing capture object.
file-name	Specifies the name of the disk file to write network traffic to.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Prerequisites

You must stop the capture object before you can execute this command.

Warning messages

```
% Capture must not be running
% Capture buffer is empty, nothing to save
% Capture object name does not exist
```

Related commands

capture start
capture stop
clear capture
show capture

Example

The following example saves captured network traffic to the file eth-mgmt.cap on disk ide1.

```
CES# capture test save /ide1/eth-mgmt.cap
Saving capture test to file /ide1/eth-mgmt.cap please wait .
. .
112 frames written successfully.
CES#
```

capture start

Use this command to start capturing network traffic.

Syntax

capture <*name*> **start**

Parameters

name	Specifies the name of an existing capture object.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must already exist.

Warning messages

```
% Capture already running
% Capture object name does not exist
```

Related commands

capture add
capture enable
capture save
capture stop
show capture
trigger

Example

The following example starts packet capture on the gateway.

```
CES# capture test start
CES#
```

capture stop

Use this command to stop capturing network traffic.

Syntax

capture <*name*> **stop**

Parameters

name	Specifies the name of an existing capture object.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must have been started.

Warning messages

```
% Capture not running
% Capture object name does not exist
```

Related commands

capture add
capture enable
capture save
capture start
show capture
trigger

Example

The following example stops packet capture on the gateway.

```
CES# capture test stop
CES#
```

clear capture

Use this command to clear captured network traffic from the capture buffer of the specified capture object.

Syntax

clear capture <*name*>

Parameters

name	Specifies the name of an existing capture object.

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
% Capture object name does not exist
% Packet capture must be enabled from the console port
```

Related commands

capture add
capture save
capture start
capture stop
show capture
wrapping

Example

The following example clears the capture buffer of the capture object “test.”

```
CES# clear capture test
CES#
```

direction

Use this command to set the direction of the traffic to be captured. If no direction is specified, PCAP will capture both inbound and outbound traffic. Use the **no** form of the command to reset packet capture to its default behavior, that is, capture both inbound and outbound traffic.

Syntax

direction {**inbound** | **outbound**}
no direction

Parameters

inbound	Capture inbound packets only.
outbound	Capture outbound packets only.

Default

Capture both inbound and outbound traffic.

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture
filter
length
show capture
trigger
wrapping

Example

The following example configures packet capture to capture inbound traffic only.

```
CES(capture-ethernet)# direction inbound
CES(capture-ethernet)#
```

The following example configures packet capture to capture outbound traffic only.

```
CES(capture-global)# direction outbound
CES(capture-global)#
```

The following example resets packet capture to its default behavior, that is, to capture both inbound and outbound traffic.

```
CES(capture-tunnel)# no direction
CES(capture-tunnel)#
```

filepath

Use this command to set the path when saving capture files.

Syntax

filepath <path>

Parameters

path	Specifies the path for saving files.

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

capture
capture enable
show capture
maxfiles
filesize

Example

```
CES (capture-ethernet)#filepath /ide0/system/log
```

filesize

Use this command to set the size of a disk capture file.

Syntax

filesize <size>

Parameters

size	Specifies the the size of the capture file. If this is set to a value other than 0, the capture is automatically saved in a file having the format {prefix}yymmdd.{extNr}.

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

capture
capture enable
show capture
maxfiles
filepath
buffersize

Example

```
CES(capture-ethernet)#filesize 10485760
```

filter

Use this command to apply an existing interface filter to a capture object. When you apply a filter, packet capture saves to its buffer only traffic that matches the filter. A filter matches IP traffic only.

By default, if a filter is set, non-IP traffic will not be saved to the capture buffer. However, if you set the **non-ip** parameter to **accept**, all non-IP frames are captured, as well as the IP frames that match the specified filter. (The default value for the **non-ip** parameter is **deny**.)

Use the **no** form of the command to reset packet capture to its default behavior, that is, to capture all traffic.

Syntax

filter <*name*> [**non-ip** {**accept** | **deny**}]
no filter <*name*>

Parameters

name	Specifies the interface filter to apply. Enter one of the following strings: deny-all, permit-all, permit-dns-tcp, permit-dns-udp, permit-entrust-ca, permit-finger, permit-ftp, permit-http, permit-ldap, permit-nntp, permit-ntp, permit-ping, or permit-telnet. You can also enter the name of a user-created filter.
non-ip	Specify whether packet capture will save non-IP packets when it applies this filter. By default, packet capture does not save non-IP packets when you apply a filter.
accept	Specify that non-IP packets are saved in the buffer, along with the IP packets specified by the filter.
deny	Specify that non-IP packets are not saved in the buffer.

Default

Capture all traffic.

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running

Warning: VJ compression may be negotiated on this interface.
Filters will not match on any VJ compressed frames.
```

Related commands

capture
direction
length
show capture
trigger
wrapping

Example

The following example applies the interface filter “permit ping” to the capture object.

```
CES# capture serial31
CES(capture-serial)# filter “permit ping”
CES(capture-serial)#
```

The following example disables the application of the interface filter and resets packet capture to its default behavior, that is, to capture all traffic.

```
CES(capture-ethernet)# no filter
CES(capture-ethernet)#
```

length

Use this command to specify the number of octets that are captured from every packet. Use the **no** form of the command to reset the length to the default value, 4096 octets.

Syntax

length <*length*>
no length

Parameters

length	Specifies the maximum number of octets to capture from each packet. Enter a value from 64 through 4096.

Default

4096 octets

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture
direction
filter
show capture
trigger
wrapping

Example

The following example sets the number of octets to capture from every packet to 1518.

```
CES(capture-ethernet)# length 1518
CES(capture-ethernet)#
```

The following example resets the number of octets to the default value, 4096.

```
CES(capture-ethernet)# no length
CES(capture-ethernet)#
```

maxfiles

Use this command to set the maximum number of disk capture files.

Syntax

maxfiles <max>

Parameters

max	Specifies the maximum number of files that will be saved to disk for this capture.

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

None

Related commands

capture
capture enable
show capture
filesize
filepath

Example

```
CES (capture-ethernet)#maxfiles 99
```

persistent

Use this command to enable persistent mode for tunnel capture objects (persistent mode applies only to tunnels—user tunnels, branch office tunnels, and ABOTs). When persistent mode is enabled and a captured tunnel disconnects, packet capture restarts automatically when it encounters another tunnel that matches the capture criteria. Use the **no** form of the command to revert to the default behavior, that is, to stop packet capture when the tunnel disconnects.

Syntax

```
persistent enable
no persistent enable
```

Parameters

None

Default

Stop packet capture when the tunnel disconnects.

Command mode

Capture Tunnel Configuration

Next command mode

Capture Tunnel Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture add
capture start
capture stop
remoteip
show capture
type
userid

Example

The following example enables persistent mode, which enables packet capture to restart when the captured tunnel disconnects so that another tunnel matching the capture criteria can be captured immediately.

```
CES(capture-tunnel)# persistent enable
CES(capture-tunnel)#
```

The following examples resets packet capture to its default behavior, that is, capture is stopped when the captured tunnel disconnects.

```
CES(capture-tunnel)# no persistent enable
CES(capture-tunnel)#
```

promiscuous

Use this command to enable promiscuous mode for an Ethernet interface capture object (promiscuous mode applies only to Ethernet interface capture objects). When promiscuous mode is enabled, the interface card will be configured to run in promiscuous mode—that is, traffic on the interface that is *not* directed to the gateway will be captured. Use the **no** form of the command to revert to the default behavior, that is, for promiscuous mode to be disabled when capture is started.

Syntax

```
promiscuous enable
no promiscuous enable
```

Parameters

None

Default

Disabled

Command mode

Capture Ethernet Configuration

Next command mode

Capture Ethernet Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture add
capture start
capture stop
show capture

Example

The following example enables promiscuous mode for packet capture on an Ethernet interface.

```
CES(capture-ethernet)# promiscuous enable
CES(capture-ethernet)#
```

The following example disables promiscuous mode for packet capture.

```
CES(capture-ethernet)# no promiscuous enable
CES(capture-ethernet)#
```

remoteip

Use this command to specify the IP address of the remote tunnel end point for the tunnel capture object. When you execute this command, only traffic that goes through a tunnel with the specified remote tunnel end point will be captured. Use the **no** form of the command to revert to the default behavior, that is, to capture traffic from tunnels with any remote end point address.

Syntax

```
remoteip <IP-address>
no remoteip <IP-address>
```

Parameters

IP-address	Specifies the IP address of the remote tunnel end point; traffic traversing a tunnel with this remote IP address will be captured.

Default

Capture traffic from tunnels with any remote IP address.

Command mode

Capture Tunnel Configuration

Next command mode

Capture Tunnel Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture add
capture start
capture stop
persistent
show capture
type
userid

Example

The following example sets the remote IP address from which the tunnel must come for it to be captured by this capture object.

```
CES(capture-tunnel)# remoteip 192.168.200.1
CES(capture-tunnel)#
```

The following example resets packet capture to its default behavior, that is, to capture tunnels from any remote IP address.

```
CES(capture-tunnel)# no remoteip
CES(capture-tunnel)#
```

show capture

Use this command to show the status of existing capture objects.

Syntax

show capture [<*name*>]

Parameters

name	Specifies the name of an existing capture object.

Default

If no capture object name is specified, print out a summary of all capture objects.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% No capture objects found
```

Related commands

capture enable
capture save
capture start
capture stop
clear capture
show capture

Example

The following example lists and briefly describes all the capture objects configured on the gateway.

```
CES# show capture
Name        Type        Size        Utilization  Count      State
test        ETHERNET    1048576         100%     1282       BUFFER FULL
test2       ETHERNET    1048576           0%     0          EMPTY
test3       TUNNEL      1048576           0%     0          STOPPED
test4       GLOBAL      1048576          12%     232        RUNNING
```

The following example displays configuration parameters for the Fast Ethernet capture object “test.”

```
CES# show capture test
Capture state:                              BUFFER FULL
Capture buffer size:                        1048576
Capture type:                               ETHERNET
Capturing on interface:                     FastEthernet 0/1
Promiscuous mode is:                        DISABLED
Capturing MAX octets per frame:             4096
Captured frames:                            1282
Capture buffer utilization:                 100%
Capture direction:                          BIDIRECTIONAL
Capture buffer wrapping:                    DISABLED
Capture buffer wrapped:                     FALSE
Capture buffer last saved to:               /ide0/nn1
Frames saved:                               1281
CES#
```

The following example displays configuration parameters for the tunnel capture object “test3.”

```
CES# show capture test3
Capture state:                              STOPPED
Capture buffer size:                        1048576
Capture type:                               TUNNEL
Tunnel type to capture:                     IPSEC
Tunnel encapsulation to capture:            INITIATOR
Restarting capture on tunnel logoff:        DISABLED
Capturing MAX octets per frame:             4096
Captured frames:                            0
Capture buffer utilization:                 0%
Capturing direction:                        BIDIRECTIONAL
Capture buffer wrapping:                    DISABLED
Capture buffer wrapped:                     FALSE
Capture filter applied:                     permit all
Capture filter discards:                    0
Start trigger applied:                      permit all
Start trigger discards:                     0
Stop trigger applied:                       permit all
CES#
```

The following example displays configuration parameters for the global capture object “test4.”

```
CES# show capture test4
Capture state:                              RUNNING
Capture buffer size:                        1048576
Capture type:                               GLOBAL
Capturing MAX octets per frame:             4096
Captured frames:                            237
Capture buffer utilization:                 12%
Capturing direction:                        BIDIRECTIONAL
Capture buffer wrapping:                    DISABLED
Capture buffer wrapped:                     FALSE
```

trigger

Use this command to set start and stop triggers. Existing interface filters are used as start and stop triggers. By default, the system saves frames to the capture buffer as soon as capture is started.

- A start trigger causes the system to wait for a specific packet before it starts saving packets to the capture buffer (traffic encountered before the start trigger is encountered is discarded).
- A stop trigger causes the system to stop saving traffic in the capture buffer after a specific packet matching the stop trigger is encountered. Capture, however, is not fully stopped.

If you set both a start and a stop trigger, the start trigger can reenable saving traffic to a capture buffer. The use of a start and a stop trigger allows capturing specific transaction-oriented traffic. Triggers can also be used with filters to allow still greater flexibility. Use the **no** form of the command to revert to the default behavior, that is, to remove the start trigger, the stop trigger, or both.

Syntax

```
trigger {start | stop} <filter>
no trigger [start | stop]
```

Parameters

filter	Specifies the name of the interface filter to use as a start or stop trigger. Enter one of the following strings: deny-all, permit-all, permit-dns-tcp, permit-dns-udp, permit-entrust-ca, permit-finger, permit-ftp, permit-http, permit-ldap, permit-nntp, permit-ntp, permit-ping, or permit-telnet. You can also enter the name of a user-created filter.
start	Create a trigger that starts packet capture when the filter criteria are met.
stop	Create a trigger that stops packet capture when the filter criteria are met.

Default

None

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running

Warning: VJ compression may be negotiated on this interface.
Triggers will not match on any VJ compressed frames.
```

Related commands

capture
capture start
capture stop
direction
filter
length
show capture
wrapping

Example

The following example sets a start and stop trigger.

```
CES(capture-ethernet)# trigger start “permit ping”
CES(capture-ethernet)# trigger stop “permit ping”
CES(capture-ethernet)#
```

The following example removes the start trigger.

```
CES(capture-tunnel)# no trigger start
CES(capture-tunnel)#
```

The following example removes all triggers.

```
CES(capture-ethernet)# no trigger
CES(capture-ethernet)#
```

type

Use this command to specify the following criteria for tunnel capture objects:

- Type of tunnel: any type, user tunnel, branch office tunnel, or asynchronous branch office tunnel (responder side or initiator side)
- Tunneling protocol: IPsec, L2F, L2TP, or PPTP

When you execute this command, only traffic from the specified type of tunnel will be captured. Use the **no** form of the command to revert to the default behavior, that is, to capture packets that traverse tunnels of any type.

Syntax

```
type {any | initiator | peer2peer | responder | user}
{ipsec | l2f | l2tp | pptp}
no type
```

Parameters

any	Capture traffic from any type of tunnel.
initiator	Capture traffic from ABOT initiator tunnels only.
peer2peer	Capture traffic from peer-to-peer branch office tunnels only.
responder	Capture traffic from ABOT responder tunnels only.
user	Capture traffic from user tunnels only.
ipsec	Capture traffic from IPsec tunnels only.
l2f	Capture traffic from L2F tunnels only.
l2tp	Capture traffic from L2TP tunnels only.
pptp	Capture traffic from PPTP tunnels only.

Default

Capture packets from all tunnel types.

Command mode

Capture Tunnel Configuration

Next command mode

Capture Tunnel Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture add
capture start
capture stop
persistent
remoteip
show capture
userid

Example

The following example configures packet capture to capture IPsec tunnels only.

```
CES(capture-tunnel)# type any ipsec
CES(capture-tunnel)#
```

The following example configures packet capture to capture only branch office tunnels running L2TP.

```
CES(capture-tunnel)# type peer2peer l2tp
CES(capture-tunnel)#
```

The following example configures packet capture to capture all types of tunnels.

```
CES(capture-tunnel)# no type
CES(capture-tunnel)#
```

userid

Use this command to specify the user name as the criterion that a tunnel capture object will use to capture packets. (For types of tunnels that do not have a user name, other information is used instead, for example, peer IP address for branch office tunnels.) When you execute this command, only traffic that goes through tunnels with the specified user name will be captured. Use the **no** form of the command to revert to the default behavior, that is, to capture traffic from tunnels with any user name.

Syntax

```
userid <name>
no userid
```

Parameters

name	Specifies the user name or other information for the tunnels.

Default

Capture tunnels with any user name.

Command mode

Capture Tunnel Configuration

Next command mode

Capture Tunnel Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture add
capture start
capture stop
persistent
remoteip
show capture
type

Example

The following example configures packet capture to capture only tunnels with the user ID set to “test.”

```
CES(capture-tunnel)# userid test
CES(capture-tunnel)#
```

The following example configures packet capture to capture packets from all tunnels, regardless of user ID.

```
CES(capture-tunnel)# no userid
CES(capture-tunnel)#
```

wrapping

Use this command to allow the capture buffer to wrap when it fills up. By default, packet capture stops when the buffer fills up. If you execute this command, the oldest captured datagrams are discarded and new ones are saved in their place. With wrapping enabled, packet capture can run indefinitely regardless of the capture buffer size. Use the **no** form of the command to revert to the default behavior, that is, to stop capturing packets when the buffer is full.

Syntax

```
wrapping enable
no wrapping enable
```

Parameters

None

Default

Stop capturing when buffer is full.

Command mode

Capture Configuration

Next command mode

Capture Configuration

Required privileges

System Management - Manage
User Management - None

Prerequisites

The capture object must be stopped before you can execute this command.

Warning messages

```
% Capture must not be running
```

Related commands

capture
capture add
direction
filter
length
show capture
trigger
wrapping

Example

The following example enables the capture buffer to wrap when it gets full.

```
CES(capture-ethernet)# wrapping enable
CES(capture-ethernet)#
```

The following example disables wrapping; that is, packet capture stops when the buffer is full.

```
CES(capture-ethernet)# no wrapping enable
CES(capture-ethernet)#
```

Chapter 46
Quality of service (QoS) commands

This chapter describes the quality of service (QoS) commands that you can use to configure the Nortel VPN Router.

Command	Page
add-rule	1789
destination-address	1790
diffserv-marking	1792
dscp-values	1794
move-rule	1795
protocol	1797
qos admission-control	1799
qos bandwidth-management	1801
qos bandwidth-rates	1802
qos egress-dscp-map enable	1804
qos egress-queuing-mode	1806
qos egress-traffic-conditioning	1808
qos ingress-dscp-map enable	1810
qos ingress-traffic-conditioning	1812
qos mf-class (Interface Configuration)	1815
qos mf-class (Global Configuration)	1817
qos mf-class add	1818
qos mf-class enable	1820
qos mf-class rule	1821
qos mf-class rule add	1823

Command	Page
qos non-tunnel-traffic-ratio	1824
qos over-subscription-ratio	1827
qos shaping	1829
qos shaping-state enable	1831
qos statistics reset	1832
qos traffic-conditioning enable	1834
remove-rule	1836
show qos admission-control	1837
show qos bandwidth-management	1838
show qos bandwidth-rates	1840
show qos interfaces	1841
show qos mf-class	1843
show qos statistics	1845
show rules	1849
source-address	1850
tcp-udp-destination-port	1852
tcp-udp-source-port	1855
use destination_address	1857
use diffserv_marking	1858
use dscp	1860
use protocol	1862
use source_address	1864
use tcp_udp_destination_port	1866
use tcp_udp_source_port	1868

add-rule

Use this command to associate a rule with an MF classifier. The rule must already exist before you can associate it with an MF classifier.

Syntax

add-rule <*rule-name*>

Parameters

rule-name	Specifies the name of the rule to add.

Default

None

Command mode

MF Class Configuration

Next command mode

MF Class Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% Rule <rule-name> does not exist
% Rule <rule-name> exists for this classifier set
```

Related commands

```
move-rule
qos mf-class rule
remove-rule
show rules
```

Example

The following example shows how to add a rule called “rule1” to the MF classifier named “gold.”

```
CES(config)# qos mf-class gold
CES(config-mfclass)# add-rule rule1
CES(config-mfclass)# exit
CES(config)#
```

The following example shows how to delete rule1 from the MF classifier named silver.

```
CES(config)# qos mf-class silver
CES(config-mfclass)# remove-rule rule1
CES(config-mfclass)# exit
CES(config)#
```

destination-address

Use this command to configure specific destination addresses for the specified rule. The destination is relative to the direction of the rule. Use the **no** form of the command to delete the destination address from the list.

Syntax

destination-address <*name*> **ip** <*IP_address*> **mask** <*net_mask*>
no destination-address <*name*>

Parameters

name	Specifies a name for this destination.
IP_address	Specifies the destination IP address for the rule in dotted-decimal notation.
net_mask	Specifies the subnet mask for the specified IP address in dotted-decimal notation.

Default

None

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

diffserv-marking
dscp-values
protocol
qos mf-class rule
source-address
tcp-udp-destination-port
tcp-udp-source-port
use destination_address

Example

The following example configures a destination address for rule1.

```
CES(config)# qos mf-class rule rule1
CES(config-mfrule)# destination-address London ip
141.21.10.183 mask 255.255.255.255
CES(config-mfrule)# exit
CES(config)#
```

The following example deletes a destination address from rule4.

```
CES(config)# qos mf-class rule rule4
CES(config-mfrule)# no destination-address London
CES(config-mfrule)# exit
CES(config)#
```

diffserv-marking

Use this command to select the DSCP that this rule applies to data, either EF (expedited forwarding) or an AF (assured forwarding) level. The DiffServ code point (DSCP) is always copied into tunnel headers.

Syntax

diffserv-marking {**EF** | **AF1** | **AF2** | **AF3** | **AF4**}

Parameters

EF	Specifies expedited forwarding, that is, premium service class.
AF1	Specifies assured forwarding level 1, that is, bronze service class.
AF2	Specifies assured forwarding level 2, that is, silver service class.
AF3	Specifies assured forwarding level 3, that is, gold service class.
AF4	Specifies assured forwarding level 4, that is, platinum service class.

Default

Expedited forwarding (EF)

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

destination-address
dscp-values
protocol
qos mf-class rule
source-address
tcp-udp-destination-port
tcp-udp-source-port
use diffserv_marking

Example

The following example configures DiffServ marking for rule1 as AF2 (assured forwarding level 2).

```
CES(config)# qos mf-class rule rule1
CES(config-mfrule)# diffserv-marking AF2
CES(config-mfrule)# exit
CES(config)#
```

dscp-values

Use this command to configure new DSCP values for rules. (To see the existing DSCP values, enter the **show dscps** command.) The DSCP value and mask assignments allow packets that are already marked to retain their settings or to be re-marked based on their previous DSCP value. This is an input criterion.

Syntax

dscp-value <*dscp_name*> **value** <*dscp_value*> **mask** <*dscp_mask*>

Parameters

To see the already configured DSCP values, see Table 12 on page 1860.

dscp_name	Specifies the name for the new DSCP value. This name will be used with the **use dscp** command.
dscp_value	Specifies the numeric value for the new DSCP value.
dscp_mask	Specifies the mask for the new DSCP value.

Default

None

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

destination-address
protocol
qos mf-class rule
source-address
tcp-udp-destination-port
tcp-udp-source-port
use dscp

Example

The following example sets the current DSCP value to AF3LowDrop.

```
CES(config)# qos mf-class rule1
CES(config-qos-rule)# dscp-value NewDscp 80 63
CES(config-qos-rule)#
```

move-rule

Use this command to move a rule within an MF class. Use the keywords **up** and **down** to move the rule within the selected MF class rule execution list.

Syntax

move-rule <*rule-name*> {**up** | **down**}

Parameters

rule-name	Specifies the name of the rule to move.
up	Move this rule before the previous rule in the classifier execution list.
down	Move this rule after the following rule in the classifier execution list.

Default

None

Command mode

MF Class Configuration

Next command mode

MF Class Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

add-rule
qos mf-class rule
remove-rule
show rules

Example

The following example moves rule1 up in the ordered list of rule executions of MF classifier gold.

```
CES(config)# qos mf-class gold
CES(config-mfclass)# move-rule rule1 up
CES(config-mfclass)# exit
CES(config)#
```

The following example moves rule1 down in the ordered list of rule executions of MF classifier gold.

```
CES(config)# qos mf-class gold
CES(config-mfclass)# move-rule rule1 down
CES(config-mfclass)# exit
CES(config)#
```

protocol

QoS rules can include a protocol criterion that references the 1-byte protocol number field in an IP packet header. IP, ICMP, TCP, and UDP are already configured on the gateway. (To see the list of protocols, enter the **show protocols** command in QoS Rule Configuration mode.)

Use this command to configure additional protocols to be used with one or more QoS rules. Use the **no** form of the command to remove a protocol from the list.

To obtain the most recent list of the numeric values assigned to various protocols, see the Internet Assigned Numbers Authority (IANA) Web site at:

http://www.iana.org/assignments/protocol-numbers

Syntax

protocol *<protocol_name> <protocol_number>*
no protocol *<protocol_name>*

Parameters

protocol_name	Specifies the name of the protocol that you want to make available for use with rules. After you configure the protocol, you can assign it to a particular rule using the **use protocol** command.
protocol_number	Specifies the 1-byte protocol number field in an IP packet header. For the list of numeric values assigned to protocols, see the IANA Web site at: http://www.iana.org/assignments/protocol-numbers

Default

IP

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

destination-address
diffserv-marking
dscp-values
qos mf-class rule
source-address
tcp-udp-destination-port
tcp-udp-source-port
use protocol

Example

The following example configures L2TP for use with rules and then assigns L2TP as a protocol criterion to rule1.

```
CES(config)# qos mf-class rule rule1
CES(config-mfrule)# protocol l2tp 115
CES(config-mfrule)# use protocol l2tp
```

The following example removes L2TP from the list of protocols that can be used with rules.

```
CES(config)# qos mf-class rule rule1
CES(config-mfrule)# no protocol l2tp
CES(config-mfrule)# exit
CES(config)#
```

qos admission-control

Admission control is a traffic control function that determines whether the gateway can supply the requested bandwidth and CPU resources of a new session while continuing to provide the bandwidth and CPU resources requested by previously admitted sessions. Admission control is used in conjunction with bandwidth policies to limit the number of concurrent user and branch tunnels.

Use this command to enable admission control. Use the **no** form of the command to disable admission control.

Syntax

```
qos admission-control enable
no qos admission-control enable
```

Parameters

None

Default

Disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos bandwidth-management
show qos admission-control
show qos bandwidth-management

Example

The following example enables admission control for all interfaces on the gateway.

```
CES(config)# qos admission-control enable
CES(config)#
```

The following example disables admission control for all interfaces on the gateway.

```
CES(config)# no qos admission-control enable
CES(config)#
```

qos bandwidth-management

Bandwidth management lets you manage CPU and interface bandwidth resources to ensure that tunneled sessions receive predictable and adequate levels of service.

Use this command to enable bandwidth management for the gateway as a whole. Use the **no** form of the command to disable bandwidth management.

Syntax

```
qos bandwidth-management enable
no qos bandwidth-management enable
```

Parameters

None

Default

disabled

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos admission-control
show qos admission-control
show qos bandwidth-management

Example

The following example enables bandwidth management for all interfaces on the gateway.

```
CES(config)# qos bandwidth-management enable
CES(config)#
```

The following example disables bandwidth management for all interfaces on the gateway.

```
CES(config)# no qos bandwidth-management enable
CES(config)#
```

qos bandwidth-rates

Use this command to add a new bandwidth rate (in bits per second) to the list of current bandwidth rates. Use the **no** form of the command to remove a bandwidth rate from the list of bandwidth rates.

Syntax

qos bandwidth-rates <*bw_value*>
no qos bandwidth-rates <*bw_value*>

Parameters

bw_value	Specifies the new bandwidth rate in bits/s. You can enter a value from 0 through 100000000.

Default

Default available bandwidth rate values are 14.4 Kb/s, 28.8 Kb/s, 56 Kb/s, 128 Kb/s, 256 Kb/s, 512 Kb/s, 1000 Kb/s, and 5000 Kb/s.

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

show qos bandwidth-rates

Example

The following example configures a new bandwidth rate of 64 Kb/s.

```
CES(config)# qos bandwidth-rates 64000
CES(config)#
```

The following example deletes the bandwidth rate 14.4 Kb/s.

```
CES(config)# no qos bandwidth-rates 14400
CES(config)#
```

qos egress-dscp-map enable

Use this command to enable the mapping of the DiffServ code point (DSCP) to 802.1p marking for packets that are exiting an interface. Use the **no** form of the command to disable DSCP-to-802.1p mapping.

Syntax

```
qos egress-dscp-map enable
no qos egress-dscp-map enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example enables the mapping of a DSCP to an 802.1p marking for packets that egress interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# qos egress-dscp-map enable
CES(config-if)#
```

The following example disables the mapping of a DSCP to an 802.1p marking for packets that egress interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no qos egress-dscp-map enable
CES(config-if)#
```

qos egress-queuing-mode

Use this command to select egress queuing mode settings for the selected physical interface.

Syntax

```
qos egress-queuing-mode {ds-phb | legacy}
```

Parameters

ds-phb	Specify DiffServ per-hop behavior as the egress queuing mode for the selected physical interface.
legacy	Specify legacy forwarding priority as the egress queuing mode for the selected physical interface. This setting provides backward compatibility for earlier Nortel VPN Router software versions.

Default

legacy

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example configures DiffServ per-hop egress behavior on interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# qos egress-queuing-mode ds-phb
CES(config-if)#
```

The following example configures legacy egress behavior on interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# qos egress-queuing-mode legacy
CES(config-if)#
```

qos egress-traffic-conditioning

Use this command to configure egress (outbound) traffic conditioning parameters of DiffServ edge settings for a selected physical interface. You can specify a value from 0 through 4294967295. Use the **no** form of the command to reset the egress traffic conditioning parameters to 0.

Syntax

qos egress-traffic-conditioning {**ef-shaping-rate** <*efs-rate*>}
no qos egress-traffic-conditioning

Parameters

efs-rate	Specifies the expedited forwarding rate in bits/s.

Default

0

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example configures egress traffic conditioning for interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# qos egress-traffic-conditioning
ef-shaping-rate 64000
CES(config-if)#
```

The following example resets all egress traffic conditioning settings for interface 2/1 to the default value, 0.

```
CES(config)# interface serial 2/1
CES(config-if)# no qos egress-traffic-conditioning
  Egress Expedited Traffic shaping reset to default, 0 bps.
CES(config-if)#
```

qos ingress-dscp-map enable

Use this command to enable the mapping of 802.1p marking to the DiffServ code point (DSCP) for packets that are arriving on an interface. Use the **no** form of the command to disable 802.1p-to-DSCP mapping.

Syntax

```
qos ingress-dscp-map enable
no qos ingress-dscp-map enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example enables the mapping of a DSCP to an 802.1p marking for packets that arrive on interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# qos ingress-dscp-map enable
CES(config-if)#
```

The following example disables the mapping of a DSCP to an 802.1p marking for packets that arrive on interface 2/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no qos ingress-dscp-map enable
CES(config-if)#
```

qos ingress-traffic-conditioning

Use this command to configure ingress (inbound) traffic conditioning parameters for a selected physical interface. For each parameter, you can specify a value from 0 through 4294967295. Use the **no** form of the command to reset one or more of the ingress traffic conditioning parameters to 0.

Syntax

```
qos ingress-traffic-conditioning {[EF <ef-rate>]
[AF1 <rate1>] [AF2 <rate2>] [AF3 <rate3>] [AF4 <rate4>]
[BE <be-rate>]}

qos ingress-traffic-conditioning {AF1 | AF2 | AF3 | AF4}
<bps> action {drop | mark}

no qos ingress-traffic-conditioning [[EF] [AF1] [AF2] [AF3]
[AF4] [BE]]
```

Parameters

EF	Specify the expedited forwarding rate in bits/s.
AF1	Specify the assured forwarding 1 rate in bits/s.
AF2	Specify the assured forwarding 2 rate in bits/s.
AF3	Specify the assured forwarding 3 rate in bits/s.
AF4	Specify the assured forwarding 4 rate in bits/s.
BE	Specify the best effort rate in bits/s.
action	Specify the action to take (drop or mark) if ingress traffic matching an AF classifier exceeds the configured rate. The default action is to mark the traffic.
drop	Specify that the gateway drop ingress traffic matching an AF classifier that exceeds the configured rate.
mark	Specify that the gateway mark ingress traffic matching an AF classifier that exceeds the configured rate.

Default

0 bit/s; default action is mark.

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example configures ingress traffic conditioning for interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# qos ingress-traffic-conditioning EF 64000
AF1 28800 AF2 19200 AF3 19200 AF4 9600
```

The following example configures traffic matching AF1 that exceeds 28800 bits/s to be dropped.

```
CES(config-if)# qos ingress-traffic-conditioning af1 28800
action drop
CES(config-if)#
```

The following example configures ingress traffic conditioning settings for interface 2/1:

```
CES(config-if)# qos ingress-traffic-conditioning af2 56000
CES(config-if)# qos ingress-traffic-conditioning af3 19200
action mark
CES(config-if)# qos ingress-traffic-conditioning af4 9600
action drop
CES(config-if)#
```

The following example resets AF1 to 0.

```
CES(config-if)# no qos ingress-traffic-conditioning af1
  AF1 ingress traffic conditioning parameters reset to
default, 0 bps.
CES(config-if)#
```

The following example resets all ingress traffic conditioning settings for interface 2/1 to their default values (0).

```
CES(config-if)# no qos ingress-traffic-conditioning
  All ingress traffic conditioning parameters reset to
default, 0 bps.
CES(config-if)#
```

qos mf-class (Interface Configuration)

Use this command to assign, change, or delete MF classifier names for the selected physical interface. Use the **no** form of the command to reset the interface MF classifier mapping to the global list of mappings.

Syntax

```
qos mf-class {[ingress-mf-class <name1>] [egress-mf-class
<name2>]}
no qos mf-class {[ingress-mf-class] [egress-mf-class]}
```

Parameters

ingress-mf-class *<name1>*	Specifies the name of an existing MF classifier that you want to apply to inbound packets that arrive at this interface.
egress-mf-class *<name2>*	Specifies the name of an existing MF classifier that you want to apply to outbound packets that leave this interface.

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example configures MF class mappings for interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# qos mf-class ingress-mf-class gold
CES(config-if)# qos mf-class egress-mf-class silver
CES(config-if)#
```

The following example deletes MF class mappings from the interface.

```
CES(config)# interface serial 2/1
CES(config-if)# no qos mf-class ingress-mf-class
egress-mf-class
CES(config-if)#
```

qos mf-class (Global Configuration)

Use this command to edit the definition of an existing MF classifier created with the **qos mf-class add** command. This command navigates to MF Class Configuration mode. Use the **no** form of the command to delete an MF classifier.

Syntax

qos mf-class *<mf-class-name>*
no qos mf-class *<mf-class-name>*

Parameters

mf-class-name	Specifies the name of the MF classifier.

Default

None

Command mode

Global Configuration

Next command mode

MF Class Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos mf-class add
qos mf-class rule
show qos mf-class

Example

The following example shows how to navigate to an existing MF classifier named "gold." At this prompt, you can edit the classifier definition.

```
CES(config)# qos mf-class gold
CES(config-mfclass)# exit
CES(config)#
```

The following example deletes an MF classifier named "silver."

```
CES(config)# no qos mf-class silver
   Mf-class silver deleted
CES(config)#
```

qos mf-class add

Use this command to create QoS classifiers to be applied to one or more interfaces. You can create multiple classifiers. A multifield (MF) classifier can contain multiple rules.

Syntax

qos mf-class add *<mf-class-name>*

Parameters

mf-class-name	Specifies the name of the MF classifier.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management – Manage
User Management – None

Related commands

qos mf-class
qos mf-class rule
show qos mf-class

Example

The following example creates an MF class named “gold.”

```
CES(config)# qos mf-class add gold
   Mf-class gold created
CES(config)#
```

qos mf-class enable

Use this command to enable or disable the use of the multifield classifier for an interface. Use the **no** form of the command to disable DiffServ on this interface.

Syntax

```
qos mf-class enable
no qos mf-class enable
```

Parameters

None

Default

disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management – None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example enables the inbound classifier “gold” on interface card 2, port 1 and the outbound classifier “silver” on the same interface.

```
CES(config)# interface serial 2/1
CES(config-if)# qos mf-class ingress-mf-class gold
egress-mf-class silver
CES(config-if)# qos mf-class enable
CES(config-if)#
```

The following example disables the use of classifiers on interface card 2, port 1.

```
CES(config)# interface serial 2/1
CES(config-if)# no qos mf-class enable
CES(config)#
```

qos mf-class rule

Use this command to modify an existing QoS rule. When you enter the command, you enter QoS Rule Configuration mode. Use the **no** form of the command to delete a QoS rule.

Syntax

```
qos mf-class rule <rule-name>
no qos mf-class rule <rule-name>
```

Parameters

rule-name	Specifies the name of the rule to modify or delete.

Default

None

Command mode

Global Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

destination-address
diffserv-marking
dscp-values
protocol
source-address
tcp-udp-destination-port
tcp-udp-source-port

Example

The following example opens a rule named “rule1.”

```
CES(config)# qos mf-class rule rule1
CES(config-mfrule)# exit
CES(config)#
```

The following example deletes a rule named “rule4.”

```
CES(config)# no qos mf-class rule rule4
   Rule rule1 deleted
CES(config)#
```

qos mf-class rule add

Use this command to create a QoS rule to be applied against one or more MF classifiers. Multiple rules can be created and applied against multiple MF classifiers.

Syntax

qos mf-class rule add <*rule-name*>

Parameters

rule-name	Specifies the name of the rule to add.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management – None

Related commands

add-rule
move-rule
qos mf-class
remove-rule
show rules

Example

The following example creates a rule named “rule1.”

```
CES(config)# qos mf-class rule add rule1
   Rule rule1 created
CES(config)#
```

qos non-tunnel-traffic-ratio

Use this command to configure the percentage of bandwidth on the interface that can be reserved for non-tunnel traffic. Enter a value from 0 through 100. Use the **no** form of the command to set the value to 90 (the default value).

Syntax

qos non-tunnel-traffic-ratio *<percentage>*
no qos non-tunnel-traffic-ratio

Parameters

percentage	Specifies the percentage of bandwidth on the interface that can be reserved for non-tunnel traffic. Enter a value from 0 through 100. The **no** form of the command sets the value to 90.

Default

90%

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example configures the non-tunnel traffic ratio for interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# qos non-tunnel-traffic-ratio 20
```

The following example resets the non-tunnel traffic ratio for interface 2/1 to its default value, that is, 90%.

```
CES(config)# interface serial 2/1
CES(config-if)# no qos non-tunnel-traffic-ratio
  Non-tunnel-traffic-ratio reset to default value, 90%
```

qos over-subscription-ratio

Use this command to configure bandwidth management settings for the selected physical interface. Enter a value from 1 through 42 that specifies for the interface how much of its bandwidth to oversubscribe.

For example, if you set the oversubscription ratio to a value of 5 (5:1 ratio) for a 1 Mb T1 interface, the gateway allows connections up to 5 Mb of total guaranteed bandwidth on the interface. Use the **no** form of the command to reset the ratio to its default value, 10.

Syntax

```
qos over-subscription-ratio <ratio>
no qos over-subscription-ratio
```

Parameters

ratio	Specifies a ratio (*n*:1) that represents how much of the bandwidth on the interface to oversubscribe. Enter a value from 1 through 42. The **no** form of the command sets the value to 10.

Default

10

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management – None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos shaping
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example sets the oversubscription ratio to 5:1 for interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# qos over-subscription-ratio 5
```

The following example resets the oversubscription ratio for interface 2/1 to the default value, 10.

```
CES(config)# interface serial 2/1
CES(config-if)# no qos over-subscription-ratio
  Over-subscription-ratio reset to default value, 10:1
```

qos shaping

Use this command to configure traffic shaping settings for the selected physical interface. Enter a value in bit/s for interface shaping. This value is used to shape (delay) the outgoing packet flow through an interface to better match the throughput of a downstream device. Nonconforming traffic is delayed, not dropped. Interface shaping is bypassed for EF traffic. Use the **no** form of the command to set the value to 0.

Syntax

qos shaping <*is-value*>
no qos shaping

Parameters

is_value	Specifies the delay (in bits/s) used for interface shaping. Enter a value from 0 through 4294967295. The **no** form of the command sets the value to 0.

Default

0

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example sets the traffic shaping rate for interface 2/1 to 64000 bits/s.

```
CES(config)# interface serial 2/1
CES(config-if)# qos shaping 64000
CES(config-if)#
```

The following example resets the traffic shaping rate for interface 2/1 to 0.

```
CES(config)# interface serial 2/1
CES(config-if)# no qos shaping
CES(config-if)#
```

qos shaping-state enable

Use this command to enable interface shaping for this physical interface. Use the **no** form of the command to disable interface shaping.

Syntax

```
qos shaping-state enable
no qos shaping-state enable
```

Parameters

None

Default

Disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos statistics reset
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example enables traffic shaping for interface 3/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# qos shaping-state enable
```

The following example disables traffic shaping for interface 3/1.

```
CES(config)# interface fastethernet 2/1
CES(config-if)# no qos shaping-state enable
  Interface shaping-state disabled
```

qos statistics reset

Use this command to reset all QoS counters on a selected interface.

Syntax

qos statistics reset

Parameters

None

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos traffic-conditioning enable
show qos interface
show qos statistics

Example

The following example resets all QoS counters on serial interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# qos statistics reset
CES(config-if)#
```

qos traffic-conditioning enable

Use this command to enable traffic conditioning for DiffServ on each port. Use the **no** form of the command to disable traffic conditioning on the interface.

Syntax

```
qos traffic-conditioning enable
no qos traffic-conditioning enable
```

Parameters

None

Default

disabled

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos statistics reset
show qos interface
show qos statistics

Example

The following example enables traffic conditioning on interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# qos traffic-conditioning enable
CES(config-if)#
```

The following example disables traffic conditioning on interface 2/1.

```
CES(config)# interface serial 2/1
CES(config-if)# no qos traffic-conditioning enable
CES(config-if)#
```

remove-rule

Use this command to delete a rule from the definition of an MF classifier.

Syntax

remove-rule <*rule-name*>

Parameters

rule-name	Specifies the name of the rule to delete.

Default

None

Command mode

MF Class Configuration

Next command mode

MF Class Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

% Rule <*rule-name*> does not exist in this classifier set

Related commands

add-rule
move-rule
qos mf-class rule
show rules

Example

The following example shows how to add a rule called “rule1” to the MF classifier named “gold” and then how to delete the rule from the classifier.

```
CES(config)# qos mf-class gold
CES(config-mfclass)# add-rule rule1
CES(config-mfclass)# show rules
   1 : rule1
CES(config-mfclass)# remove-rule rule1
CES(config-mfclass)# show rules
CES(config-mfclass)# exit
CES(config)#
```

show qos admission-control

Use this command to display the status of admission control (enabled or disabled).

Syntax

show qos admission control

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

qos admission-control
qos bandwidth-management
show qos bandwidth-management

Example

The following example displays the status of admission control.

```
CES# show qos admission-control
Admission Control : Enabled
CES#
```

show qos bandwidth-management

Use this command to display the status of bandwidth management (enabled or disabled).

Syntax

show qos bandwidth-management

Parameters

None

Default

None

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

qos admission-control
qos bandwidth-management
show qos admission-control

Example

The following example displays the status of bandwidth management.

```
CES# show qos bandwidth-management
Bandwidth Management : Disabled
CES#
```

show qos bandwidth-rates

Use this command to display the list of bandwidth rates.

Syntax

show qos bandwidth-rates

Parameters

None

Default

Default available bandwidth rate values are 14.4 Kb/s, 28.8 Kb/s, 56 Kb/s, 128 Kb/s, 256 Kb/s, 512 Kb/s, 1000 Kb/s, and 5000 Kb/s.

Command mode

Privileged EXEC

Next command mode

Privileged EXEC

Required privileges

System Management - Manage
User Management - None

Related commands

qos bandwidth-rates

Example

The following example displays the currently available bandwidth rates.

```
CES# show qos bandwidth-rates
The available bandwidth rates are 14400, 28800, 56000,
128000, 256000, 512000, 1000000, and 5000000 bps.
CES#
```

show qos interfaces

Use this command to display QoS configuration information for an interface.

Syntax

show qos interfaces

Parameters

None

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos statistics

Example

```
CES(config-if)# show qos interfaces
FastEthernet Interface 2/1 QOS Configuration
  Interface Shaping State    :    Disabled
  Shaping Rate               :    0
  Over-Subscription Ratio    :    10:1
  Non-Tunnel Traffic Rating  :    Default
  Multi-Field Classifier     :    Disabled
  Ingress (Inbound) Multi-Field Classifier:    None
  Ingress (Inbound) Multi-Field Classifier:    None
  Traffic Conditioning       :    Disabled
  Expedited Forwarding Rate  :    0
  Assured Forwarding 1 Rate  :    0
  Assured Forwarding 2 Rate  :    0
  Assured Forwarding 3 Rate  :    0
  Assured Forwarding 4 Rate  :    0
  Best Effort Forwarding Rate:    2880154539
  Queuing Mode               :    Legacy Forwarding Priority
  dscp-802.1p ingress mapping:    Disabled
  dscp-802.1p egress mapping :    Disabled
CES(config-if)#
```

show qos mf-class

Use this command to display the list of MF classifiers.

Syntax

show qos mf-class {<*mf-class-name*> | **rule** [<*rule-name*>]}

Parameters

mf-class-name	Specifies the name of the MF classifier to display information about.
rule-name	Specifies the name of a specific rule to display information about.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos mf-class
qos mf-class add
qos mf-class rule

Example

The following example displays the list of MF classifiers.

```
CES(config)# show qos mf-class
  mf-classifiers: gold, silver, bronze
CES(config)#
```

The following example displays the list of MF rules.

```
CES(config)# show qos mf-class rule
   1  :  rule1
   2  :  rule2
   3  :  rule3
CES(config)#
```

The following example displays information about the rule “rule2.”

```
CES(config)# show qos mf-class rule rule2
Rule: myrule
  dscps              : AF2LowDrop
  diffserv_marking   : AF2
  Protocol           : icmp
  Source Port        : gopher
  Destination Port   : gopher
  Source Address     : HttpServer
  Destination Address: HttpServer
CES(config)#
```

show qos statistics

Use this command to display operational statistics for the interface.

Syntax

show qos statistics

Parameters

None

Default

None

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos egress-dscp-map enable
qos egress-queuing-mode
qos egress-traffic-conditioning
qos ingress-dscp-map enable
qos ingress-traffic-conditioning
qos mf-class
qos mf-class enable
qos non-tunnel-traffic-ratio
qos over-subscription-ratio
qos shaping
qos shaping-state enable
qos statistics reset
qos traffic-conditioning enable
show qos interface

Example

```
          CES(config-if)# show qos statistics
          Date:  07/27/2001  Time: 09:58:14

       Interface QoS Statistics:

       Private:  LAN: Line Speed=100000000 bps

       Interface Admission Control: (Disabled)
       Over-Subscription Ratio = 10
       IP Address      Bandwidth: Used Total (bps)   Session: Active
Pending Denied
       -----------     ---------------------------
------------------------------
      10.0.8.210                 0  100000000            0      0
0

       Tunnel Traffic Meter: (Disabled)
       Committed Rate:                 10000000 bps
       Excess Rate:                    20000000 bps
       Excess Action:                  mark
       Below Committed Rate:           0 bytes
       Between Committed & Excess Rate: 0 bytes
       Above Excess Rate:              0 bytes


       Non-Tunnel Traffic Meter: (Disabled)
       Committed Rate:                 90000000 bps
       Excess Rate:                    180000000 bps
       Excess Action:                  mark
       Below Committed Rate:           0 bytes
       Between Committed & Excess Rate: 0 bytes
       Above Excess Rate:              0 bytes


       Interface Linespeed = 100000000
       Queue1:
       pktReceived=0, octReceived=0, overlimit = 0, currentQ=0
       Configured shaping rate=5000000 Actual shaping rate = 4999680
       Queue2:
       pktReceived=0, octReceived=0, overlimit = 0, currentQ=0
       Configured shaping rate=10000000 Actual shaping rate = 9999840
       Queue3:
```

```
        pktReceived=0, octReceived=0, overlimit = 0, currentQ=0
        pktDropped=0, octDropped=0 , pktOverLimit=0
        bwmRedPkt    (received=0, dropped=0)
        bwmYellowPkt (received=0, dropped=0)
        bwmGreenPkt  (received=0, dropped=0)
        avgQ = 0
        Queue4(Highest Priority):
        pktReceived=0, octReceived=0, overlimit = 0, currentQ=0
        pktDropped=0, octDropped=0 , pktOverLimit=0
        bwmRedPkt    (received=0, dropped=0)
        bwmYellowPkt (received=0, dropped=0)
        bwmGreenPkt  (received=0, dropped=0)
        avgQ = 0
        Queue5(High Priority):
        pktReceived=0, octReceived=0, overlimit = 0, currentQ=0
        pktDropped=0, octDropped=0 , pktOverLimit=0
        bwmRedPkt    (received=0, dropped=0)
        bwmYellowPkt (received=0, dropped=0)
        bwmGreenPkt  (received=0, dropped=0)
        avgQ = 0
        Queue6(Medium Priority):
        pktReceived=0, octReceived=0, overlimit = 0, currentQ=0
        pktDropped=0, octDropped=0 , pktOverLimit=0
        bwmRedPkt    (received=0, dropped=0)
        bwmYellowPkt (received=0, dropped=0)
        bwmGreenPkt  (received=0, dropped=0)
        avgQ = 0
        Queue7(Low Priority)
        pktReceived=340, octReceived=128566, overlimit = 0, currentQ=0
        pktDropped=0, octDropped=0 , pktOverLimit=0
        bwmRedPkt    (received=0, dropped=0)
        bwmYellowPkt (received=0, dropped=0)
        bwmGreenPkt  (received=340, dropped=0)
        avgQ = 0
        Queue8(Unused):
        pktReceived=0, octReceived=0, overlimit = 0, currentQ=0
        pktDropped=0, octDropped=0 , pktOverLimit=0
        bwmRedPkt    (received=0, dropped=0)
        bwmYellowPkt (received=0, dropped=0)
        bwmGreenPkt  (received=0, dropped=0)
        avgQ = 0
CES(config)#
```

show rules

Use this command to print an ordered list of execution rules within an MF class. The rules are printed in the order of execution. To move a rule up or down the execution list, use the **move-rule** command.

Syntax

show rules

Parameters

None

Default

None

Command mode

MF Class Configuration

Next command mode

MF Class Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

add-rule
move-rule
qos mf-class rule
remove-rule

Example

The following example displays the ordered list of rules within the MF classifier named gold.

```
CES(config)# qos mf-class gold
CES(config-mfclass)# show rules
  rule1, rule2, rule14, rule3, rule9
CES(config-mfclass)# exit
CES(config)#
```

The rules are displayed in the order of execution. To move a rule up or down the execution list, use the **move-rule** command.

source-address

Use this command to configure specific source addresses for the specified rule. The source is relative to the direction of the rule. Use the **no** form of the command to delete the source address from the list.

Syntax

source-address <*name*> **ip** <*IP_address*> **mask** <*net_mask*>
no source-address <*name*>

Parameters

name	Specifies a name for this source.
IP_address	Specifies the source IP address for the rule in dotted-decimal notation.
net_mask	Specifies the subnet mask for the source IP address in dotted-decimal notation.

Default

None

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

destination-address
diffserv-marking
dscp-values
protocol
qos mf-class rule
tcp-udp-destination-port
tcp-udp-source-port
use source_address

Example

The following example configures a source address for rule1.

```
CES(config)# qos mf-class rule rule1
CES(config-mfrule)# source-address Beijing ip 141.21.10.171
mask 255.255.255.255
CES(config-mfrule)# exit
CES(config)#
```

The following example deletes a source address from rule1.

```
CES(config)# qos mf-class rule rule1
CES(config-mfrule)# no source-address Beijing
CES(config-mfrule)# exit
CES(config)#
```

tcp-udp-destination-port

Use this command to filter packets according to one or more TCP or UDP destination ports. With this command, you can configure the gateway to transfer or drop packets based on the value of the TCP/UDP destination port field. The destination is relative to the direction of the rule. (To see the existing DSCP values, enter the **show tcp_udp_destination_port** command.) Use the **no** form of the command to remove the destination port from the list of ports.

Syntax

tcp-udp-destination-port <*port-name*> <*port-address*>
no tcp-udp-destination-port <*port-name*>

Parameters

Enter any of the following value pairs with the **`tcp-udp-destination-port`** command (Table 11). You can also specify other protocol-port combinations not in this list. For the list of well-known ports, see http://www.iana.org/assignments/port-numbers.

Table 11 TCP/UDP port names and addresses

Port name	Port addresses	Port name	Port addresses
any	0	nntp	119
dns	53	ntp	123
dynamic-port-begin	1023	pcANYWHERE/data	5631
entrust-ca	709	pcANYWHERE/stat	5631
finger	79	pop2	109
ftp	21	pop3	110
ftp-data	20	portmap	111
gopher	70	smtp	25
http	80	snmp	161
laplink	1547	telnet	23
ldap	389	telnet	23
nbdatagram	138	wais	210
nbname	137	whois	43
nbsession	139		

Default

any, 0

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

destination-address
diffserv-marking
dscp-values
protocol
qos mf-class rule
source-address
tcp-udp-source-port
use tcp_udp_destination_port

Example

The following example configures a destination transport protocol rule for LDAP (port 389) under the rule named rule1.

```
CES(config)# qos rule rule1
CES(config-mfrule)# tcp-udp-destination-port ldap 389
CES(config-mfrule)# exit
CES(config)#
```

The following example removes a destination transport protocol rule for LDAP under the rule named rule1.

```
CES(config)# rule rule1
CES(config-mfrule)# no tcp-udp-destination-port ldap
CES(config-mfrule)# exit
CES(config)#
```

tcp-udp-source-port

Use this command to filter packets according to one or more TCP or UDP source ports. With this command, you can configure the gateway to transfer or drop packets based on the value of the TCP/UDP source port field. The source is relative to the direction of the rule. Use the **no** form of the command to remove the source port from the list of ports.

Syntax

tcp-udp-source-port *<port-name> <port-address>*
no tcp-udp-source-port *<port-name>*

Parameters

See Table 11 for the list of value pairs that you can enter with the **tcp-udp-source-port** command. You can also specify other protocol-port combinations not in this list. For the list of well-known ports, see http://www.iana.org/assignments/port-numbers.

Default

any, 0

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

destination-address
diffserv-marking
dscp-values
protocol
qos mf-class rule
source-address
tcp-udp-destination-port
use tcp_udp_source_port

Example

The following example configures a source transport protocol rule for HTTP (port 80) under the rule named rule1.

```
CES(config)# mf-class rule1
CES(config-mfrule)# tcp-udp-source-port http 80
CES(config-mfrule)# exit
CES(config)#
```

The following example deletes a source transport protocol rule for HTTP (port 80) from the rule named rule1.

```
CES(config)# mf-class rule1
CES(config-qos)# no tcp-udp-source-port http
CES(config-mfrule)# exit
CES(config)#
```

use destination_address

Use this command to assign the destination address for a rule.

Syntax

use destination_address <*name*>

Parameters

name	Specifies a configured address name. You configure the address with the **destination-address** command.

Default

any

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

destination-address
qos mf-class rule
use diffserv_marking
use dscp
use protocol
use source_address
use tcp_udp_destination_port
use tcp_udp_source_port

Example

The following example configures a destination address for rule “rule1.”

```
CES(config)# qos mf-class rule rule1
CES(config-mfrule)# use destination_address London
CES(config-mfrule)# exit
CES(config)#
```

use diffserv_marking

Use this command to select the DSCP—either EF (expedited forwarding) or an AF (assured forwarding) level—that this rule applies to data. The DiffServ code point (DSCP) is always copied into tunnel headers.

Syntax

use diffserv_marking {**EF** | **AF1** | **AF2** | **AF3** | **AF4**}

Parameters

EF	Specifies expedited forwarding, that is, premium service class.
AF1	Specifies assured forwarding level 1, that is, bronze service class.
AF2	Specifies assured forwarding level 2, that is, silver service class.
AF3	Specifies assured forwarding level 3, that is, gold service class.
AF4	Specifies assured forwarding level 4, that is, platinum service class.

Default

Expedited forwarding (EF)

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

diffserv-marking
qos mf-class rule
use destination_address
use dscp
use protocol
use source_address
use tcp_udp_destination_port
use tcp_udp_source_port

Example

The following example sets DiffServ marking for rule1 to AF2 (assured forwarding level 2).

```
CES(config)# qos mf-class rule rule1
CES(config-qos-rule)# use diffserv_marking AF2
CES(config-qos-rule)# exit
CES(config)#
```

use dscp

Use this command to assign the DSCP value to a rule. The DSCP value and mask assignments allow packets that are already marked to retain their settings or to be re-marked based on their previous DSCP value. This is an input criterion.

Syntax

use dscp *<value>*

Parameters

Table 12 lists the values that you can enter for the **use dscp** command and briefly describes each value. (AF=assured forwarding; EF=expedited forwarding.)

Table 12 DSCP values for rules

DSCP Name	DSCP Value	DSCP Mask	Meaning
AF1HighDrop	14	63	Bronze service class
AF1LowDrop	10	63	Bronze service class
AF1MedDrop	12	63	Bronze service class
AF2HighDrop	22	63	Silver service class
AF2LowDrop	18	63	Silver service class
AF2MedDrop	20	63	Silver service class
AF3HighDrop	30	63	Gold service class

Table 12 DSCP values for rules (Continued)

DSCP Name	DSCP Value	DSCP Mask	Meaning
AF3LowDrop	26	63	Gold service class
AF3MedDrop	28	63	Gold service class
AF4HighDrop	38	63	Platinum service class
AF4LowDrop	34	63	Platinum service class
AF4MedDrop	36	63	Platinum service class
any	0	0	Any
EF	46	63	Premium service class

Default

any

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Warning messages

```
% No such DSCP value exists
```

Related commands

dscp-values
qos mf-class rule
use destination_address
use diffserv_marking
use protocol
use source_address
use tcp_udp_destination_port
use tcp_udp_source_port

Example

The following example sets the current DSCP value to AF3LowDrop.

```
CES(config)# qos mf-class rule1
CES(config-qos-rule)# use dscp AF3LowDrop
CES(config-qos-rule)# exit
CES(config)#
```

use protocol

Use this command to assign the appropriate protocol to be used for a QoS rule.

Syntax

use protocol {**icmp** | **ip** | **tcp** | **udp**}

Parameters

icmp	Specifies Internet Control Message Protocol (ICMP) as the protocol to be used by the QoS rule. ICMP is a network layer protocol. The ping utility used to check network availability, generates ICMP packets.
ip	Specifies Internet Protocol (IP) as the protocol to be used by the QoS rule. IP is a network layer protocol in the TCP/IP stack that offers a connectionless internetwork service. IP packets that are encapsulated within other packets create “IP over IP.” Multicast IP packets (packets that have multicast destinations), carried between networks that support multicasting over intermediate networks that do not, are the most common implementation. Conferencing and other services that are offered through the Multicast Backbone (MBONE) are examples.
tcp	Specifies Transmission Control Protocol (TCP) as the protocol to be used by the QoS rule. TCP is a transport layer protocol that is connection oriented and that provides reliable full-duplex data transmission. Web browsers using HTTP and FTP are examples.
udp	Specifies User Datagram Protocol (UDP) as the protocol to be used by the QoS rule. UDP is a transport layer protocol in the TCP/IP protocol stack. UDP is a connectionless service that exchanges datagrams without acknowledgment or delivery guarantees and therefore, requires that error handling and retransmissions be handled by other protocols. DNS and WINS are examples.

Default

ip

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

protocol
qos mf-class rule
use destination_address
use diffserv_marking
use dscp
use source_address
use tcp_udp_destination_port
use tcp_udp_source_port

Example

The following example configures TCP as the protocol to use for the rule named rule1.

```
CES(config)# qos mf-class rule rule1
CES(config-mfrule)# use protocol tcp
CES(config-mfrule)# exit
CES(config)#
```

use source_address

Use this command to assign the source address for the particular rule. The source is relative to the direction of the rule.

Syntax

use source_address <*name*>

Parameters

name	Specifies a configured address name. You configure the address with the **source-address** command.

Default

any

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos mf-class rule
source-address
use destination_address
use diffserv_marking
use dscp
use protocol
use tcp_udp_destination_port
use tcp_udp_source_port

Example

The following example configures a source address rule for the rule “rule1.”

```
CES(config)# qos mf-class rule rule1
CES(config-mfrule)# use source_address FtpServer
CES(config-mfrule)# exit
CES(config)#
```

The following example configures a source address rule for the rule “rule2.”

```
CES(config)# qos mf-class rule rule2
CES(config-mfrule)# use source_address HttpServer
CES(config-mfrule)# exit
CES(config)#
```

The following example configures a source address rule for the rule “rule3.”

```
CES(config)# qos mf-class rule rule3
CES(config-mfrule)# use source_address any
CES(config-mfrule)# exit
CES(config)#
```

use tcp_udp_destination_port

Use this command to assign a TCP or UDP destination port to a rule.

Syntax

use tcp_udp_destination_port <*value*>

Parameters

See Table 11 on page 1853 for the list of values that you can enter with the **use tcp_udp_destination_port** command. You can also specify other protocol-port combinations not in this list. For the list of well-known ports, see http://www.iana.org/assignments/port-numbers.

Default

any, 0

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos mf-class rule
tcp-udp-destination-port
use destination_address
use diffserv_marking
use dscp
use protocol
use source_address
use tcp_udp_source_port

Example

The following example configures a destination transport protocol rule for LDAP (port 389) for the rule “rule1.”

```
CES(config)# qos mf-class rule rule1
CES(config-mfrule)# use tcp_udp_destination_port ldap
CES(config-mfrule)# exit
CES(config)#
```

use tcp_udp_source_port

Use this command to assign a TCP or UDP source port to a rule.

Syntax

use tcp_udp_source_port <*value*>

Parameters

See Table 11 on page 1853 for the list of values that you can enter with the **use tcp_udp_destination_port** command. You can also specify other protocol-port combinations not in this list. For the list of well-known ports, see http://www.iana.org/assignments/port-numbers.

Default

any,0

Command mode

QoS Rule Configuration

Next command mode

QoS Rule Configuration

Required privileges

System Management - Manage
User Management - None

Related commands

qos mf-class rule
tcp-udp-source-port
use destination_address
use diffserv_marking
use dscp
use protocol
use source_address
use tcp_udp_destination_port

Example

The following example configures a source transport protocol rule for HTTP (port 80) under the MF classification rule “rule1.”

```
CES(config)# qos mf-class rule1
CES(config-mfrule)# use tcp_udp_source_port http
CES(config-mfrule)# exit
CES(config)#
```

Chapter 47
DLSw configuration commands

This chapter describes DLSw configuration commands:

Commands	Page
dlsw clear circuit	1875
dlsw clear mac-cache	1876
dlsw local-peer	1878
dlsw local-peer backlevel-flowcontrol	1879
dlsw local-peer enable	1881
dlsw local-peer mac-translation	1883
dlsw local-peer unconfigured-peer enable	1884
dlsw mac-translation	1885
dlsw remote-peer	1886
dlsw remote-peer backup	1887
dlsw remote-peer backup-peer holdtime backuptime	1888
dlsw remote-peer circuit-inactivity	1890
dlsw remote-peer cost	1891
dlsw remote-peer enable	1892
dlsw remote-peer receive-initial-pacing	1893
dlsw remote-peer rfc1795	1895
dlsw timer circuit-ack-timeout	1896
dlsw timer explorer-delay	1897
dlsw timer explorer-timeout	1898
dlsw timer explorer-wait-timeout	1899
dlsw timer idle-timeout	1900

Commands	Page
dlsw timer tcp-connect-retry	1901
dlsw timer test-timeout	1902
llc2 ack-delay-time	1904
llc2 busy-time	1906
llc2 enable	1907
llc2 idle-time	1909
llc2 lantype	1910
llc2 max-received-window	1911
llc2 max-retry	1912
llc2 lpf-time	1913
llc2 rej-time	1914
llc2 t2timeout	1916
clock-type	1918
counter disconnect	1920
counter fast-contact	1921
counter fast-poll	1922
counter no-response	1923
counter remote-busy	1924
counter slow-contact	1925
counter slow-poll	1926
enable	1927
encapsulation sdlc	1928
grouppoll	1930
line-encoding	1931
line-speed	1932
lmac lsap	1933
pollframe	1934
proxy-xid	1935
recvwindow	1936
rmac rsap	1937

Commands	Page
sdlc activation-sequence	1938
sdlc counter idle-time	1940
sdlc counter non-productive	1941
sdlc counter write-port	1942
sdlc debug	1944
sdlc interframe-fill enable	1945
sdlc link-station polladdress	1946
sdlc max-received-window	1947
sdlc polladdress	1948
sdlc primary-full-duplex	1949
sdlc role	1950
sdlc secondary-full-duplex	1952
sdlc send-rej	1953
sdlc timer idle-time	1954
sdlc timer non-productive	1955
sdlc timer write-port	1956
sendwindow	1958
start	1959
stop	1961
timer disconnect	1962
timer fast-contact	1963
timer fast-poll	1964
timer no-response	1965
timer rnr-limit	1966
timer slow-contact	1968
timer slow-poll	1969
timer turn-around	1970
show dlsw circuits	1973
show dlsw directory	1975
show dlsw capabilities	1971

Commands	Page
show dlsw port	1981
show dlsw sdlc	1984
show dlsw peers	1978
show dlsw mac-table	1977
dlsw debug_level	1986
dlsw ips-trace enable	1988

Listed below are all of the available DLSw CLI commands for Earl.

Global configuration mode commands

This section describes all of the DLSw Global Configuration mode NNCLI commands.

Command	Page
dlsw clear circuit	1875
dlsw clear mac-cache	1876
dlsw local-peer	1878
dlsw local-peer backlevel-flowcontrol	1879
dlsw local-peer enable	1881
dlsw local-peer mac-translation	1883
dlsw local-peer unconfigured-peer enable	1884
dlsw mac-translation	1885
dlsw remote-peer	1886
dlsw remote-peer backup	1887
dlsw remote-peer backup-peer holdtime backuptime	1888
dlsw remote-peer circuit-inactivity	1890
dlsw remote-peer cost	1891
dlsw remote-peer enable	1892
dlsw remote-peer receive-initial-pacing	1893

Command	Page
dlsw remote-peer rfc1795	1895
dlsw timer circuit-ack-timeout	1896
dlsw timer explorer-delay	1897
dlsw timer explorer-timeout	1898
dlsw timer explorer-wait-timeout	1899
dlsw timer idle-timeout	1900
dlsw timer tcp-connect-retry	1901
dlsw timer test-timeout	1902

dlsw clear circuit

Use this command to close all opened circuits. A specific circuit could be closed if the command is entered with local MAC/SAP and remote MAC/SAP peers. All associated DLC links are also closed.

Syntax

dlsw clear circuit [lmac *mac-address* **| rmac** *mac-address*]

Parameters

lmac (Optional) Limits the circuit deletion to a specific local MAC/SAP pair (the default is all).

rmac (Optional) Limits the circuit deletion to a specific remote MAC/SAP pair (the default is all).

Default

None

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw clear circuit
```

dlsw clear mac-cache

Use this command to delete the entries in MAC cache. This could be required when a new peer is configured with a lower priority in order to be used by DLSw circuits.

Syntax

dlsw clear mac-cache

Parameters

None

Default

None

Commahnd Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw clear mac-cache
```

dlsw local-peer

Use this command to configure a DLSW node.

Use the **no** form of this command to remove the DLSW node.



Caution: The command **no dlsw local-peer** will delete the entire DLSw configuration from the switch. As a precaution, you must first disable the local peer using the command **no dlsw local-peer enable** before the delete will be accepted.

Syntax

```
dlsw local-peer ip-address
no dlsw local-peer
```

Parameters

ip-address	Address on which to listen for incoming connections.

Default

None

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw local-peer 172.19.5.67
```

dlsw local-peer backlevel-flowcontrol

Use this command to configure when operating with a RFC1434 peer.

Use the **no** form of the command to restore the default value.

Syntax

```
dlsw local-peer backlevel-flowcontrol
no dlsw local-peer backlevel-flowcontrol
```

Parameters

None

Default

None

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw local-peer backlevel-flowcontrol
```

dlsw local-peer enable

Use this command to disable or re-enable the DLSw feature. Disabling the feature stops it immediately. Existing connections through the switch are not terminated explicitly and the end stations detect failures. The existing configuration is saved by the disable command and is re-applied to the DLSw node when it is re-enabled.

Syntax

```
dlsw local-peer enable
no dlsw local-peer enable
```

Parameters

None

Default

None

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw local-peer enable
```

dlsw local-peer mac-cache

Use this command to configure the maximum number of entries in the MAC cache table.

Use the **no** form of this command to change the value to the default one.

Syntax

```
dlsw local-peer mac-cache mac-cache-limit
no dlsw local-peer mac-cache
```

Parameters

mac-cache-limit	Maximum number of entries in the MAC cache table. This is the table of MAC cache entries. The value is between 0 and 65535.

Default

0

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

CES(config)# dlsw local-peer mac-cache 50

dlsw local-peer mac-translation

Use this command to enable the MAC address translation feature on the local node.

Use the **no** form of this command to disable the feature.

Syntax

```
dlsw local-peer mac-translation
no dlsw local-peer mac-translation
```

Parameters

None

Default

Disable

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw local-peer mac-translation
```

dlsw local-peer unconfigured-peer enable

Use this command to enable un-configured remote peer support.

Use the **no** form of this command to reset to the default setting.

Syntax

```
dlsw local-peer unconfigured-peer enable
no dlsw local-peer unconfigured-peer
```

Parameters

None

Default

Disabled

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw local-peer unconfigured-peer enable
```

dlsw mac-translation

Use this command to configure the local or remote MAC translation tables. Local table is used for locally initiated connections and the remote table is used for connections initiated by remote peers.

Syntax

dlsw mac-translation {local|remote} *mac-address* **to** *new-mac-address*
no mac-translation {local|remote} *mac-address*

Parameters

local	The rule is applied for packets received on the locally conected link stations.
remote	The rule is applied for packets received from remote peers.
mac-address	Source/destination MAC addresses.
to	New MAC address.
new-mac-address	Translated MAC address.

Default

None

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw mac-translation local 04-00-12-34-87-65 to
04-00-12-34-78-89
```

dlsw remote-peer

Use this command to create a remote DLSW peer. The connection will be established using RFC 2166. If the remote peer does not respond, an RFC1795 connection will be tried.

Use the **no** form of this command to remove the remote DLSW node.

Syntax

dlsw remote-peer *ip-address*
no dlsw remote-peer *ip-address*

Parameters

ip-address	Address of the remote DLSw peer.

Default

No remote DLSw node is defined.

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw remote-peer 172.19.5.67
```

dlsw remote-peer backup

Use this command to create a backup peer. This remote peer type will not be contacted until the defined primary peer fails.

Use the **no** form of this command to delete a backup peer.

Syntax

dlsw remote-peer *ip-address* **backup**
no dlsw remote-peer *ip-address* **backup**

Parameters

ip-address Address of the remote DLSW backup peer.

Default

No backup peer is defined.

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw remote-peer 172.19.5.67 backup
```

dlsw remote-peer backup-peer holdtime backuptime

Use this command to configure a backup-peer for a specific primary peer connection.

Use the **no** form of this command to remove the backup peer.

Syntax

dlsw remote-peer *ip-address* **backup-peer [***backup-address*
holdtime *holddowntim***] backuptime** *backupmaxtime*
no dlsw remote-peer *ip-address* **backup-peer**

Parameters

ip-address Address of the remote DLSW backup peer.

backup-address Address of backup peer.

holddowntime Holddown time before the backup peer is contacted.

backupmaxtime Backup maximum time. The initial peer is contacted and the backup connection is destroyed when this time expires.

Default

No backup peer is defined.

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw remote-peer 172.19.5.67 backup-peer
     192.168.29.57
```

dlsw remote-peer circuit-inactivity

Use this command to configure the DLSw circuit timeout in seconds.

Use the **no** form of the command to restore the default value.

Syntax

dlsw remote-peer *ip-addresss* **circuit-inactivity** *timeout*
no dlsw remote-peer *ip-address* **circuit-inactivity**

Parameters

ip-address	Address of remote DLSW peer.
timeout	No circuits time-out in seconds. The connection is brought down if it is connected to a DLSw v2.0 capable peer and it is not carrying circuits for longer than this value. Zero means no time-out is used (the connection will not be brought down). The values are between 0 - 65535.

Default

The default circuit inactivity value is 180 seconds.

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw remote-peer 172.19.5.67 circuit-inactivity 0
```

dlsw remote-peer cost

Use this command to configure the remote peer cost. The peer with the minimum cost will be the first one chosen to receive a CANUREACH message.

Use the **no** form of the command to restore the default value.

Syntax

dlsw remote-peer *ip-address* **cost** *value*
no dlsw remote-peer *ip-address* **cost**

Parameters

ip-address	Address of remote DLSW peer.
value	The cost of remote-peer connection. The values are from 1 to 5.

Default

5

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw remote-peer 172.19.5.67 cost 3
```

dlsw remote-peer enable

Use this command to enable a remote peer.

Use the **no** form of the command to disable a remote peer. A remote peer must be disabled before the peer configuration can be changed.



Caution: Disabling a remote peer will terminate all SNA connections currently active over that peer.

Caution: Omitting the **enable** parameter in the **no** form of the command will remove the peer definition from the configuration.

Syntax

```
dlsw remote-peer ip-address enable
no dlsw remote-peer ip-address enable
```

Parameters

ip-address Address of the remote DLSW peer.

Default

None

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw remote-peer 192.101.90.100 enable
```

dlsw remote-peer receive-initial-pacing

Use this command to configure the initial pacing window used for incoming TCP connections for the remote peer.

A larger initial pacing window will permit more data to flow between RFC1795 / RFC2166 type peers before flow control is asserted. A larger pacing window might increase the performance over high latency high speed links, such as a satellite circuit.

Use the **no** form of this command to set the value to its default.

Syntax

dlsw remote-peer *ip-address* **receive-initial-pacing** *initialpacingwindow*
no dlsw remote-peer *ip-address* **receive-initial-pacing**

Parameters

ip-address	Address of the remote peer.
initialpacingwindow	The default value of the initial receive pacing window used on incoming Transport Connections.

Default

1

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw remote-peer 172.19.5.67 receive-initial-pacing 5
```

dlsw remote-peer rfc1795

Use this command to create a remote DLSW peer that is compliant with RFC 1795.

Use the **no** form of this command to remove the remote peer.

Syntax

dlsw remote-peer *ip-address* **rfc1795**
no dlsw local-peer *ip-address* **rfc1795**

Parameters

ip-address Address of the remote peer.

Default

No DLSw remote peer is created.

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw remote-peer 172.19.5.67 rfc1795
```

dlsw timer circuit-ack-timeout

Use this command to specify the timeout in seconds after which a circuit pending a REACH_ACK message from the circuit originator is destroyed.

Use the **no** form of the command to restore the default value.

Syntax

dlsw timer circuit-ack-timeout *acktimeout*
no dlsw timer circuit-ack-timeout

Parameters

acktimeout	Timeout in seconds after which a circuit pending a REACH_ACK message from the circuit originator is destroyed.

Default

10 seconds

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw timer circuit-ack-timeout 30
```

dlsw timer explorer-delay

Use this command to specify the number of milliseconds between sending of CANUREACH frames to different levels (1-5) of preferred peers.

Use the **no** form of the command to restore the default value.

Syntax

```
dlsw timer explorer-delay value
no dlsw timer explorer-delay
```

Parameters

value	Number of seconds milliseconds between sending CANUREACH frames at different preferred peers levels.

Default

200 milliseconds.

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw timer explorer-delay 20
```

dlsw timer explorer-timeout

Use this command to specify the timeout in seconds after which an attempt to reach a target via a single DLSw peer has failed.

Use the **no** form of this command to set the value to its default value (15 seconds).

Syntax

dlsw timer explorer-timeout *circtimeout*
no dlsw timer explorer-timeout

Parameters

circtimeout	Timeout in seconds after which an attempt to reach a target via a single DLSw peer has failed. This happens when an entry from the MAC-cache is used to reach the target.

Default

15 seconds.

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw timer explorer-timeout 30
```

dlsw timer explorer-wait-timeout

Use this command to specify the timeout in seconds after which an attempt to reach a target via multiple DLSw peers has failed.

Use the **no** form of this command to set the value to its default.

Syntax

dlsw timer explorer-wait-timeout *multicirctimeout*
no dlsw timer explorer-wait-timeout

Parameters

multicirctimeout Timeout in seconds after which an attempt to reach a target via multiple DLSw peers has failed.

Default

15 seconds.

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw timer explorer-wait-timeout 30
```

dlsw timer idle-timeout

Use this command to specify the timeout in seconds after which a circuit in a CIRC_ESTABLISHED state that exchanges no traffic is disconnected.

Use the **no** form of the command to restore the default value.

This command applies only for RFC 2166. The timeout is used when no circuits are using a TCP connection. This command does not relate to the issue of no traffic over a circuit, but rather it is about no circuits (SNA connections) over a TCP connection. 0 means that the connection will not be closed even if there are not any circuits using the connection.

Syntax

```
dlsw timer idle-timeout idletime
no dlsw timer idle-timeout
```

Parameters

idletime	When a circuit in CIRC_ESTABLISHED state exchanges no traffic for the number of seconds specified by **idletimeout**, the circuit is disconnected.

Default

30 seconds.

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw timer idle-timeout 30
```

dlsw timer tcp-connect-retry

Use this command to specify the number of seconds between attempts to establish a configured Transport Connection.

Use the **no** form of the command to restore the default value.

Syntax

```
dlsw timer tcp-connect-retry connectretry
no dlsw timer tcp-connect-retry
```

Parameters

connectretry	Number of seconds between attempts to establish a configured Transport Connection.

Default

15 seconds.

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw timer tcp-connect-retry 20
```

dlsw timer test-timeout

Use this command to specify the timeout in seconds after which an attempt to establish an SNA connection using configured LAN ports has failed.

Use the **no** form of the command to restore the default value.

Syntax

dlsw timer test-timeout *conntimeout*
no dlsw timer test-timeout

Parameters

conntimeout	Timeout in seconds after which an attempt to establish an SNA connection using configured LAN ports has failed.

Default

15 seconds

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config)# dlsw timer test-timeout 20
```

LAN interface configuration commands

This section describes port and LLC2 commands.

Command	Page
llc2 ack-delay-time	page 1904
llc2 busy-time	page 1906
llc2 enable	page 1907
llc2 idle-time	page 1909
llc2 lantype	page 1910
llc2 max-received-window	page 1911
llc2 max-retry	page 1912
llc2 lpf-time	page 1913
llc2 rej-time	page 1914
llc2 t2timeout	page 1916

llc2 ack-delay-time

Use this command to configure the timeout in milliseconds within which LLC2 expects a response to any I-frames sent to the adjacent link station.

Use the **no** form of the command to restore the default value.

Syntax

llc2 ack-delay-time *value*
no llc2 ack-delay-time

Parameters

value	The timeout in milliseconds within which LLC2 expects a response to any I-frames sent to the adjacent link station.

Default

5000 ms

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# llc2 ack-delay-time 1000
```

llc2 busy-time

Use this command to configure the time in seconds for which LLC2 waits for indication of clearance of a busy condition at the adjacent link station. After this period, LLC2 sends an RR to check the status of the adjacent link station. There is no maximum retry limit for this timer.

Use the **no** form of the command to restore the default value.

Syntax

```
llc2 busy-time value
no llc2 busy-time
```

Parameters

value	The time in seconds for which LLC2 waits for indication of clearance of a busy condition at the adjacent link station.

Default

30 seconds

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# llc2 busy-time 20
```

llc2 enable

Use this command to start an LLC2 port defined on a CES DLSw node.

Use the **no** form of this command to disable the port.

Syntax

```
llc2 enable
no llc2 enable
```

Parameters

None

Default

None

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# llc2 enable
```

llc2 idle-time

Use this command to setup the RR 'keep-alive' interval in seconds for an otherwise idle link.

Use the **no** form of the command to restore the default value.

Syntax

```
llc2 idle-time value
no llc2 idle-time
```

Parameters

value	The RR 'keep-alive' interval in seconds for an otherwise idle link.

Default

30 seconds

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# llc2 idle-time 20
```

llc2 lantype

Use this command to configure LAN type.

Use the **no** form of the command to restore the default value.

Syntax

```
llc2 lantype {8023 | dix | 8023dix}
no llc2 lantype
```

Parameters

8023	Normal 802.3 frame format.
dix	DIX frame format.
8023dix	Both 802.3 and DIX frames format

Default

8023

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# llc2 lantype dix
```

llc2 max-received-window

Use this command to configure the size of the receive window for the LLC2 to use on this port. This value is used in XID negotiations and for NRM ports will influence the choice between Normal and Extended sequence numbering. The default is 0.

The value 0 has a special meaning. It instructs DLSw and the LLC2 to use the receive window size passed in on an XID from a co-operating remote LLC2 (in the case of local switching) or over TCP/IP.

Use the **no** form of the command to restore the default value.

Syntax

```
llc2 max-received-window maxrecvwindow
no llc2 max-received-window
```

Parameters

maxrecvwindow The size of receive window for the LLC2 to use on this port.

Default

0

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# llc2 max-received-window 10
```

llc2 max-retry

Use this command to configure the maximum number of retries for any of the following timers: ack-delay-time, tpf-time, rej-time, idle-time.

Use the **no** form of the command to restore the default value.

Syntax

```
llc2 max-retry retryvalue
no llc2 max-retry
```

Parameters

retryvalue	Maximum number of retries for any of the following timers: **ack-delay-time, lpf-time, rej-time, idle-time**.

Default

10

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# llc2 max-retry 5
```

llc2 lpf-time

Use this command to configure the timeout in milliseconds that LLC2 waits for a response to a frame sent with the POLL bit set.

Use the **no** form of the command to restore the default value.

Syntax

llc2 lpf-time *value*
no llc2 lpf-time

Parameters

value	The timeout in milliseconds within which LLC2 waits for a response to a frame sent with the POLL bit set.

Default

5000 ms

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# llc2 lpf-time 1000
```

llc2 rej-time

Use this command to configure the time in seconds during which LLC2 expects to receive a response to a REJ frame.

Use the **no** form of the command to restore the default value.

Syntax

llc2 rej-time *value*
no llc2 rej-time

Parameters

value	Time in seconds during which LLC2 expects to receive a response to a REJ frame.

Default

5 seconds

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# llc2 rej-time 20
```

llc2 t2timeout

Use this command to configure the period in milliseconds that LLC2 will withhold a response to a received I-frame in order to allow further I-frames to be received and acknowledged with the same RR, thus reducing acknowledgement traffic. SNAP-LLC2 will send the acknowledgement at latest after this period, but may send it before then.

Use the **no** form of the command to restore the default value.

Syntax

llc2 t2timeout *value*
no llc2 t2timeout

Parameters

value	Period in milliseconds that LLC2 will withhold a response to a received I-frame in order to allow further I-frames to be received and acknowledged with the same RR.

Default

100 ms

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# llc2 t2timeout 200
```

SDLC and Link Station configuration commands

This section describes SDLC commands.

Command	Page
clock-type	1918
counter disconnect	1920
counter fast-contact	1921
counter fast-poll	1922
counter no-response	1923
counter remote-busy	1924
counter slow-contact	1925
counter slow-poll	1926
enable	1927
encapsulation sdlc	1928
grouppoll	1930
line-encoding	1931
line-speed	1932
lmac lsap	1933
pollframe	1934
proxy-xid	1935
recvwindow	1936
rmac rsap	1937
sdlc activation-sequence	1938
sdlc counter idle-time	1940

Command	Page
sdlc counter non-productive	1941
sdlc counter write-port	1942
sdlc debug	1944
sdlc interframe-fill enable	1945
sdlc link-station polladdress	1946
sdlc max-received-window	1947
sdlc polladdress	1948
sdlc primary-full-duplex	1949
sdlc role	1950
sdlc secondary-full-duplex	1952
sdlc send-rej	1953
sdlc timer idle-time	1954
sdlc timer non-productive	1955
sdlc timer write-port	1956
sendwindow	1958
start	1959
stop	1961
timer disconnect	1962
timer fast-contact	1963
timer fast-poll	1964
timer no-response	1965
timer rnr-limit	1966
timer slow-contact	1968
timer slow-poll	1969
timer turn-around	1970

clock-type

Use this command to configure internal or external clock setting.

Use the **no** form of the command to restore the default value.

Syntax

```
clock-type {internal|external}
no clock-type
```

Parameters

external	external clock
internal	internal clock

Default

external

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# clock-type internal
```

counter disconnect

This SDLC link station count controls the number of times transmission and retransmission of a DISC is allowed.

Use the **no** form of the command to restore the default value.

Syntax

counter disconnect *counter*
no counter disconnect

Parameters

counter	Number of disconnect transmissions and retransmissions.

Default

4

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# counter disconnect 5
```

counter fast-contact

This SDLC link station count controls the number of times transmission and retransmission of a contact frame (e.g., SNRM) is allowed before switching to the slow poll contact timer.

Use the **no** form of the command to restore the default value.

Syntax

```
counter fast-contact counter
no counter fast-contact
```

Parameters

counter	Number of contact frames per fast contact sequence.

Default

4

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# counter fast-contact 5
```

counter fast-poll

This SDLC link station timer controls the number of times a station is removed from the polling list on the normal poll timer before switching to the slow poll timer.

Use the no form of the command to restore the default value.

Syntax

counter fast-poll *counter*
no counter fast-poll

Parameters

counter	Number of times used after a station removed from the polling list is switched to the slow poll timer.

Default

16

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# counter fast-poll 15
```

counter no-response

This SDLC link station count controls the number of times an adjacent secondary station is seen to fail to respond before an outage message is sent.

Use the no form of the command to restore the default value.

Syntax

counter no-response *counter*
no counter no-response

Parameters

counter	Number of times an adjacent secondary station is seen to fail to respond before an outage message is sent.

Default

10

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# counter no-response 15
```

counter remote-busy

The remote busy retry limit value for an SDLC link station is used with the timeout value to provide the overall timeout before an outage message is sent.

Use the **no** form of the command to restore the default value.

Syntax

```
counter remote-busy counter
no counter remote-busy
```

Parameters

counter	Number of retries before an adjacent station is “inoperative”.

Default

4

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# counter remote-busy 5
```

counter slow-contact

This SDLC link station count controls the number of times transmission and retransmission of a contact frame (e.g. SNRM) is allowed before an outage message is sent to the SDLC user.

Use the no form of the command to restore the default value.

Syntax

counter slow-contact *counter*
no counter slow-contact

Parameters

counter	Number of contact frames per slow poll contact sequence.

Default

8

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# counter slow-contact 6
```

counter slow-poll

This SDLC link station count controls the number of times a station is removed from the polling list before an outage message is sent. If the link station is to be polled without being taken off the poll list, this count should be set to infinite (65535).

Use the no form of the command to restore the default value.

Syntax

counter slow-poll *counter*
no counter slow-poll

Parameters

counter	Number of times a station is removed from the polling list before an error indication is sent.

Default

65535

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# counter slow-poll 100
```

enable

Use this command to enable an SDLC link station for DLSw.

Use the **no** form of this command to disable an SDLC link station.

Syntax

```
enable
no enable
```

Parameters

Default

None

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# enable
```

encapsulation sdlc

Use this command to start an SDLC port defined on a DLSw node.

Syntax

```
encapsulation {frame-relay|ppp|sdlc}
```

Parameters

frame-relay	Specifies frame-relay protocol on the port.
ppp	Specifies PPP protocol on the port.
sdlc	Specifies SDLC protocol on the port.

Default

None

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

The DLSw node and the port must be defined and the DLSw node must be started before issuing this command.

show dlsw port

Example

```
CES(config-if)# enacapsulation sdlc
```

grouppoll

Use this command to configure the group poll address.

Use the **no** form of this command to change the remove the group poll address.

Syntax

grouppoll *grouppolladdress*
no groupoll

Parameters

grouppolladdress Group poll address.

Default

None

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

CES(config-ls)# **grouppoll f0**

line-encoding

Use this command to configure line encoding.

Use the **no** form of the command to restore the default value.

Syntax

```
line-encoding {nrz|nrzi}
no line-encoding
```

Parameters

nrz	Non-return to zero
nrzi	Non-return to zero (inverse)

Default

nrz

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# line-encoding nrzi
```

line-speed

Use this command to configure the internal clock (in bit/s) when the clock is used.

Use the **no** form of the command to restore the default value.

Syntax

```
line-speed value
no line-speed
```

Parameters

value	Internal clock rate (bit/second)

Default

112.500

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# no line-speed
```

lmac lsap

Use this command to specify the local LAN (MAC) address of this station. This address is allowed to be defined multiple times on a port. This allows (on a leased port) multiple circuits to connect to the same remote node.

Use the **no** form of this command to delete the local MAC and SAP.

Syntax

lmac *lmac* **lsap** *lsap*
no lmac lsap

Parameters

lmac	Local LAN (MAC) address of this station.
lsap	Local SAP for this station. Local SAP is defined as a hexadecimal value.

Default

None

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# localmac 04-00-12-34-98-76 lsap 04
```

pollframe

Use this command to configure the frame to use for pre-activation polling. This is normally set to XID (the default) to show that polling is in the control of the DLC user. However, when the role is primary talking to an old secondary implementation, it may be necessary to poll using some other frame.

Use the **no** form of the command to restore the default value.

Syntax

```
pollframe {xid|snrm|disc|test}
no pollframe
```

Parameters

Default

XID frame

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# pollframe test
```

proxy-xid

Use this command to configure the node ID sent upstream by DLSw on behalf of an older downstream SDLC PU that does not support XIDs.

Use the **no** form of this command to remove the node ID.

Syntax

proxy-xid *xidstring*
no proxy-xid

Parameters

xidstring	Node ID sent upstream by DLSw on behalf of an older downstream SDLC PU that does not support XIDs. The value must be 4 bytes (8 digits) in length and is specified with hexadecimal digits.

Default

None

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# proxy-xid 01720002
```

recvwindow

Use this command to configure the default rcvwindow size for link level flow control if the value can not be determined from an XID exchange.

Use the **no** form of the command to restore the default value.

Syntax

```
recvwindow recvwindowsize
no recvwindow
```

Parameters

recvwindowsize	Default **rcvwindow** size for link level flow control if the value can not be determined from an XID exchange. This value overrides the default specified on the **dlsw local-peer** command.

Default

Use the XID or global default value.

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# recvwindow 7
```

rmac rsap

Use this command to specify the destination LAN (MAC) address called during SDLC initiated circuit activation. If this address is not specified, this link station cannot support SDLC-initiated circuits.

Use the **no** form of this command to delete the destination MAC and SAP.

Syntax

rmac *rmac* **rsap** *rsap*
no rmac rsap

Parameters

rmac	Destination LAN (MAC) address called during SDLC initiated circuit activation.
rsap	Destination Remote SAP, defined as a hexadecimal value.

Default

None

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# rocalmac 04-00-12-34-98-77 rsap 04
```

sdlc activation-sequence

Use this command to configure the activation seuqence used when a primary SDLC device is starting. The activation sequence is used when the poll bit is set to XID.

Syntax

sdlc activation-sequence {*localdevicefirst* | *peerfirst*}

Parameters

localdevicefirst When an SDLC device is activated using the **start** command the local connected secondary device is contacted first.

peerfirst When an SDLC device is activated the remote peer is contacted first. If there is no response the local station is not contacted.

Default

Disabled

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc activation-sequence localdevicefirst
```

sdlc counter idle-time

This counter indicates how many retries are made for a completely inactive line before the line is considered "idle" and an alert is sent to the SDLC client (DLSw). The line remains inoperative until the client restarts the line.

Use the **no** form of this command to restore the counter default value.

Syntax

```
sdlc counter idle-time value
no sdlc counter idle-time
```

Parameters

value	Indicates how many times idle-time timer is started before the line is considered idle.

Default

20

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc counter idle-time 10
```

sdlc counter non-productive

For an SDLC primary station, the count is used to produce an outage message when a secondary link station produces continuous frames without setting the F-bit (final).

For an SDLC secondary station this counter indicates how many retries are made before an outage message is issued because a valid frame is not received from the primary.

Use the **no** form of the command to restore the default value.

Syntax

sdlc counter non-productive *value*
no sdlc counter non-productive

Parameters

value	Indicates how many times non-productive timer is started before an error is considered.

Default

15

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc counter non-productive 10
```

sdlc counter write-port

The write timer retry limit is used in conjunction with the write-port timeout value to provide the overall time before an outage message is issued.

Use the **no** form of the command to restore the default value.

Syntax

sdlc counter write-port *value*
no sdlc counter write-port

Parameters

value	Indicates how many times write-port timer is started before an error is considered.

Default

10

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc counter write-port 15
```

sdlc debug

Use this command to enable debug on SDLC packets. When debug is enabled all SDLC packets sent/received on a specific serial port are displayed in Event Log.

Use the **no** form of this command to change the setting to the default.

Syntax

```
sdlc debug
no sdlc debug
```

Parameters

None

Default

Disabled

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc debug
```

sdlc interframe-fill enable

Use this command to enable/disable interframe fill setting. When this option is enabled the serial card fills flags before and after the SDLC packet is sent. This is used when communicating with an AS 400.

Use the **no** form of this command to restore the default value.

Syntax

```
sdlc interframe-fill enable
no sdlc interframe-fill
```

Parameters

None

Default

Disabled

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc interframe-fill enable
```

sdlc link-station polladdress

Use this command to specify the SDLC poll address. This address identifies the link station on the port. If this address is already defined on the port then this command is treated as a re-definition. The command is used also to enter in link station configuration mode.

Use the **no** form of this command to delete the link station from the port.

Syntax

sdlc link-station polladdress *polladdress*
no sdlc link-station polladdress *polladdress*

Parameters

polladdress	SDLC poll address. This address identifies the link station on the port.

Default

No default.

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc link-station polladdress C2
```

sdlc max-received-window

Use this command to configure the size of receive window for the SDLC to use on this port. This value is used in XID negotiations and for NRM ports will influence the choice between Normal and Extended sequence numbering. The default is 0.

The value 0 has a special meaning. It instructs DLSw and the SDLC to use the receive window size passed in on an XID from a co-operating remote SDLC (in the case of local switching) or over TCP/IP.

Use the **no** form of the command to restore the default value.

Syntax

sdlc max-received-window *maxrecvwindow*
no sdlc max-received-window

Parameters

maxrecvwindow The size of receive window for the SDLC to use on this port.

Default

0

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc max-received-window 10
```

sdlc polladdress

Use this command to configure the address used by the SDLC provider when it accepts incoming calls if its role is negotiable or secondary.

Use the **no** form of this command to remove the poll address.

Syntax

```
sdlc polladdress polladdress
no sdlc polladdress
```

Parameters

polladdress	The poll address. It is a hexadecimal number (base 16) that indicated the address of the serial link. The range is 1 to ff.

Default

None

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc polladdress C1
```

sdlc primary-full-duplex

Use this command to specify that the primary station on this port can operate in full-duplex mode, meaning that it can send to one secondary station while another has the poll bit. If omitted, the primary operates in half-duplex mode, meaning it can not send to any other station if it does not have the poll bit.

Use the **no** form of the command to restore the default value.



Note: The primary and secondary full duplex settings are NOT "Constant Carrier". Very few IBM devices support true full duplex. Therefore, it is almost always incorrect to enable full duplex. If the line is primary/secondary two-way alternating communications, do NOT enable these options.

Syntax

```
sdlc primary-full-duplex
no sdlc primary-full-duplex
```

Parameters

None

Default

Half-duplex mode.

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc primary-full-duplex
```

sdlc role

Use this command to configure the SDLC role to be used on the port. The role is important for use on incoming calls.

Use the **no** form of this command to delete the role.

Syntax

```
sdlc role {pri|neg|sec}
no sdlc role
```

Parameters

pri	primary
sec	secondary
neg	negotiable

Default

None

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc role primary line-type switched
```

sdlc secondary-full-duplex

Use this command to specify that the secondary station(s) is capable of operating in full-duplex mode, meaning it can receive data while it holds the poll bit. When omitted, the secondary operates in half-duplex mode.

Use the **no** form of the command to restore the default value.



Note: The primary and secondary full duplex settings are NOT "Constant Carrier". Very few IBM devices support true full duplex. Therefore, it is almost always incorrect to enable full duplex. If the line is primary/secondary two-way alternating communications, do NOT enable these options.

Syntax

```
sdlc secondary-full-duplex
no sdlc secondary-full-duplex
```

Parameters

None

Default

Half-duplex mode.

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc secondary-full-duplex
```

sdlc send-rej

Use this command to specify if a REJ frame is sent for an out of order sequence.

Use the **no** form of the command to restore the default value.

Syntax

```
sdlc send-rej
no sdlc send-rej
```

Parameters

None

Default

REJ frame is not sent.

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc send-rej
```

sdlc timer idle-time

Use this timer to monitor for a completely inactive line. If nothing is transmitted or received over the line for the specified period of time determined by the product of the timer and the retry count, the line will be considered "idle" and an alert will be sent to the SDLC code (DLSw). The line will be inoperative until the client restarts the line. The value is in milliseconds.

Use the **no** form of the command to restore the default value.

Syntax

```
sdlc timer idle-time value
no sdlc timer idle-time
```

Parameters

value	Time used to monitor a completely inactive line.

Default

6000 ms

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc timer idle-time 15000
```

sdlc timer non-productive

For SDLC secondary, the Non-Productive receive timer gives the time allowed for receipt of a valid frame from the primary. This is usually set in conjunction with the retry limit to give a long timeout before outage message is issued (such as 30s).

For SDLC primary, this timer and count are used to produce an outage message when a secondary link station produces continuous frames without setting F-bit (final). The timer is specified in milliseconds.

Use the **no** form of the command to restore the default value.

Syntax

```
sdlc timer non-productive value
no sdlc timer non-productive
```

Parameters

value	Time allowed for receipt of a valid frame from the primary for the secondary station. For a primary station the time is used to monitor frames received from secondary station that do not have the final bit set.

Default

2000 ms

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc timer non-productive 5000
```

sdlc timer write-port

The Write timer controls the maximum amount of time allowed to transmit a complete frame. The timer should be based on the size of the frame, the line speed, and any overhead such as line turn-around, etc. A frame of 2k bytes on a 56,000bps line would require about 500 milliseconds. On a 9600bps line, about 2 seconds would be necessary. The timer is specified in milliseconds.

Use the **no** form of the command to restore the default value.

Syntax

```
sdlc timer write-port value
no sdlc timer write-port
```

Parameters

value	Time controlling the maximum amount of time allowed to transmit a complete frame.

Default

3000 ms

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-if)# sdlc timer write-port 4000
```

sendwindow

Use this command to configure the default sendwindow size for link level flow control if the value cannot be determined from an XID exchange.

Use the **no** form of the command to restore the default value.

Syntax

```
sdlc link-station polladress polladdress sendwindow sendwindowsize
no sdlc link-station polladdress polladdress sendwindow
```

Parameters

polladdress	SDLC poll address. This address identifies the link station on the port.
sendwindowsize	Default **sendwindow** size for link level flow control if the value cannot be determined from an XID exchange. This value overrides the default specified on the **dlsw local-peer** command.

Default

Use the XID or global default value.

Command Mode

Interface Configuration

Next Command Mode

Interface Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# sendwindow 7
```

start

Use this command to start an SDLC link station for DLSw.

Syntax

```
start
```

Parameters

Default

None

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# start
```

stop

Use this command to stop an SDLC link station for DLSw.

Syntax

stop

Parameters

Default

None

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# stop
```

timer disconnect

This timer controls the time in milliseconds before a DISC is retransmitted in the event of non-acknowledgement (for primary SDLC only). The value is specified in milliseconds.

Use the **no** form of the command to restore the default value.

Syntax

```
timer disconnect timervalue
no timer disconnect
```

Parameters

timervalue	Disconnect timer value.

Default

4000 milliseconds

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# timer disconnect 6000
```

timer fast-contact

This timer controls the timeout required before a SNRM or XID is retransmitted in the event of non-acknowledgement. Used for Primary SDLC only. The timer is specified in milliseconds.

Use the **no** form of the command to restore the default value.

Syntax

```
timer fast-contact timervalue
no timer fast-contact
```

Parameters

timervalue	Fast Contact timer value.

Default

4000 milliseconds

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# timer fast-contact 6000
```

timer fast-poll

This timer controls the timeout required before an adjacent secondary station is re-inserted into the polling list after being removed for non-response. A link station will be fast if there is an exchange of other than RR's (I-Frames) with it. The fast poll will continue until the fast retry limit is reached without any further exchange of I-Frames, at which time poll timing will be determined by the slow poll timer. If any I-Frames are sent or received while using the slow poll timer, polling will continue using the fast poll timer. The time is specified in milliseconds.

Use the **no** form of the command to restore the default value.

Syntax

timer fast-poll *timervalue*
no timer fast-poll

Parameters

timervalue	Fast Poll timer value.

Default

400 milliseconds

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# timer fast-poll 600
```

timer no-response

The No Response (or T1) Timer controls the time an SDLC primary link station waits (after having sent a frame with a poll bit) for a response frame before polling another station. This timer is restarted when a frame without the F-bit is received and stopped only when a frame with the F-bit is received. The timeout should be set to a value not less then twice the transmission time for the longest I-frame plus adjacent station frame processing time.

This timer controls the reply timeout, in tenths of seconds (1...600), for an SDLC link station. If the link station does not receive a response to a poll or message before the specified time expires then the appropriate error recovery will be initiated.

The recommended T1 timer is twice the longest I-Frame, multiplied by the window size, plus processing delay. The delay between transmit of "Poll" and receipt of "Final" is the propagation delay, plus serialization delay of the maximum sized frame multiplied by the maximum window size (typically 7), plus local processing and turnaround.

This timer has no effect on secondary SDLC link stations.

Use the **no** form of the command to restore the default value.

Syntax

timer no-response *timervalue*
no timer no-response

Parameters

timervalue No response timer value.

Default

40 seconds

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# timer no-response 600
```

timer rnr-limit

This timer controls the length of time, in minutes (1...90) that an SDLC link station allows its adjacent link station to remain in a busy (RNR) state before declaring it inoperative.

Use the **no** form of the command to restore the default value.

Syntax

```
timer rnr-limit timervalue
no timer rnr-limit
```

Parameters

timervalue RNR timer value.

Default

3 minutes

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# timer rnr-limit 5
```

timer slow-contact

This timer controls the timeout required before an SNRM or XID is retransmitted in the event of non-acknowledgement. This timer controls the slow poll contact timer in milliseconds. When the contact timer retry count expires, polling continues using this timer.

Use the **no** form of the command to restore the default value.

Syntax

```
timer slow-contact timervalue
no timer slow-contact
```

Parameters

*timervalue*Slow Contact timer value.

Default

4000 milliseconds

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# timer slow-contact 6000
```

timer slow-poll

This timer controls the timeout required before an adjacent secondary station is re-inserted into the polling list after being removed for non-response. The time is specified in milliseconds.

Use the **no** form of the command to restore the default value.

Syntax

```
timer slow-poll timervalue
no timer slow-poll
```

Parameters

timervalue	Slow Poll timer value.

Default

1000 milliseconds

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# timer slow-poll 2000
```

timer turn-around

This timer is used to allow a delay before an SDLC link station responds to a poll bit when it has no data to send. The user can configure this so that RRs are not turned around instantly, which helps prevent the link from being stressed. The timer is also applied to poll bits on received I-frames. It is often the case that the data in an I-frame carrying the poll bit will cause a response from the high level software. In this case, holding on to the poll bit for a short period allows the response data to reach the SDLC link station and be sent at once without requiring a pause for the next poll.

Use the **no** form of the command to restore the default value.

Syntax

```
timer turn-around timervalue
no timer turn-around
```

Parameters

timervalue	The RR Turn-around timer is in milliseconds. It is the time that SDLC link station waits before turning the poll bit around when it has no work to do.

Default

32 milliseconds

Command Mode

Link Station Configuration

Next Command Mode

Link Station Configuration

Required Privileges

System Management - Manage

User Management - None

Example

```
CES(config-ls)# timer turn-around 40
```

Privileged exec mode commands

This section describes all of the DLSW Privileged Exec mode NNCLI commands.

Command	Page
show dlsw circuits	page 1973
show dlsw directory	page 1975
show dlsw capabilities	page 1971
show dlsw port	page 1981
show dlsw sdlc	page 1984
show dlsw peers	page 1978
show dlsw mac-table	page 1977

show dlsw capabilities

This command displays information about the local DLSw node.

Syntax

`show dlsw capablities`

Parameters

None

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Example

The following is an example of the show dlsw capabilities command:

```
CES# show dlsw capabilities (modified output)
DLSW Node Capabilities:
   VendorID                                  = 000045(Nortel)
   Version string                           = NORTEL DLSW V1
   Local ip address                          =
150.150.150.150
   State                                     = ENABLED
   Maximum BTU size supported                = 1470
   Time between Tconn set up retries        = 15s
   SNA connection set up timeout             = 15s
   Single DLSw search timeout                = 15s
   Multiple DLSw search timeout              = 15s
   Preferred peer level timeout             = 200ms
   Circuit pending REACH_ACK timeout       = 10s
   Circuit idle timeout                      = 30s
   Maximum number of MAC cache entries   = 0
   Default send window                       = 7
   Default receive window                    = 7
   Default initial receive pacing window     = 1
   Back level flow control supported         = YES
   Local switching supported                 = YES
   MAC address translation                   = DISABLED
   Support for unconfigured peers            = DISABLED
   Time since DLSw started                   = 01:24:13
   Debug level                               = LOW
   Ips Trace                                 = DISABLED
   Trace Level                               = DETAIL
   Size of ips log file                      = 250kb
CES#
```

show dlsw circuits

This command displays the state of all circuits involving MAC address and SAP combination as a source address and destination.

Syntax

show dlsw circuits [{brief | detail} lmac *address* **rmac** *address***]**

Parameters

brief	Specifies the slot where the backup interface is installed.
detail	Specifies the port on the backup interface card.
address	Limits the display to a specific MAC/SAP pair

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Example

The following is an example of the **show dlsw circuit** command:

```
CES# show dlsw circuits detail localmac
04-00-12-34-87-65(04) rmac 00-0C-12-34-AB-CD(04)
DLSW Circuit Configuration:
  Local MAC address= 04-00-12-34-87-65(04)
  Remote MAC address= 00-0C-12-34-AB-CD(04)
  Circuit state   = CONNECTED
  Remote switch address= 172.12.11.12
  Port providing this circuit= 0/1
  Local circuit ID= b45f0003b4630003
  Remote circuit ID= 0002243545234235
  Time since creation of circuit= 500.00s
  Time since circuit entered this state= 100.00s
  Circuit priority= 2
  Current paced SSP message send window   = 6
  Current paced SSP message receive window = 1
  Current data send window= 6
  Current data receive window= 1
  Maximum data send window= 6
  Maximum data receive window= 1
  Total number of Halve Windows sent= 0
  Total number of Halve Windows received= 0
  Total number of Reset Windows sent= 0
  Total number of Reset Windows received= 0
CES#
```

show dlsw directory

This command displays the current DLSw directory.

Syntax

show dlsw directory [*address***]**

Parameters

address	(Optional) Limits the display to a specific local MAC/SAP pair (the default is all).

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Example

The following is an example of the **show dlsw directory** command:

```
CES# show dlsw directory
DLSW directory entries:
  Total number of MAC entries    = 2
  Total number of successful MAC searches= 7
  Total number of unsuccessful MAC searches  = 2
  Mac address        Location entry
  ------------------------------------
  04-00-C2-B2-A2-02   10.55.2.180
  00-0C-98-98-89-89    LOCAL
CES#
```

For each MAC entry, this command lists the MAC address and location of the entry.

show dlsw mac-table

This command displays the MAC translation tables (local and remote).

Syntax

`show dlsw mac-table`

Parameters

None

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Example

The following is an example of the **show dlsw circuit** command (s/d means source/destination addresses that are translated):

```
CES# show dlsw mac-table
DLSW MAC Translation Tables
  old address(s/d)  new address
  040012348765(s)000C1234ABCD
CES#
```

show dlsw peers

This command displays information about DLSw peers.

Syntax

show dlsw peers [*ip-adddress* **[brief|detail]]**

Parameters

brief	(Optional) Provides brief output. This is the default.
detail	(Optional) Provides detailed output.
ip-address	(Optional) Indicates the address of remote DLSW.

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Example

```
CES# show dlsw peers 172.13.9.12 detail (modified output)
Partner address                                =
10.77.30.130
 Type                                           = Normal
 Admin. state                                   = Enabled
 State                                          = Connected
 Number of circuits                             = 0
 Dlsw v1                                        = Enabled
 Backup peer                                    = No
 Time since creation                            = 01:05:35
 Time since connected                          = 01:05:00
 Total number of created circuits               = 2
 Time since disconnected                        = 00:00:00
 Reason for disconnection                       = Last
Circuit Disconn
 Flow control mode                             = Pacing
 Cost                                          = 5
 Partner Version                               = rfc2166
 Partner Vendor ID                              = 000045
 Partner Version string                         = NORTEL
DLSW V1
 Partner's initial pacing window               = 1
 Circuit inactivity timeout                     = 180s
 Total number of data packets received         = 5
 Total number of data packets sent              = 5
 Total number of bytes in data packets received = 100
 Total number of bytes in data packets sent     = 200
 Total number of control packets received       = 0
 Total number of control packets sent           = 0
 Total number of CANUREACH_ex messages received = 0
 Total number of CANUREACH_ex messages sent     = 0
 Total number of ICANREACH_ex messages received = 0
 Total number of ICANREACH_ex messages sent     = 0
CES#
```

show dlsw port

This command displays current status information about ports.

Syntax

show dlsw port [*port-id* **[brief|detail]]**

Parameters

brief	(Optional) Provides brief output (this is the default)
detail	(Optional) Provides detailed output.
port-id	Optional) Provides the identity of the port to be displayed.The values are 0..6/1..4

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Example

The following are examples of the **show dlsw port** command:

```
CES#show dls sdlc port
DLSW Port Configuration:
    Name  Type       Status
    ----   ----     ---------
  1> 0/1   ETHERNET Enabled
  2> 1/1    SDLC     Enabled
CES#

CES# show dlsw port 0/1 detail
DLSW Port Configuration:
  Interface Name= LAN 0/1
  Type            = Ethernet
  State           = Enabled
  Maximum receive window= 7
  Lan type        = 802.3/DIX
  Local MAC address= 04-00-12-34-98-76
  I Frame acknowledgement timeout= 5000ms
  P bit response timeout= 5000ms
  T2 timeout   = 100ms
  REJ response timeout= 30s
  Busy condition timeout= 30s
  RR keep-alive interval= 30s
  Maximum number of retries= 10
  Number of link stations= 1
  Total number of I frames sent= 0
  Total number of I frames received= 0
```

Where the port type is SDLC, the following additional information is displayed:

```
SDLC Role
Primary full duplex
Secondary full duplex
Polladdress
Send REJ frame
Interframe fill
Activation sequence
Idle line timer
Idle line retry limit
Non-productive timer
Non-productive retry-limit
Port write timer
Port write retry limit
SDLC debug status
```

Where the port type is LLC2, the following additional information is displayed:

```
Lan type
Local MAC address (Token Ring)
I Frame acknowledgement timeout
P bit response timeout
T2 timeout
REJ response timeout
Busy condition timeout
RR keep-alive interval
Maximum number of retries
Number of link stations
Total number of I frames sent
Total number of I frames received
```

show dlsw sdlc

This command displays information about SDLC link stations.

Syntax

show dlsw sdlc [**port** *port-id* **polladress** *poll_adddress* **[brief|detail]]**

Parameters

brief	(Optional) Provides brief output. This is the default.
detail	(Optional) Provides detailed output.
port-id	(Optional) Limit the display to a specific port-id. The default is all.
sdlc_address	(Optional) Limit the display to a specific link station (the default is all). It is 1..2 hexadecimal digits.

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Example

The following is an example of the **show dlsw sdlc** command:

```
CES# show dlsw sdlc
  DLSW SDLC Link Stations configuration:
  Port namePoll address
  --------------------
1> 1/1         C1
CES#

CES# show dlsw sdlc port 1/1 polladdress C1 detail
  DLSW SDLC Link Stations configuration:
  Link station state = Enabled
  Active              = YES
  SDLC Role        = PRIMARY
  Group poll address = NOT DEFINED
  Poll frame       = XID
  Local address of corresponding circuit =
04-00-12-34-87-65(04)
  Remote address of corresponding circuit =
00-0C-12-34-AB-CD(04)
  Send window size = 7
  Receive window size = 7
  XID string       = 00000000
  Fast contact timer = 4000ms
  Fast contact counter = 4
  Slow contact timer = 4000ms
  Slow contact counter = 65535
  Fast negative poll timer = 400ms
  Fast negative poll counter = 16
  Slow negative poll timer = 1000ms
  Slow negative counter = 65535
  No response (T1) timer = 3s
  No response counter = 10
  Busy timer       = 3min
  Busy timer retry = 5
  Disconnect timer = 4000ms
  Disconnect timer retry = 3
  Turn-around timer (RR) = 32ms
  Number of retries per sequence = 10
  Number of retries sequences= 5
```

```
  Current interval between retry sequences= 5s
  Last fail control in=
  Last fail control out=
  I-frames out       = 30
  I-frames in        = 12
  UI-frames out      = 26
  UI-frames in       = 32
  XID-frames out     = 5
  XID-frames in      = 2
  REJ-frames out     = 1
  REJ-frames in      = 4
  FRMR-frames out = 2
  FRMR-frames in     = 7
  Last fail FRMR Info=
CES#
```

Debug mode commands

This section describes DLSw debugging commands. The commands are available in the configuration mode.

Command	Page
dlsw debug_level	page 1986
dlsw ips-trace enable	page 1988

dlsw debug_level

Use this command to configure the problem determination logging.

Use the **no** form of the command to restore the default value.

Syntax

```
dlsw debug-level {low|medium|high|none}
no dlsw debug-level
```

Parameters

low	Only errors|exceptions are logged
medium	Medium level errors are logged.
high	Minimal errors are logged.
none	No errors are logged.

Default

Low

Command Mode

General Configuration

Next Command Mode

General Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

Example

```
CES(config-if)# dlsw debug-level high
```

dlsw ips-trace enable

Use this command to enable or disable internal DLSw code tracing. This command logs the traces to a file located in the ide0\system\ directory. You can FTP the file from this location in order to examine it.

Use the **no** form of this command to disable tracing.

Syntax

```
dlsw ips-trace enable
no dlsw ips-trace enable
```

Parameters

None

Default

Disabled

Command Mode

General Configuration

Next Command Mode

General Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

Example

```
CES(config-if)# dlsw ips-trace enable
```

tx-ringsize

Use this command to set the size of the transmit ring.

Syntax

```
tx-ringsize
no tx-ringsize
```

Parameters

transmit ring size	Value must be a power of 2. Valid ring sizes are 1,2, 4, 8, 16, 32, 64, 128. <1-128>

Default

Command mode

Interface Configuration

Next command mode

Interface Configuration

Required privileges

System Management – None
User Management – Manage

Prerequisites

None

Related commands

Example

```
CES(config-if)# tx-ringsize <transmit ring size>
CES(config-if)# no tx-ringsize
```

Chapter 48
Digital Data Service (DDS) configuration commands

This section describes DLSw Digital Data Service (DDS) CLI commands.

A DDS CSU/DSU is often called a 56K/64K CSU/DSU. These DDS CLI commands operate at the controller, or physical layer, and the interface, or data link layer. DDS supports frame relay, PPP, and SDLC layer 2 protocols. These protocols are configured as they currently are; there is no modification necessary to run over a DDS link.

Command	Page
clock rate	1992
clock source	1994
controller 56k	1996
show controller 56k	1998
transmit-data-monitor	2000

clock rate

Use this command from the controller DDS configuration mode to configure the clock rate used (or data rate).

Syntax

clock rate *{56|64}*

Parameters

56	56 kilobits per seconds.
64	64 kilobits per seconds.

Default

56

Command Mode

DDS Controller Configuration mode

Next Command Mode

DDS Controller Configuration mode

Required Privileges

System Management - Manage

User Management - None

Example

Example of a successful configuration of clock rate on DDS card

```
CES(config-controller)# clock rate 56k
CES(config-controller)#
```

clock source

Use this command from the controller DDS configuration mode to configure the clock source used at the physical layer.

Syntax

clock source *{internal|line}*

Parameters

line	Clock source is derived from the received signal. This is the only valid mode for 64 k clock rate
internal	Clock source is the local on-board oscillator

Default

Internal

Command Mode

DDS Controller Configuration mode

Next Command Mode

DDS Controller Configuration mode

Required Privileges

System Management - Manage

User Management - None

Example

Example of a successful configuration of clock source on DDS card

```
CES(config-controller)# clock source line
CES(config-controller)#
```

controller 56k

This command enters the DDS controller configuration mode.

The **exit** command leaves the controller configuration mode and returns to the general configuration mode.

Syntax

```
controller 56k slot/port
exit
```

Parameters

slot	Specifies the card slot on a Nortel VPN Router <1-6>, depending on the gateway model.
port	Specifies the port on a DDS card. For DDS, 1 is mandatory.

Default

None

Command Mode

General configuration

Next Command Mode

Controller configuration

Required Privileges

System Management - Manage

User Management - None

Example

Below is an example of entering the DDS controller configuration mode.

```
CES(config)# controller 56k 1/1
CES(config-controller)#exit
CES(config)#
```

Error Messages

The following error messages may be returned:

```
% Slot/Port and Type mismatch
% Invalid Slot/Port
```

show controller 56k

Use this Privileged Exec command to display DDS attributes.

Syntax

show controller 56k [slot/port]

Parameters

slot	Specifies the card slot on a Nortel VPN Router <1-6>, depending on the gateway model.
port	Specifies the port on a card on a Nortel VPN Router <1-4 >, depending on I/O card model. For DDS, the only permitted value is 1.

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Example

Below is an example of a successful display of information about the DDS card on slot 1 port 1:

```
CES# show controller 56k 1/1
DDS CSU/DSU Interface 3/1 Configuration
    Clock rate            :  56 kbps
    Clock source          :  Internal
    Transmit data monitor :  ENABLED
    Data inversion        :  Normal
    Encapsulation         :  PPP
CES#
```

transmit-data-monitor

Use this command from the controller DDS configuration mode to enable the transmit data monitor function.

Use the **no** form to disable the feature.

The transmit-data-monitor feature is available to prevent latching loopback conditions.

When receiving data, the hardware detects the latching loopback sequence, and guards against accidental activation with regard to when the data was received and over what period of time it received that data.

There is no support in hardware for detecting and preventing latching loopbacks on the transmit side, so the detection must be done in software. TR 62310 mandates that a DCE should not transmit more than 29 Loopback Enable (LBE) bytes out of any 40 consecutive bytes, in order to prevent activating a latching loopback. This means that when the Transmit Data Monitor feature is enabled, each packet needs to be inspected for this characteristic. If a particular packet matches this characteristic, then it will get dropped and a Framing Error counter will be incremented. Performance-wise, even though 64K is a low speed link, the software inspection of every packet in 40 byte increments does affect CPU performance. However, the 40 byte window does not have to be maintained across packets, as the HDLC flags which delineate packets serve as automatic LBE pattern breakers.

Syntax

```
[no] transmit-data-monitor enable
```

Parameters

None

Default

Internal

Command Mode

DDS Controller Configuration mode

Next Command Mode

DDS Controller Configuration mode

Required Privileges

System Management - Manage

User Management - None

Example

Below is an example of a successful configuration of the clock source on a DDS card.

```
CES(config-controller)# transmit-data-monitor enable
CES(config-controller)#
```

Chapter 49
BGP configuration commands

This section describes Routing BGP NNCLI commands. Most commands follow Cisco IOS command format. Please note that Routing BGP NNCLI commands (with the exception of the commands indicated by *) are either identical or a subset of Cisco IOS commands, and that they could be executed on Cisco routers and vice versa.

Commands	Page
auto-summary	2005
bgp always-compare-med	2007
bgp client-to-client reflection	2008
bgp cluster-id	2010
bgp default local-preference	2011
bgp multiple-paths	2013
bgp public	2014
bgp redistribute-internal	2015
bgp router-id	2017
default-information originate	2018
default-metric	2020
ip as-path access-list	2021
ip community-list	2024
match as-path	2026
match community	2028
match ip address	2030
multiple-paths	2032

Commands	Page
neighbor	2033
neighbor advertisement-interval	2034
neighbor allow-as-in	2036
neighbor default-originate	2037
neighbor distribute-list	2039
neighbor ebgp-multihop	2041
neighbor enable	2042
neighbor filter-list	2043
neighbor next-hop-self	2045
neighbor loop-detection	2047
neighbor password	2048
neighbor remote-as	2050
neighbor retry-interval	2051
neighbor route-map	2053
neighbor route-reflector-client	2055
neighbor send-community	2056
neighbor shutdown	2058
neighbor update-source	2059
neighbor timers	2061
neighbor weight	2062
network	2065
redistribute	2066
route-map	2068
route-reflector enable	2070
router bgp	2071
set as-path	2073
set community	2075
set ip next-hop	2078
set local-preference	2079
set metric	2080

Commands	Page
set origin	2081
set weight	2083
show ip as-path access-list	2084
show ip bgp	2085
show ip bgp community	2088
show ip bgp neighbors	2089
show ip bgp networks	2094
show ip bgp redistribution	2095
show ip bgp redistribute-routes	2096
show ip bgp regexp	2098
show ip bgp regexp	2098
show ip community-list	2102
show ip route-map	2103
synchronization	2104
timers bgp	2105

auto-summary

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the auto-summary command in router configuration mode. To disable this feature and transmit sub-prefix routing information across classful network boundaries, use the no form of this command.

This NNCLI command first appeared in CES Release 6.0.

Syntax

[no] **auto-summary**

Parameters

Default

Disabled

Command Mode

Router BGP Configuration

Next Command Mode

Router BGP Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

Example

Route summarization reduces the amount of routing information in the routing tables.

By default, BGP accepts subnets redistributed from an IGP. To advertise and carry subnet routes in BGP, use an explicit network command or the no auto-summary command. If you disable auto-summarization and have not entered a network command, you will not advertise network routes for networks with subnet routes unless they contain a summary route.

In the following example, network numbers are not summarized automatically:

```
CES# configure terminal
CES(config)# router bgp 500
CES(config-bgp)# no auto-summary
```

bgp always-compare-med

This command allows configuration of BGP to always compare Multi-Exit Discriminator (MED) metrics from neighbors coming from different ASs. Use the **no** form of this command to change the value to its default value.

This NNCLI command first appeared in CES Release 5.1.

Syntax

[no] bgp always-compare-med

Parameters

None

Default

Disabled

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

default-metric *number*

Example

Example of a successful enabling of “Always Compare MED” parameter:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# bgp always-compare-med
```

Example of a successful disabling of “Always Compare MED” parameter:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no bgp always-compare-med
```

bgp client-to-client reflection

Use this command to enable client-to-client route reflection. Use the no form of this command to disable client-to-client route reflection. This NNCLI command first appeared in CES Release 6.0.

Syntax

[no] **bgp client-to-client reflection**

Parameters

None

Default

Disabled

Command Mode

Router BGP Configuration

Next Command Mode

Router BGP Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

route-reflector enable

Example

Example of a successful enabling of client to client reflection:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-router)# bgp client-to-client reflection
```

Example of a successful disabling of client to client reflection:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-router)# no bgp client-to-client reflection
```

bgp cluster-id

Use this command to configure a BGP cluster ID. Use the no form of this command to delete a BGP cluster ID. This NNCLI command first appeared in CES Release 6.0.

Syntax

[no] **bgp cluster-id cluster-id**

Parameters

cluster-id—Specifies cluster ID number. Permitted values are between 0 and 4294967295.

Default

None

Command Mode

Router BGP Configuration

Next Command Mode

Router BGP Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

route-reflector enable

Example

Example of a successful setting BGP cluster ID number to 1000:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-router)# bgp cluster-id 1000
```

Example of a successful deleting BGP cluster ID number 1000:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-router)# no bgp cluster-id
```

bgp default local-preference

You can define a particular path as more preferable or less preferable than other paths by changing the default local preference value of 100. Use this command to assign a different default local preference value. Use the **no** form of this command to change the value back to its default value.

This NNCLI command first appeared in CES Release 5.1.

Syntax

default local-preference *value*
no default local-preference

Parameters

value	Local preference value. Permitted range is between 0 and 4294967295.

Default

Local preference value of 100

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

`set local-preference`

Example

Generally, the default value of 100 allows you to easily define a particular path as less preferable than paths with no local preference attribute. The preference is sent to all routers and access servers in the local AS.

Example of a successful setting of a default local preference parameter to 200:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# bgp default local-preference 200
```

Example of a successful reset to default value of “default local-preference” parameter:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no bgp default local-preference
```

bgp multiple-paths

This command indicates the number of maximum paths that are installed for the same destination. The no form deletes the existing maximum path number and set it to default value 1. For BGP this is used for updates received from (E-BGP peering) the same AS and with the same cost.

This NNCLI command first appeared in CES Release 6.0.

Syntax

```
bgp multiple-paths maximum-number
no bgp multiple-paths
```

Parameters

maximum-number	Maximum number of parallel routes the BGP protocol installs in a routing table, in the range from 1 to 6.

Default

1

Command Mode

Router BGP Configuration

Next Command Mode

Router BGP Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

Example

Example of successful setting maximum-paths to 6

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# maximum-paths 6
```

Example of a successful resetting maximum-paths parameter to its default value:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no maximum-paths
```

bgp public

Use this command to enable BGP protocol over public interfaces. Use the no form of this command to disable BGP on public interfaces.

This NNCLI command first appeared in CES Release 6.0.

Syntax

```
bgp public
no bgp public
```

Parameters

None

Default

BGP is disabled over public interfaces

Command Mode

Global Configuration

Next Command Mode

Global Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

None

Example

Example of a successful enabling BGP over public:

```
CES# configure terminal
CES(config)# bgp public
CES(config)#
```

bgp redistribute-internal

Use this command to configure redistribution of imported routes (via network or redistribution command) to internal BGP peers. Use the **no** form of this command to disable sending of imported routes to I-BGP peers.

This NNCLI command first appeared in CES Release 6.0.

Syntax

[no] **bgp redistribute-internal**

Parameters

None

Default

Enabled

Command Mode

Router BGP Configuration

Next Command Mode

Router BGP Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

Example

Example of a successful enable of redistribution of imported routes to IBGP peers:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# bgp redistribute-internal
```

bgp router-id

Use this command to set the BGP identifier of the local system. Use the **no** form of this command to delete the value of router ID and to restore the default value of the router ID.

This NNCLI command first appeared in CES Release 5.1.

Syntax

```
bgp router-id ip-address
no bgp router-id ip-address
```

Parameters

ip-address	Specifies IP address of the local BGP component

Default

The router ID is set to the IP address of a virtual interface if one is configured. If no virtual interfaces are configured, the highest IP address is configured for a physical interface on that router. Peering sessions will be reset if the router ID is changed.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

Example of a successful setting of BGP router ID parameter:

```
CES# configure terminal
CES(config)# router bgp 500
CES(config-bgp)# bgp router-id 192.12.23.34
```

Example of a successful deletion of the BGP router ID parameter:

```
CES# configure terminal
CES(config)# router bgp 563
CES(config-bgp)# no bgp router-id
```

default-information originate

To control the redistribution of a protocol or network into the BGP, use the **default-information originate** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

[no] default-information originate

Parameters

None

Default

Disabled

Command modemode

Router BGP Configuration

Next command mode

Required privileges

System Management — Manage

User Management — None

Related commands

None

Example

The **default-information originate** command should be used if the network operator needs to control the redistribution of default routes. Using the **default-information originate** command in BGP is similar to using the **network** command. However, to achieve the same result as configuring the **network** command with the route 0.0.0.0, the **default-information originate** command requires an explicit redistribution of the route 0.0.0.0. The **network** command requires only that route 0.0.0.0 is specified in the Interior Gateway Protocol (IGP) routing table. For this reason, the **network** command is preferred for redistributing default routes and protocols into BGP. But **network** command is not implemented yet in CES.

```
CES# configure terminal
CES(config)# router bgp 500
CES(config-bgp)# redistribute static
CES(config-bgp)# default-information originate
```

default-metric

Use this command to define the metric used to discriminate between multiple exit points to an adjacent AS. Use the **no** form of this command to change the metric to its default value.

This NNCLI command first appeared in CES Release 5.1.

Syntax

[no] default-metric *number*

Parameters

number	Permitted values are between 1 and 42949667245.

Default

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

bgp always-compare-med
route-map *map-tag* [**permit | deny**] [*sequence-number*]

Example

Example of a successful setting default metric parameter to 1000:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# default-metric 1000
```

Example of a successful resetting the Default Metric parameter to its default value:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no default-metric
```

ip as-path access-list

To define a community list for Border Gateway Protocol (BGP) autonomous system (AS) path access list it, use the **ip as-path access-list** global configuration command. To disable the use of the access list, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

ip as-path access-list *access-list-number* {**permit|deny**} *as-regular-expression*
no ip as-path-list *access-list-number*

Parameters

access-list-number	Integer from 1 to 199 that identicates the regular expression access list number.
permit	Permits access for matching conditions.
deny	Denies access to matching conditions.
As-regular-expression	Autonomous system in the access list using a regular expression.

A BGP path can be described as a sequence of characters drawn from the alphabet consisting of the set of AS numbers plus the following punctuation characters: '^' the start of a path, '$' the end of a path, '{' the start of an AS_SET, '}' the end of an AS_SET.

Note that an AS number, for example 1234, is a single character in the alphabet. Where necessary to unambiguously delimit characters, white space is used. However, white space is not considered part of the alphabet. For example, to specify an AS number of 23 followed by AS number 45, the string **23 45** should be used.

To match a single character in a path, the following forms may be used:

- The character itself
- '.' which matches any single character
- '.*' which matches 0 or more any characters
- '.+' which matches 1 or more any characters
- '_' (underscore) which matches 0 or 1 instance of any punctuation character (^,$,{,})
- [ ] which is used to specify a set of characters. For example, "[1234 45 6789]" or "[{$]". All members of set must be the same type, either AS numbers or punctuation.
- '-' which are used within brackets to specify a range of AS numbers. For example, "[23-45]" will match any AS number between 23 and 45.

- '^' which when used as the first item within brackets specifies any AS number except the set specified. For example, to specify any AS number except 11 or 13, use "[^11 13]". Also, the '^' character may be used in conjunction with '-' to specify any AS number except the specified range: "[^100-200]" will match any AS number except those between 100 and 200.

Default

No access list is defined.

Command mode

Global configuration

Next command mode

Global configuration

Required privileges

System Management — Manage

User Management — None

Related commands

match as-path
neighbor filter-list
show ip as-path access-list
set as-path

Example

You can specify an access list filter on both inbound and outbound BGP routes. Each filter is an access list based on regular expressions. If the regular expression matches the representation of the AS path of the route as an ASCII string, then the **permit** or **deny** condition applies. The AS path does not contain the local AS number. Use the **ip as-path access-list** global configuration command to define an BGP access list, and the **neighbor** router configuration command to apply a specific access list.

The following example specifies that the BGP neighbor with IP address 128.125.1.1 is not sent advertisements about any path through or from the adjacent AS 123:

```
CES(config)# ip as-path access-list 1 deny _123_
CES(config)# ip as-path access-list 1 deny ^123$
CES(config)# router bgp 109
CES(config-bgp)# neighbor 129.140.6.6 remote-as 123
CES(config-bgp)# neighbor 128.125.1.1 remote-as 47
CES(config-bgp)# neighbor 128.125.1.1 filter-list 1 out
```

ip community-list

To define a community list for Border Gateway Protocol (BGP) and control access to it, use the **ip community-list** global configuration command. To delete the community list, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

ip community-list *community-list-number* {**permit|deny**} *community-number*
no community-list *community-list-number*

Parameters

community-list-number	integer from 1 to 99 that identifies one or more permit or deny groups of communities
permit	permits access for matching conditions
deny	denies access to matching conditions
community-number	community number configured by a set community command. Valid value is one of the following: • **A number from 1 to 1000** — You can specify a single number or multiple numbers separated by a space. • **Internet** —The Internet community. • **no-export** — Routes with this community are sent to peers in other ASs. • **local-as** — Do not advertise this route to peers outside the local AS. The route will not be advertised to other systems or sub-ASs when confederations are configured. • **no-advertise** — Do not advertise this route to any peer (internal or external).

Default

Once you permit a value for the community number, the community list defaults to an implicit deny for everything else that has not been permitted.

Command mode

Global configuration

Next command mode

Global configuration

Required privileges

System Management — Manage

User Management — None

Related commands

set community
show ip community-list

Example

In the following example, CES permits all routes except the routes with the communities 5 and 10 or 10 and 15:

```
CES(config)# ip community-list 1 deny 5 10
CES(config)# ip community-list 1 deny 10 15
CES(config)# ip community-list 1 permit internet
```

The following example permits all routes within the local AS:

```
CES(config)# ip community-list 1 permit local-as
```

match as-path

To match a Border Gateway Protocol (BGP) AS path access list, use the **match as-path** route-map configuration command. To remove a path list entry, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

match as-path *path-list-number*
no match as-path *path-list-number*

Parameters

path-list-number	Autonomous system path access list. An integer from 1 to 199.

Default

No AS path list is defined.

Command mode

Route Map Configuration

Next command mode

Route Map Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

route-map — Defines the conditions for redistributing routes from one protocol to another.

set as-path — Modifies an AS path for BGP routes

set community — Sets the BGP communities attribute

set local preference — specifies a preference value for the AS path

set weight — Specifies the BGP weight for the routing table

Example

The values set by the **match as-path** and **set weight** commands override global values. For example, the weights assigned with the **match as-path** and **set weight** route-map configuration commands override the weight assigned using the **neighbor weight** command.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified.

The following example sets the AS path to match BGP AS path access list 20:

```
CES(config)# route-map igp2bgp
CES(config-route-map)# match as-path 20
```

match community

To match a Border Gateway Protocol (BGP) community, use the **match community** command in route-map configuration mode. To remove the **match community** command from the configuration file and restore the system to its default condition where the software removes the BGP community list entry, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

match community *standard-list-number*
no match community *standard-list-number*

Parameters

standard-list-number	Specifies a standard community list number from 1 to 99 that identifies one or more permit or deny groups of communities.

Default

No community list is matched by the route map.

Command modemode

Route Map Configuration

Next command mode

Route Map Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

ip community-list — Creates a community list for BGP and controls access to it.

route-map — Defines the conditions for redistributing routes from one protocol to another

set weight — Specifies the BGP weight for the routing table.7.2.8Example

A route map can have several parts. Any route that does not match at least one **match** command relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified.

Matching based on community list number or name is one of the types of **match** commands applicable to BGP.

The following example shows that the routes matching community list 1 will have the weight set to 100. Any route that has community 109 will have the weight set to 100.

```
CES(config)# ip community-list 1 permit 109
CES(config)# route-map set_weight
CES(config-route-map)# match community 1
CES(config-route-map)# set weight 100
```

The following example shows that the routes matching community list 1 will have the weight set to 200. Any route that has community 109 alone will have the weight set to 200.

```
CES(config)# ip community-list 1 permit 109
CES(config)# route-map set_weight
CES(config-route-map)# match community-list 1
CES(config-route-map)# set weight 200
```

match ip address

This command examines the match criteria ip address to determine the action of the associated set commands in BGP route map configuration. The no form disables the match of ip address.

Syntax

[no] match ip address *access-list-name*

Parameters

access-list-name Name of the access-list.

Default

None

Command mode

Route map Configuration

Next command mode

Route map Configuration

Prerequisites

System Management — Manage

User Management — None

Related commands

Example

This example examines any match of ip address specified by access list my-access-list-name.

```
CES(config-route-map)# match ip address my-access-list-name
```

multiple-paths

This command indicates the number of maximum paths that are installed for the same destination. The no form deletes the existing maximum path number and set it to default value 1. For BGP this is used for updates received from (E-BGP peering) the same AS and with the same cost.

This NNCLI command first appeared in CES Release 5.1.

Syntax

```
multiple-paths maximum-number
no multiple-paths
```

Parameters

maximum-number	Maximum number of parallel routes the BGP protocol installs in a routing table, in the range from 1 to 6.

Default

1

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

Example of successful setting maximum-paths to 6

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# maximum-paths 6
```

Example of a successful resetting maximum-paths parameter to its default value:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no maximum-paths
```

neighbor

Use this command to configure a new BGP neighbor. Use the **no** form of this command to delete the neighbor.

This NNCLI command first appeared in CES Release 5.1.

Syntax

[no] neighbor *ip-address*

Parameters

ip-address	Specifies IP address of the remote BGP peer.

Default

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

Example of a successful configuration of a new neighbor whose BGP IP address is 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# neighbor 192.47.20.34
```

Example of a successful deletion of a neighbor whose BGP IP address is 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no neighbor 192.47.20.34
```

neighbor advertisement-interval

Use this command to configure a new advertisement interval for a specified BGP neighbor. It overrides the BGP advertisement interval value. Use the **no** form of this command to return the value to the global advertisement interval value.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **advertisement-interval** *seconds*
no neighbor *ip-address* **advertisement-interval**

Parameters

ip-address	Specifies IP address of the neighbor BGP component.
seconds	Specifies time between two successive BGP advertisements. Permitted range is between 0 and 600 seconds.

Default

30 seconds

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

This is an example of a successful configuration of a new advertisement interval of 120 seconds for a neighbor whose BGP IP address is 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# neighbor 192.47.20.34
advertisement-interval 120
CES(config-bgp)#
```

This is an example of a successful deletion of the advertisement interval for a neighbor whose BGP IP address is 192.47.20.34. The value of this neighbor's advertisement interval will be returned to the BGP advertisement value:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no neighbor 192.47.20.34
advertisement-interval
CES(config-bgp)#
```

neighbor allow-as-in

To disable loop detection for updates received from a neighbor use the neighbor allow-as-in router configuration command. To enable loop detection, use the **no** form of this command.

This NNCLI command first appeared in CES Release 6.0.

Syntax

```
[no] neighbor ip-address allow-as-in
```

Parameters

None

Default

Disabled

Command Mode

Router BGP Configuration

Next Command Mode

Router BGP Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

Example

```
CES(config)# router bgp 109
CES(config-bgp)# no neighbor 131.108.1.1 allow-as-in
```

neighbor default-originate

To allow a Border Gateway Protocol (BGP) speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the **neighbor default-originate** command in address family or router configuration mode. To send no route as a default, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **default-originate**
no neighbor *ip-address* **default-originate**

Parameters

ip-address	Specifies IP address of the neighbor BGP component.

Default

No default route is sent to the neighbor.

Command modemode

Router BGP Configuration

Next command modemode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

This command does not require the presence of 0.0.0.0 in the local router.

In the following router configuration example, the local router injects route 0.0.0.0 to the neighbor 160.89.2.3 unconditionally:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# neighbor 160.89.2.3
CES(config-bgp)# neighbor 160.89.2.3 remote-as 100
CES(config-bgp)# neighbor 160.89.2.3 default-originate
```

neighbor distribute-list

To distribute BGP neighbor information as specified in an access list, use **neighbor distribute-list** command. Use the **no** form of this command to delete an entry. Right now it is possible to attach 1 distribute-list to a neighbor.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **distribute-list** *access-list-name*{**in|out**}
no neighbor *ip-address* **distribute-list** {**in|out**}

Parameters

ip-address	Specifies IP address of the neighbor BGP component.
access-list-name	Name of a standard access list.
in	Specifies incoming advertisements only.
out	Specifies outgoing advertisements only.

Default

No BGP neighbor is specified

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

access-list — Defines a standard IP access list

ip as-path access-list — Defines a BGP-related access list

neighbor filter-list — Sets up a BGP filter

Example

Using a distribute list is one of several ways to filter advertisements. Advertisements can also be filtered by using the following methods:

- Autonomous system path filters can be configured with the **ip as-path access-list** and **neighbor filter-list** commands.
- The **access-list (IP standard)** commands can be used to configure standard access lists for the filtering of advertisement.
- The **route map** command can be used to filter advertisements.

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# neighbor 192.47.20.34 distribute-list test
out
CES(config-bgp)#
```

neighbor ebgp-multihop

Use this BGP neighbor command to enable BGP connections to external peers residing on networks that are not directly connected. Use the **no** form of this command to delete the value.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **ebgp-multihop**
[no] neighbor *ip-address* **ebgp-multihop**

Parameters

ip-address	Specifies IP address of the neighbor BGP component.

Default

Only directly connected neighbors are allowed.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

This is an example of a successful enabling of BGP multi-hop for a specified neighbor:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# neighbor 192.47.20.34 ebgp-multihop
CES(config-bgp)#
```

This is an example of a successful disabling of BGP multihop for a specified neighbor:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no neighbor 192.47.20.34 ebgp-multihop
CES(config-bgp)#
```

neighbor enable

This command enables the administrative state of BGP neighbor. The **no** form disables the neighbor.

Syntax

[no] neighbor *ip-address* **enable**

Parameters

ip-address	IP address of the neighbor.

Default

The neighbor is disabled after creation.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Prerequisites

System Management — Manage

User Management — None

Example

This example disables the neighbor 11.254.1.20.

```
CES(config-bgp)# no neighbor 11.254.1.20 enable
```

neighbor filter-list

Use this command to establish a BGP filter to be applied to incoming or outgoing advertisements to a specified neighbor. Use the **no** form of this command to disable the function. It is possible to attach one filter list to an neighbor.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **filter-list** *access-list-number* {**in|out**}
[no] neighbor *ip-address* **filter-list** *access-list-number* {**in|out**}

Parameters

ip-address	Specifies IP address of the neighbor BGP component.
access-list-number	Specifies Access List Number. Permitted values are all defined AS-path Access Lists with **ip as-path access-list** command.
in	Specifies incoming advertisements only.
out	Specifies outgoing advertisements only.

Default

No filter is used.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

neighbor distribute-list — distributes BGP neighbor information as specified in an access list

ip as-path access-list — defines a BGP-related access list

Example

This command establishes filters on both inbound and outbound BGP routes.

In the following router configuration mode example, the BGP neighbor with IP address 128.125.1.1 is not sent advertisements about any path through or from the adjacent AS 123:

```
CES(config)# ip as-path access-list 1 deny _123_
CES(config)# ip as-path access-list 1 deny ^123$

CES(config)# router bgp 100
CES(config-bgp)#neighbor 128.125.1.1 remote-as 40
CES(config-bgp)#neighbor 128.125.1.1 filter-list 1 out
```

neighbor next-hop-self

Use this command to disable next hop processing on BGP updates to the specified neighbor. Configuring this command causes the current router to advertise its peering address as the next hop for the specified neighbor. Therefore, other BGP neighbors will forward to it packets for that address. This configuration is useful in a non-meshed environment because you know that a path exists from the present router to that address. In a fully meshed environment, this configuration is not useful because it will result in unnecessary extra hops and because there might be a direct access through the fully meshed cloud with fewer hops.

Use the **no** form of this command to enable next hop processing on BGP updates to the specified neighbor.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **next-hop-self**
no neighbor *ip-address* **next-hop-self**

Parameters

ip-address	Specifies IP address of the neighbor BGP component.

Default

Disabled

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

set ip next-hop — Indicates where the output packets that pass a match clause of a route map for policy routing.

Example

This is an example of a successful enabling of next hop processing on BGP updates to the specified neighbor 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# neighbor 192.47.20.34 next-hop-self
CES(config-bgp)#
```

This is an example of a successful disabling of next hop processing on BGP updates to the specified neighbor 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no neighbor 192.47.20.34 next-hop-self
CES(config-bgp)#
```

neighbor loop-detection

To enable loop detection for updates received from a neighbor use the **neighbor loop-detection** router configuration command. To disable loop detaection, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

[no] neighbor *ip-address* **loop-detection**

Parameters

None

Default

Enabled

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

```
CES(config)# router bgp 109
CES(config-bgp)# no neighbor 131.108.1.1 loop-detection
```

neighbor password

To enable Message Digest 5 (MD5) authentication on a TCP connection between two Border Gateway Protocol (BGP) peers, use the **neighbor password** router configuration command. To disable this function, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **password string**
no neighbor *ip-address* **password**

Parameters

ip-address	Specifies IP address of the neighbor BGP component.

Case-sensitive password of up to 80 characters. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces. You cannot specify a password in the format number-space-anything.

Default

Disabled

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

You can invoke authentication between two BGP peers, causing each segment sent on the TCP connection between them to be verified. This feature must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. The authentication feature uses the MD5 algorithm. Specifying this command causes the generation and checking of the MD5 digest on every segment sent on the TCP connection.

Configuring a password for a neighbor will cause an existing session to be torn down and a new one established.

The following example enables the authentication feature between this router and the BGP neighbor at 131.102.1.1. The password that must also be configured for the neighbor is bla4u00=2nkq.

```
CES(config)# router bgp 109
CES(config-bgp)# neighbor 131.108.1.1 password bla4u00=2nkq
```

neighbor remote-as

To add an entry to the Border Gateway Protocol (BGP) use the **neighbor remote-as** router configuration command. To remove an entry from the table, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **remote-as** *autonomous-system-number*
no neighbor *ip-address* **remote-as** *autonomous-system-number*

Parameters

ip-address	Specifies IP address of the neighbor BGP component.
autonomous-system-number	Autonomous System number to which the neighbor belongs. Permitted values are between 1 and 65535.

Default

There are no BGP neighbor peers.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

router bgp — Configures the BGP routing process.

Example

Specifying a neighbor with an AS number that matches the AS number specified in the **router bgp** global configuration command identifies the neighbor as internal to the local AS. Otherwise, the neighbor is considered external.

The following example specifies that a router at the address 131.108.1.2 is a neighbor in AS number 109:

```
CES(config)# router bgp 100
  CES(config-bgp)# neighbor 131.108.1.2 remote-as 109
```

neighbor retry-interval

Use this command to configure the time interval that the BGP speaker should wait before retrying the connection after the connection has failed to the specified neighbor. Use the **no** form of this command to reset the retry interval to its default value. This is Nortel VPN Router specific.

This NNCLI command first appeared in CES Release 5.1.

Syntax

```
neighbor ip-address retry-interval time
no neighbor ip-address retry-interval
```

Parameters

ip-address	Specifies IP address of the neighbor BGP component.
time	Specifies time interval that the BGP speaker should wait before retrying the connection after the connection has failed. Permitted values are between 30 and 600.

Default

30 seconds

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

None

Example

This is an example of a successful configuration of a retry interval of 60 seconds to the specified neighbor 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# neighbor 192.47.20.34 retry-interval 60
CES(config-bgp)#
```

This is an example of a successful reset of a retry interval to the default value from the specified neighbor 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no neighbor 192.47.20.34 retry-interval
CES(config-bgp)#
```

neighbor route-map

Use this command to configure a route map to incoming or outgoing routes. Use the **no** form of this command to delete the route-map. It is possible to attach 1 route-map to an neighbor.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **route-map** *route-map-name* {**in|out**}
no neighbor *ip-address* **route-map** *route-map-name* {**in|out**}

Parameters

ip-address	Specifies IP address of the neighbor BGP component.
route-map-name	Specifies a route-map.
in	Specifies incoming advertisements only
out	Specifies outgoing advertisements only

Default

No route maps are applied to a peer.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

The following router configuration mode example applies a route map named internal-map to a BGP incoming route from 198.92.70.24:

```
CES(config)# router bgp 500
CES(config-bgp)# neighbor 198.92.70.24 route-map
internal-map in

CES(config)# route-map internal-map
CES(config-route-map)#  match as-path 1
CES(config-route-map)#  set local-preference 100
```

neighbor route-reflector-client

Use this command to configure the local router as a BGP route reflector and the specified neighbor as a client.

This NNCLI command first appeared in CES Release CES 5.1.

Syntax

[no] **neighbor ip-address route-reflector-client**

Parameters

ip-address	Specifies IP address of the neighbor BGP component.

Default

None

Command Mode

Router BGP Configuration

Next Command Mode

Router BGP Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

Example

This is an example of a successful configuration of a route reflector client to the specified neighbor 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-router)# neighbor 192.47.20.34
route-reflector-client
CES(config-router)#
```

This is an example of a successful deletion of a route reflector client to the specified neighbor 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-router)# no neighbor 192.47.20.34
route-reflector-client
CES(config-router)#
```

neighbor send-community

Use this command to configure that the communities attribute will be sent to the neighbor at this IP address. Use the **no** form of this command to prevent sending the communities attribute to the neighbor at this IP address.

This NNCLI command first appeared in CES Release 5.1.

Syntax

```
neighbor ip-address send-community
no neighbor ip-address send-community
```

Parameters

ip-address	Specifies IP address of the neighbor BGP component.

Default

No community attribute is sent to any neighbor.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

match community — Matches a BGP community.

set community — Sets the BGP communities attribute.

Example

This is an example of a successful configuration that the communities attribute will be sent to the neighbor at 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# neighbor 192.47.20.34 send-community
CES(config-bgp)#
```

This is an example of a successful prevention of sending the communities attribute to the neighbor at 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no neighbor 192.47.20.34 send-community
CES(config-bgp)#
```

neighbor shutdown

Use this command to disables a BGP neighbor with this IP address. Use the **no** form of this command to enable a BGP neighbor at this IP address.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **shutdown**
no neighbor *ip-address* **shutdown**

Parameters

ip-address	Specifies IP address of the neighbor BGP component.

Default

No change is made to the status of any BGP neighbor or peer group.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

show ip bgp summary — Displays the status of all BGP connections.

Example

This is an example of a successful enabling of a neighbor at 192.47.20.34:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no neighbor 192.47.20.34 shutdown
CES(config-bgp)#
```

neighbor update-source

This command indicates an interface to be used as a source ip address of the BGP session with the neighbors. The **no** form resets the interface to the best local address.

Syntax

[no] neighbor *ip-address* **update-source** *interface-address*

Parameters

ip-address	Specifies IP address of the neighbor BGP component.
interface-address	IP address for TCP connections to the specified neighbor/ peer group

Default

Best local address

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Prerequisites

System Management — Manage

User Management — None

Related commands

Example

This example assigns 11.254.1.10 as the source ip address for TCP connections to the specified neighbor 11.254.1.20.

```
CES(config-bgp)# neighbor 11.254.1.20 update-source
11.254.1.10
```

neighbor timers

Use this command to set Keep-Alive Timer (time interval at which periodic keep alive messages are sent to a specified neighbor after the BGP connection is established) and Hold-Time (time interval in seconds for the hold time configured with all peers) BGP parameters. Use the **no** form of this command to change the value to its global default value.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **timers** *keepalive holdtime*
no neighbor *ip-address* **timers** *keepalive holdtime*

Parameters

ip-address	Specifies IP address of the neighbor BGP component.
keepalive	Specifies the time interval at which periodic keep alive messages sent to the neighbor after the BGP connection is established. Recommended value is 1/3 of holdtime.
holdtime	Specifies the time interval in seconds for the hold time configured with all peers. Permitted values are either 0 or between 3 and 65535 seconds.

Default

keepalive — 60 seconds

holdtime — 90 seconds

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

Example of a successful setting of neighbor *keepalive* and *holdtime* BGP parameters different from the global default value set for other BGP neighbors:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# timers bgp 60 180
CES(config-bgp)# neighbor 47.192.43.20 timers 120 240
CES(config-bgp)#
```

Example of a successful resetting of *keepalive* and *holdtime* BGP parameters for a specified neighbor to the global default value:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no neighbor 47.192.43.20 timers
CES(config-bgp)#
```

neighbor weight

Use this command to specify weight of inbound updates from a neighbor.

A weight is a number that you assign to a path so that you can control the path selection process. The administrative weight is local to the router. A weight can be a number from 0 to 65535. Any path router originates have a default weight of 32768; other paths have weight 0. If you have particular neighbors that you want to prefer for most of your traffic, you assign a higher weight to all routes learned from that neighbor.

Weights can be assigned based on AS path access lists. A given weight becomes the weight of the route if the AS path is accepted by the access list. Any number of weight filters is allowed.

Use the **no** form of this command to delete the value.

This NNCLI command first appeared in CES Release 5.1.

Syntax

neighbor *ip-address* **weight** *weight*
no neighbor *ip-address* **weight**

Parameters

ip-address	Specifies IP address of the neighbor BGP component.
weight	Specifies the weight for the neighbor. Permitted values are either 0 or between 0 and 65535 seconds.

Default

Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

neighbor distribute-list — Distributes BGP neighbor information as specified in an access list

neighbor filter-list — Sets up a BGP filter

Example

All routes learned from this neighbor will have the assigned weight initially. The route with the highest weight will be chosen as the preferred route when multiple routes are available to a particular network.

The weights assigned with the **set weight** route-map command overrides the weights assigned using the **neighbor weight** command.

Example of a successful setting of weight attribute to value = 1000 for a BGP neighbor 47.192.43.20:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# neighbor 47.192.43.20 weight 1000
CES(config-bgp)#
```

Example of a successful deleting of weight attribute for a BGP neighbor 47.192.43.20:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# no neighbor 47.192.43.20 weight
CES(config-bgp)#
```

network

To specify the networks to be advertised by the Border Gateway Protocol (BGP), use the **network** command router configuration mode. To remove an entry, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

network *network-number* [**mask** *network-mask*]
no network *network-number* [**mask** *network-mask*]

Parameters

network-number	Network that BGP will advertise
network-mask	Network mask address

Default

No networks are defined.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

Example of successful setting maximum-paths to 6:

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# network 10.100.0.0 mask 255.255.0.0
```

redistribute

This command redistributes routes from one routing domain into another routing domain. The no form disables redistribution.

Syntax

redistribute { **clip** | **direct** | **hosts** | **mgmt**| **nat** | **ospf**|**rip** | **static** | **utunnel**}
no redistribute { **clip** | **direct** | **hosts** | **mgmt**| **nat** | **ospf**|**rip** | **static** |**utunnel**}

Parameters

clip	CLIP Address
direct	Direct Connected Networks
hosts	Distribute routes from directly connected hosts
mgmt	Distribute management virtual address routes
nat	Distribute NAT routes
ospf	Distribute routes authored byOSPF
rip	Distribute routes authored by RIP
static	Distribute static routes.
utunnel	Distribute routes from non-local clients.

Default

No redistribution is done.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

These examples show that static and direct routes are to be redistributed into BGP domain.

```
CES# configure terminal
CES(config)# router bgp 500
CES(config-bgp)# redistribute static
```

Example of a successful disable redistribution of static routes into BGP:

```
CES# configure terminal
CES(config)# router bgp 500
CES(config-bgp)# no redistribute static
```

route-map

Use this command to create a route-map.

This NNCLI command first appeared in CES Release 5.1.

Syntax

route-map *map-tag* [**permit | deny**] [*sequence-number*]

Parameters

map-tag	Specifies a route-map tag. Maximum length is 64 characters.
permit	Specifies a characteristic of the route map.
deny	Specifies a characteristic of the route map.
sequence-number	Specifies a sequence number in the order in which route map tags will be applied. Permitted values are between 0 and 65535.

Default

Denied

Command mode

Global Configuration

Next command mode

Route Map Configuration mode

Required privileges

System Management — Manage

User Management — None

Related commands

Example

Example of a successful creating a route map tag west, permitting with sequence number 4:

```
CES# configure terminal
CES(config)# route-map west permit 4
CES(config-route-map)#
```

route-reflector enable

Use this command to enable BGP route reflector. Use the no form of this command to disable BGP route reflector.

This NNCLI command first appeared in CES Release 6.0.

Syntax

[no] **route-reflector enable**

Parameters

None

Default

Disabled

Command Mode

Router BGP Configuration

Next Command Mode

Router BGP Configuration

Required Privileges

System Management - Manage

User Management - None

Related Commands

bgp client-to-client reflection
bgp cluster-id *cluster-id*

Example

Example of a successful enabling of BGP route reflector feature:

```
CES# configure terminal
CES(config)# router bgp 563
CES(config-router)# route-reflector enable
CES(config-router)#
```

Example of a successful disabling of BGP route reflector feature:

```
CES# configure terminal
CES(config)# router bgp 563
CES(config-router)# no route-reflector enable
CES(config-router)#
```

router bgp

Use this command to configure a BGP routing component. Use the **no** form of this command to delete the BGP component and its sub-components.

This NNCLI command first appeared in CES Release 5.1.

Syntax

router bgp *as-number*
no router bgp *as-number*

Parameters

as-number	Number of an AS that identifies the router to other BGP routers and tags the routing information passed along.

Default

None

Command mode

Global Configuration

Next command mode

Router BGP Configuration

Global Configuration for no form of the command

Required privileges

System Management — Manage

User Management — None

Related commands

None

Example

Example of a successful configuration of a BGP component for Autonomous System (AS) 563:

```
CES# configure terminal
CES(config)# router bgp 563
CES(config-bgp)#
```

Example of a successful deletion of the BGP component:

```
CES# configure terminal
CES(config)# no router bgp 563
CES(config)#
```

set as-path

To modify an AS path for Border Gateway Protocol (BGP) routes, use the **set as-path** route-map configuration command. To not modify the AS path, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

set as-path prepend *as-path-string*
no set as-path prepend *as-path-string*

Parameters

prepend as-path-string	Appends the string following the keyword prepend to the as-path of the route that is matched by the route map. Applies to inbound and outbound BGP route maps. Maximum 4 AS-PATH can be applied.

Default

Disabled

Command mode

Route Map Configuration

Next command mode

Route Map Configuration.

Required privileges

System Management — Manage

User Management — None

Related commands

match community — Creates a community list for BGP and controls access to it.

route-map — Defines the conditions for redistributing routes from one protocol to another.

set as-path — Modifies an AS path for BGP routes

set community — Sets the BGP communities attribute

set local preference — Specifies a preference value for the AS path

set weight — Specifies the BGP weight for the routing table

Example

The only global BGP metric available to influence the best path selection is the AS-PATH length. By varying the length of the AS-PATH, a BGP speaker can influence the best path selection by a peer further away.

The **set as-path prepend** variation allows you to "prepend" an arbitrary AS path string to BGP routes. Usually the local AS number is prepended multiple times, increasing the AS path length.

The following example prepends 100 100 100 to all the routes advertised to 131.108.1.1:

```
CES(config)#  route-map set-as-path
CES(config-route-map)# match as-path 1
CES(config-route-map)# set as-path prepend 100 100 100

CES(config)# router bgp 100
CES(config-bgp)# neighbor 131.108.1.1 route-map set-as-path
out
```

set community

To set the Border Gateway Protocol (BGP) COMMUNITIES attribute, use the **set community** route-map configuration command. To delete the entry, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

set community *community-number*
no set community *community-number*

Parameters

community-number	Valid values are 1 to 4294967200, no-export, or no-advertise or local-as.

Default

No BGP Communities attributes exist.

Command mode

Router Map Configuration

Next command mode

Router Map Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

ip community-list — Creates a community list for BGP and control access to it.

match community — Matches a BGP community

route-map — Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing

show ip bgp community — Displays routes that belong to specified BGP communities.

Example

You must have a match clause (even if it points to a "permit everything" list) if you want to set tags. Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current route-map command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all of a route map's match criteria are met. When all match criteria are met, all set actions are performed.

In the following example, routes that pass the AS path access list 1 have the community set to 109. Routes that pass the AS path access list 2 have the community set to no-export (these routes will not be advertised to any EBGP peers).

```
CES(config)# route-map set_community 10 permit
CES(config-route-map)# match as-path 1
CES(config-route-map)# set community 109

CES(config)# route-map set_community 20 permit
CES(config-route-map)# match as-path 2
CES(config-route-map)# set community no-export
```

In the following similar example, routes that pass the AS path access list 1 have the community set to 109. Routes that pass the AS path access list 2 have the community set to local-as (the router will not advertise this route to an EBGP peer outside the local AS.

```
CES(config)# route-map set_community 10 permit
CES(config-route-map)# match as-path 1
CES(config-route-map)# set community 109
CES(config)# route-map set_community 20 permit
CES(config-route-map)# match as-path 2
CES(config-route-map)# set community local-as
```

set ip next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set ip next-hop** route-map configuration command. To delete an entry, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

```
set ip next-hop ip-address
no set ip next-hop ip-address
```

Parameters

ip-address	IP address of the next hop to which packets are output. It need not be an adjacent router.

Default

Disabled

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

```
CES(config)#  router bgp 200
CES(config-bgp)# neighbor 1.1.1.3
CES(config-bgp)# neighbor 1.1.1.3 remote-as 100
CES(config-bgp)# neighbor 1.1.1.3 route-map set-peer-address
out

CES(config)# route-map set-peer-address permit 10
CES(config-bgp)# set ip next-hop peer-address
```

set local-preference

This command sets the local preference if the match criteria have met in BGP route map configuration. The *no* form disables the set of local preference.

Syntax

[no] set local-preference *local-preference-number*

Parameters

local-preference -number	0-4294967295

Default

100

Command mode

Route map Configuration

Next command mode

Route map Configuration

Prerequisites

System Management — Manage

User Management — None

Related commands

Example

This example sets the local preference to 5.

```
CES(config-route-map)# set local-preference 5
```

set metric

This command sets the metric if the match criteria have met in BGP route map configuration. The **no** form disables the set of metric.

Syntax

[no] set metric *metric-number*

Parameters

metric-number	0-4294967295

Default

None

Command mode

Route map Configuration

Next command mode

Route map Configuration

Prerequisites

System Management — Manage

User Management — None

Related commands

Example

This example sets the metric to 5.

```
CES(config-route-map)# set metric 5
```

set origin

This command sets the origin if the match criteria have met in BGP route map configuration. The **no** form disables the set of origin.

Syntax

[no] set origin {igp | egp | incomplete}

Parameters

igp	remote IGP
egp	local EGP
incomplete	unknown heritage

Default

None

Command mode

Route map Configuration

Next command mode

Route map Configuration

Prerequisites

System Management — Manage

User Management — None

Related commands

Example

This example sets the origin to egp.

```
CES(config-route-map)# set origin egp
```

set weight

To specify the Border Gateway Protocol (BGP) weight for the routing table, use the **set weight** route-map configuration command. To delete an entry, use the **no** form of this command.

This NNCLI command first appeared in CES Release 5.1.

Syntax

set weight *weight*
no set weight *weight*

Parameters

weight	Weight value can be an integer from 0 to 65535.

Default

The weight is not changed by the specified route map.

Command mode

Route Map Configuration

Next command mode

Route Map Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

The implemented weight is based on the first matched AS path. Weights indicated when an AS path is matched override the weights assigned by global **neighbor** commands. In other words, the weights assigned with the **set weight** route-map configuration command override the weights assigned using the **neighbor weight** command.

The following example sets the BGP weight for the routes matching the AS path access list to 200:

```
CES(config)# route-map set-weight
 CES(config-route-map)# match as-path 10
 CES(config-route-map)# set weight 200
```

show ip as-path access-list

This command displays all as-path access lists configured or only the one specified.

This NNCLI command first appeared in 5.1 CES Release.

Syntax

show ip as-path access-list [*access-list-number*]

Parameters

access-list-number	Specifies the access-list-number.

Default

None

Command mode

Privileged Exec

Next command mode

Privileged Exec

Required privileges

System Management — Manage

User Management — None

Example

Example of a successful display of as-path access-list with number 10:

```
CES# show ip as-path access list 10
AS path access list 10:
permit $100
CES#
```

show ip bgp

This command displays the contents of the BGP routing table (RIB). This NNCLI command first appeared in CES Release 6.0.

Syntax

show ip bgp [address mask {exact|range}**]**

Parameters

address	Network number, entered to display a particular network/mask pair in the BGP routing table.
mask	Network mask, entered to display a particular network/mask in the BGP routing table.

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Related Commands

show ip bgp community community-number
show ip bgp regexp as-regular-expression

Example

Example of a successful display of contents of the BGP routing table:

```
CES# show ip bgp
Local router ID: 10.77.10.220
Status codes: * - valid, > - best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network            Next Hop        Metric LocPrf Weight
Community Path
*> 1.0.0.0/8        10.77.20.100       0   100     0 -
(300) i
CES#
```

Table 13 *show ip bgp* field descriptions

Status code	Stats of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network.
Metric	The value of the inter-autonomous system metric
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.

Table 13 *show ip bgp* field descriptions

Community	Community list to the destination.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp community

This command displays routes that belong to the specified communities. This NNCLI command first appeared in CES Release 6.0

Syntax

show ip bgp community community-number

Parameters

community-number	Valid value is a community number in the range 1 to 4294967200 or AA.NN (autonomous system-community number/2-byte number), internet, no-export, local-as, or no-advertise.

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Related Commands

show ip bgp

Example

Example of a successful display of routes that belong to community 100:

```
CES#show ip bgp community 100
Local router ID: 10.77.10.220
Status codes: * - valid, > - best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network            Next Hop        Metric LocPrf Weight
Community Path
*>1.0.0.0/8       10.77.20.100        0    100     0 100
(300) i
CES#
```

show ip bgp neighbors

This command displays detailed information on the BGP and TCP connections to individual neighbors.

Syntax

show ip bgp neighbors [*address***] [received-routes | routes | advertised-routes]**

Parameters

address	(Optional) Address of the neighbor whose routes you have learned from. If you omit this argument, all neighbors are displayed.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. This is a subset of the output from the **received-routes** keyword
advertised-routes	(Optional) Displays all the routes advertised to the neighbor.

Default

None

Command mode

Privileged Exec

Next command mode

Privileged Exec

Required privileges

System Management — Manage

User Management — None

Example

Example of a successful display of detailed information on the BGP and TCP connections to neighbor 47.100.0.0:

```
CES# show ip bgp neighbors 47.100.0.0
BGP neighbor 10.77.10.181
Remote AS: 100, external link
Remote router ID: 10.77.10.181
BGP status: Established, up for 14:28:58
Hold time: 90, keepalive interval: 30 seconds
Advertisement interval: 5 retry interval: 30 seconds
Connection: 43 established 0 dropped
              1341 starts    0 stops
              43 opens       0 closes
              1 failures     0 fatals
              1302 expires   3 hold expires
              3474 keepalive expires
  Sent:       6952 messages
              1 opens        3475 keepalives
              0 updates      0 notifies
  Received:   3477 messages:
              1 opens        3475 keepalives
              1 updates      0 notifies
  Local host: 10.77.30.191
  Foreign host: 10.77.10.181
  Number of routes: 1, sent: 0
```

Table 14 *show ip bgp neighbors* field descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its AS number. If the neighbor is in the same AS as the router, then the link between them is internal; otherwise, it is considered external.
Remote AS	Autonomous system of the neighbor.
External link	Indicates that this peer is an Exterior Border Gateway Protocol (EBGP) peer.
Remote router ID	IP address of the neighbor
BGP state	Internal state of this BGP connection

Table 14 *show ip bgp neighbors* field descriptions

Field	Description
Up for	Amount of time that the underlying TCP connection has been in existence
Hold time	Maximum amount of time that can elapse between messages from the peer
Keepalive interval	Time period between sending keepalive packets, which help ensure that the TCP connection is up
Received	Number of total BGP messages received from this peer, including keepalives
Notifications	Number of error messages received from the peer
Sent	Total number of BGP messages that have been sent to this peer, including keepalives
Notifications	Number of error messages the router has sent to this peer
Advertisement interval	Value of minimum advertisement interval
Local host	Peering address of local router
Foreign host	Neighbor's peering address

The following is sample output from the **show ip bgp neighbors** command with the **advertised-routes** keyword in privileged EXEC mode:

```
CES# show ip bgp neighbors 172.16.232.178 advertised-routes
Local router ID is 172.16.232.181
Status codes: * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*>i 110.0.0.0        172.16.232.179         0    100      0 ?
*>  200.2.2.0        0.0.0.0                0         32768 i
```

The following is sample output from the **show ip bgp neighbors** command with the **routes** keyword in privileged EXEC mode:

```
CES# show ip bgp neighbors 172.16.232.178 routes
Local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*> 10.0.0.0        172.16.232.178       40             0 10 ?
*> 20.0.0.0        172.16.232.178       40             0 10 ?
```

Table 15 show **ip bgp neighbors** advertised-routes and routes field descriptions

Field	Description
Local Router ID	IP address of the router
Status codes	s — The table entry is suppressed * — The table entry is valid > —The table entry is the best entry to use for that network i–The table entry was learned via an internal BGP session
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i–Entry originated from Interior Gateway Protocol (IGP) and was advertised with a network router configuration command e–Entry originated from Exterior Gateway Protocol (EGP) ?–Origin of the path is not clear Usually, this is a router that is redistributed into BGP from an IGP
Network	IP address of a network entity
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network
Metric	If shown, this is the value of the inter-AS metric. This field is frequently not used

Table 15 show **ip bgp neighbors** advertised-routes and routes field descriptions

Field	Description
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100
Weight	Weight of the route as set via AS filters
Path	Autonomous system paths to the destination network. There can be one entry in this field for each AS in the path

show ip bgp networks

This command displays all the routes advertised using network command. This NNCLI command first appeared in CES Release 6.0

Syntax

```
show ip bgp networks
```

Parameters

None

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Related Commands

`bgp network`

Example

show ip bgp redistribution

This command displays the route policies for redistribution tables in BGP. This NNCLI command first appeared in CES Release 6.0.

Syntax

`show ip bgp redistribution`

Parameters

None

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Example

Example of displaying redistribution table in BGP:

```
CES#show ip bgp redistribution
Redistribution table for
  Static:       Disabled
  Direct Nets:  Disabled
  Direct Hosts: Disabled
  OSPF:         Disabled
  RIP:          Disabled
  UTunnel:      Disabled
  CLIP:         Disabled
  MGMT:         Disabled
  NAT:          Disabled
```

show ip bgp redistribute-routes

This command displays the routes redistributed from other protocols in BGP. This NNCLI command first appeared in CES Release 6.0.

Syntax

show ip bgp redistributed-routes

Parameters

None

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Example

Example of routes redistributed from other protocols in BGP:

```
CES#show ip bgp redistributed-routes
Local router ID: 10.77.20.150
Status codes: * - valid, > - best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network           Next Hop Metric LocPrf Weight Community Path
9.9.9.0/24          0.0.0.0               0      0       0
10.77.20.0/24       0.0.0.0               0      0       0
```

show ip bgp regexp

This command displays the routes that have an autonomous system path that matches the specified regular expression entered on the command line.

This NNCLI command first appeared in CES Release 6.0.

Syntax

show ip bgp regexp as-regular-expression

Parameters

as-regular-expression	Specifies the regular expression.

Default

None

Command Mode

Privileged Exec

Next Command Mode

Privileged Exec

Required Privileges

System Management - Manage

User Management - None

Related Commands

show ip bgp

Example

Example of a successful display of status of all BGP connections:

```
CES#show ip bgp regexp 300
Local router ID: 10.77.10.220
Status codes: * - valid, > - best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network            Next Hop        Metric LocPrf Weight
Community Path
*>1.0.0.0/8       10.77.20.100        0    100     0 -
(300) i
CES#
```

show ip bgp summary

This command displays the status of all BGP connections.

This NNCLI command first appeared in CES Release 5.1.

Syntax

show ip bgp summary

Parameters

None

Default

None

Command mode

Privileged Exec

Next command mode

Privileged Exec

Required privileges

System Management — Manage

User Management — None

Example

Example of a successful display of status of all BGP connections:

```
CES# show ip bgp summary
Router ID: 151.100.1.1
Local AS: 100
Hold interval: 90
Keep alive interval: 30
Synchronization: DISABLED
Local preference: 100
Default metric: 200
Always compare med: DISABLED
Maximum paths: 1
Admin state: ENABLED
Number of peers: 1
Neighbor     V  AS  NumRt  MsgRcvd  MsgSent  UpTime     State
10.55.1.11   4  200   4       26       22     00:14:23
Connected
```

Table 16 *show ip bgp summary* field descriptions

Field	Description
BGP router identifier	In order of precedence and availability, router identifier specified by the bgp router-id command, loopback address, or lowest IP address
Neighbor	IP address of a neighbor
V	BGP version number spoken to that neighbor
AS	Autonomous system
NumRt	Number of routes received from that neighbor
MsgRcvd	BGP messages received from that neighbor
MsgSent	BGP messages sent to that neighbor
UpTime	The length of time that the BGP session has been in state Established, or the current state if it is not Established
State	Current state of the BGP session. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command

show ip community-list

This command displays all community-lists configured or only the one specified.

This NNCLI command first appeared in 5.1 CES Release.

Syntax

show ip community-list [*community-list-number*]

Parameters

community-list-number	Specifies the community-list-number

Default

None

Command mode

Privileged Exec

Next command mode

Privileged Exec

Required privileges

System Management — Manage

User Management — None

Example

Example of a successful display of community list with number 10:

```
CES# show ip community-list 10
Community list 10
permit internet local-as
CES#
```

show ip route-map

This command displays all route maps configured or only the one specified.

This NNCLI command first appeared in 5.1 CES Release.

Syntax

show route-map [*map-name*]

Parameters

map-name	Specifies the route-map name.

Default

None

Command mode

Privileged Exec

Next command mode

Privileged Exec

Required privileges

System Management — Manage

User Management — None

Example

Example of a successful display of route-maps with name east:

```
CES# show route-map test
Route-map test, permit, sequence 10
Match clauses:
    as-path (access list number) 10
    community-list 10
Set clauses:
    ip next-hop 10.88.10.1
CES#
```

synchronization

To enable the synchronization between Border Gateway Protocol (BGP) and your Interior Gateway Protocol (IGP) system, use the **synchronization** command in BGP router configuration mode. To enable the advertisement of network routes without waiting for the IGP, use the *no* form of this command.

Use the **synchronization** command if there are routers in the AS that do not speak BGP.

This NNCLI command first appeared in CES Release 5.1.

Syntax

[no] synchronization

Parameters

None

Default

Synchronization is disabled.

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

Example

Example of successful setting maximum-paths to 6

```
CES# configure terminal
CES(config)# router bgp 100
CES(config-bgp)# synchronization
```

timers bgp

Use this command to set Keep-Alive Timer (time interval at which periodic keep alive messages are sent to neighbors after the BGP connection is established) and Hold-Time (time interval in seconds for the hold time configured with all peers) BGP parameters. This is a default value for all BGP neighbors.

Use the **no** form of this command to change the value to its default value.

This NNCLI command first appeared in CES Release 5.1.

Syntax

timers bgp *keepalive holdtime*
no timers bgp

Parameters

keepalive	Specifies the time interval at which periodic keep alive messages sent to the neighbor after the BGP connection is established. Recommended value is 1/3 of holdtime.
holdtime	Interval, in seconds, after not receiving a keepalive message that the software declares a peer dead.

Default

keepalive — 30 seconds

holdtime — 90 seconds

Command mode

Router BGP Configuration

Next command mode

Router BGP Configuration

Required privileges

System Management — Manage

User Management — None

Related commands

router bgp
show ip bgp

Example

Example of a successful setting of keepalive and holdtime BGP parameters:

```
CES# configure terminal
CES(config)# router bgp 500
CES(config-bgp)# timers bgp 60 180
```

Example of a successful deleting of keepalive and holdtime BGP parameters:

```
CES# configure terminal
CES(config)# router bgp 563
CES(config-bgp)# no timers bgp
```

Appendix A
Sample scripts and output files generated by the show running-config command

You can use the **show running-config** command to capture information about the current running configuration and output it to a **.cli** script file. The **.cli** script files are written to the directory **system/runconf**. You can use files generated with the **show running-config** command as the basis for new scripts or to add to existing scripts.

You can provision single or multiple Nortel VPN Routers using these scripts. Scripts must use the CLI commands, must be in ASCII text format, and must have a file extension of **.cli** . You use FTP to copy a script file to the **system/prov** directory on the gateway. The script executes automatically after it is copied to the directory.

This appendix provides examples of **.cli** script files and the resulting **.out** files.

Topic	Page
Example 1: Add networks, domains, access hours, and groups	2110
Example 2: Add users to a group	2112
Example 3: Add branch office connections	2115
Example 4: Configure group properties	2117

Example 1: Add networks, domains, access hours, and groups

```
!
! ----------------------------
!  Test1
! ----------------------------
!

enable
setup
configure terminal

! Add networks
network add "testNetwork" ip 1.1.1.1 mask 255.255.255.255
show networks

! Add domain
domain add TestDomain domain-name test
show domains
show domains TestDomain

! Add access hours
access-hours add "TestHours"
show access-hours

show group

! Add group test
group add /Base/grouptest

! Show groups
show group
exit
exit
exit
```

Resulting output script: test1.out

```
CES>
CES>!
CES>! ----------------------------
CES>!  Test1
CES>! ----------------------------
CES>!
CES>enable
Password:
CES#configure terminal
Enter configuration commands, one per line.  End with Ctrl/z.
CES(config)#! Add networks
CES(config)#network add "testNetwork" ip 1.1.1.1 mask 255.255.255.255
CES(config)#show networks
Networks:
   testNetwork
CES(config)#
CES(config)#! Add domain
CES(config)#domain add TestDomain domain-name "test"
CES(config)#show domains
Domain sets:
   TestDomain
CES(config)#show domains TestDomain
Domains for  TestDomain :
   test
CES(config)#
CES(config)#! Add Access hours
CES(config)#access-hours add "TestHours"
CES(config)#show access-hours
Anytime
TestHours
Weekdays
Weekends
CES(config)#
CES(config)#show group
  /Base
CES(config)#! Add group test
CES(config)#group add /Base/grouptest
CES(config)#! Show groups
CES(config)#show group
  /Base
  /Base/grouptest
CES(config)#exit
```

```
CES#exit
CES>exit
```

Example 2: Add users to a group

```
!
! ----------------------------
!  Test2
! ----------------------------
!
enable
setup
configure terminal
show groups
group add "/Base/grouptest"
show users group "/Base/grouptest"
user add "User One" "/Base/grouptest"
user add "User Two" "/Base/grouptest"
user add "User Three" "/Base/grouptest"
user add "User Four" "/Base/grouptest"
user add "User Five" "/Base/grouptest"
!
! Configure User
!
user "User One" "/Base/grouptest"
ipsec uid GPipsec password blah
l2f uid GPl2f password blah
l2tp uid GPl2tp password blah
pptp uid GPpptp password blah
admin uid GPadmin password blah
administration group-manage "/Base/grouptest"
administration switch-manage manage
administration users-manage manage
static-ipaddress 1.1.1.1
static-subnet-mask 255.255.255.255
exit
show users group "/Base/grouptest"
show users "User One" "/Base/grouptest"
exit
! Show running config for users
show running config profile users
config terminal
```

```
! Delete Group with users
no group "/Base/grouptest"
no group "/Base/grouptest" rec delete
show groups
exit
exit
exit
```

Resulting output script: test2.out

```
CES>
CES>!
CES>! ----------------------------
CES>!  Test2
CES>! ----------------------------
CES>!
CES>enable
Password:
CES#configure terminal
Enter configuration commands, one per line.  End with Ctrl/z.
CES(config)#show groups
  /Base
CES(config)#group add "/Base/grouptest"
CES(config)#show users group "/Base/grouptest"
Users for Group /Base/grouptest:
CES(config)#user add "User One" "/Base/grouptest"
CES(config)#user add "User Two" "/Base/grouptest"
CES(config)#user add "User Three" "/Base/grouptest"
CES(config)#user add "User Four" "/Base/grouptest"
CES(config)#user add "User Five" "/Base/grouptest"
CES(config)#!
CES(config)#! Configure User
CES(config)#!
CES(config)#user "User One" "/Base/grouptest"
CES(config-user)#ipsec uid GPipsec password blah
CES(config-user)#l2f uid GPl2f password blah
CES(config-user)#l2tp uid GPl2tp password blah
CES(config-user)#pptp uid GPpptp password blah
CES(config-user)#admin uid GPadmin password blah
CES(config-user)#administration group-manage "/Base/grouptest"
CES(config-user)#administration switch-manage manage
CES(config-user)#administration users-manage manage
CES(config-user)#static-ipaddress 1.1.1.1
```

```
CES(config-user)#static-subnet-mask 255.255.255.255
CES(config-user)#exit
CES(config)#show users group "/Base/grouptest"
Users for Group /Base/grouptest:
   User Five
   User Four
   User One
   User Three
   User Two
CES(config)#show users "User One" "/Base/grouptest"
  Static IP Address                                    : 1.1.1.1
  Static Subnet Mask                                 : 255.255.255.255
L2TP User Accounts
  User ID                                              : gpl2tp
  Password                                             : ********
  IPsec Credentials                                    : Disabled
  UID Lockout                                        : Not Configured
Administration Properties:
  User ID                                              : gpadmin
  Password                                             : ********
  Manage Switch                                        : MANAGE
  Manage Users                                         : MANAGE
  Manage Group                                       : /Base/grouptest
IPsec User Accounts
  Subject Alternative Name                           : Not Configured
  Subject Alternative Name Type                        : email
  Subject Distinguished Name                         : Not Configured
  User ID                                              : gpipsec
  Password                                             : ********
  UID Lockout                                        : Not Configured
  Issuer Certificate Authority                       : Not Configured
  Server Certificate                                 : Not Configured
L2F User Accounts
  User ID                                              : gpl2f
  Password                                             : ********
  UID Lockout                                        : Not Configured
PPTP User Accounts
  User ID                                              : gppptp
  Password                                             : ********
  UID Lockout                                        : Not Configured
CES(config)#exit
CES#! Show running config for users
CES#show running-config profile users
CES#config terminal
```

```
Enter configuration commands, one per line.  End with Ctrl/z.
CES(config)#! Delete Group with users
CES(config)#no group "/Base/grouptest"
% Group "/Base/grouptest" contains users
CES(config)#no group "/Base/grouptest" rec delete
CES(config)#show groups
  /Base
CES(config)#exit
CES#exit
CES>exit
```

Example 3: Add branch office connections

```
!
!  Test 3
!  This script will add a Branch Office connection
!
enable
setup
configure terminal

! Add networks
network add 10.x.x.x ip 10.0.0.0 mask 255.255.0.0
show bo-group
! Add BO group
bo-g add "/Base/cli_branch_test"
! Add Interface
interface fastEthernet 1/1
ip address 12.12.1.1 255.255.255.0
exit

! Add BO connection
bo-conn add branch "/Base/cli_branch_test"
bo-conn branch "/Base/cli_branch_test"
state disable
filter "permit all"
local-endpoint 12.12.1.1
remote-endpoint 13.13.13.2
routing type static
routing static
local-network 10.x.x.x
remote-network 1.0.0.0 mask 255.255.0.0 state enable cost 10
```

```
exit
tunnel-type ipsec
ipsec authentication hex-pre-shared-key AAAA
exit
!
show bo-conn
no bo-conn branch "/Base/cli_branch_test"
no bo-g "/Base/cli_branch_test" rec purge
no network 10.x.x.x
exit
exit
exit
```

Resulting output script: test3.out

```
CES>!
CES>!  Test 3
CES>!  This script will add a Branch Office connection
CES>!
CES>enable
Password:
CES#configure terminal
Enter configuration commands, one per line.  End with Ctrl/z.
CES(config)#! Add networks
CES(config)#network add 10.x.x.x ip 10.0.0.0 mask 255.255.0.0
CES(config)#show bo-group
  /Base
CES(config)#! Add BO group
CES(config)#bo-g add "/Base/cli_branch_test"
CES(config)#! Add Interface
CES(config)#interface fastEthernet 1/1
CES(config-if)#ip address 12.12.1.1 255.255.255.0
CES(config-if)#exit
CES(config)#! Add BO connection
CES(config)#bo-conn add branch "/Base/cli_branch_test"
CES(config)#bo-conn branch "/Base/cli_branch_test"
CES(config/bo_conn)#state disable
CES(config/bo_conn)#filter "permit all"
CES(config/bo_conn)#local-endpoint 12.12.1.1
CES(config/bo_conn)#remote-endpoint 13.13.13.2
CES(config/bo_conn)#routing type static
CES(config/bo_conn)#routing static
CES(config/bo_conn/routing_static)#local-network 10.x.x.x
```

```
CES(config/bo_conn/routing_static)#remote-network 1.0.0.0 mask
255.255.0.0 state enable cost 10
CES(config/bo_conn/routing_static)#exit
CES(config/bo_conn)#tunnel-type ipsec
CES(config/bo_conn)#ipsec authentication hex-pre-shared-key AAAA
CES(config/bo_conn)#exit
CES(config)#!
CES(config)#show bo-conn
Group                    Connection
-------------------------------------
/Base
/Base/cli_branch_test
                         branch
CES(config)#no bo-conn branch "/Base/cli_branch_test"
CES(config)#no bo-g "/Base/cli_branch_test" rec purge
CES(config)#no network 10.x.x.x
CES(config)#exit
CES#exit
CES>exit
```

Example 4: Configure group properties

```
!
! Group Configuration Script
! test4.cli
!
enable
setup
con ter
!#####################################
! Set ROOT properties
!#####################################
! Set IPSEC Tunnel
ipsec authentication local username-password
ipsec authentication local rsa-sig
ipsec authentication radius passgo-defender
ipsec authentication radius dynamic-securid
ipsec authentication radius username-password
ipsec encryption des56-md5
ipsec encryption hmac-md5
ipsec encryption md5
ipsec encryption sha1
```

```
ipsec encryption hmac-sha1
ipsec encryption des40-md5
ipsec encryption 3des-sha1
ipsec encryption des56-sha1
ipsec encryption 3des-md5
ipsec encryption des40-sha1
ipsec encryption ike des56-group1
ipsec encryption ike 3des-group2
ipsec encryption ike 3des-group7
ipsec nat-traversal port 12345
ipsec nat-traversal

! Set PPTP Tunnel
pptp authentication pap
pptp authentication chap
pptp authentication ms-chap version 1
pptp authentication ms-chap version 2
pptp authentication ms-chap encryption rc4-128
pptp authentication ms-chap encryption rc4-40

! Set L2TP Tunnel
l2tp authentication pap
l2tp authentication chap
l2tp authentication ms-chap version 1
l2tp authentication ms-chap version 2
l2tp authentication ms-chap encryption rc4-128
l2tp authentication ms-chap encryption rc4-40
! Set L2F Tunnel
l2f authentication pap
l2f authentication chap

! Add networks
network add "testNetwork" ip 1.1.1.1 mask 255.255.255.255
show networks

! Add domain
domain add TestDomain domain-name test
sh domains TestDomain

! Add Access hours
access-hours add "TestHours"
show access-hours

show group
```

```
! Add group test
group add /Base/grouptest

! Show groups
show group
!
! ########################################
! Test Properties of the group
! ########################################
!
! Show General Properties
show group con /Base/grouptest
group con /Base/grouptest
access-hours "TestHours"
ip address-pool "blah"
priority call-admission highest
contact "You are the contact person"
priority forwarding high
idle-timeout 15:15:00
ipx
filters "deny all"
rsvp
rsvp token-bucket depth 3000
rsvp token-bucket rate 28
no password alphabetic
no password management
password max-age 30
password min-length 8
ppp-links max-number "2"
login max-attempts 5
logins 3
static-ipaddress
committed rate 56000
excess rate 128000
excess action drop
exit

! Default all
group con /Base/grouptest
default all
exit

! Show the parent properties
show group con /Base
```

```
! Show the group properties
show group con /Base/grouptest
!
! ####################################
!  Test IPSEC Properties of the Group
! ####################################
!
! Enter ipsec mode for group "/Base/grouptest"
group ipsec "/Base/grouptest"
exit
! Show ipsec Properties
show group l2f /Base
! Set all the values to default
group ipsec "/Base/grouptest"
banner "Hello World"
display-banner
rekey timeout 00:00:01
rekey data-count 123
password-storage
pfs
compress
encryption des56-md5
encryption hmac-md5
encryption md5
no encryption sha1
encryption hmac-sha1
encryption des40-md5
encryption 3des-sha1
no encryption des56-sha1
encryption 3des-md5
encryption des40-sha1
encryption ike 3des-group7
nortel-client action none
nortel-client version none
no nortel-client message
nortel-client filter "deny all"
client allowed ALL
no client policy
no client screen-saver password
client screen-saver activation-time 5
client undefined-networks
client failover-tuning
client failover-tuning interval 00:01:00
client failover-tuning retransmissions 3
```

```
client nat interval 00:00:18
nat-traversal nat-detect
no client auto-connect
no client auto-connect networks
no client auto-connect domains
ip domain-name "test"
ip address 0.0.0.0
ip address 0.0.0.0 secondary
wins address 0.0.0.0
wins address 0.0.0.0 secondary
no authentication local rsa-sig
authentication local username-password
authentication local rsa-sig server-ca "CN=CLI1 interop, O=contivity,
C=US, OU=interop-lab"
authentication external passgo-defender
authentication external username-password
no authentication external dynamic-securid
authentication external groupid "hello" password "asdf"
forced-logoff 00:00:00
no split tunneling
split tunnel-network "testNetwork"
exit

! Default All
group ipsec "/Base/grouptest"
def all
exit

! Show IPSEC Properties
show group ipsec /Base
! Show IPSEC Properties
show group ipsec /Base/grouptest

! Show L2TP Properties
show group l2tp /Base/grouptest

! Change L2TP Properties
group l2tp /Base/grouptest
client-address
default ipsec-data-protection
default ipsec-credentials
no compress
ip address 12.23.23.3
ip address 12.23.0.45 secondary
```

```
wins address 123.23.23.3
wins address 123.2.12.33 secondary
no authentication pap
no authentication chap
no authentication ms-chap version 1
no authentication ms-chap version 2
no authentication ms-chap encryption none
no authentication ms-chap encryption rc4-40
no authentication ms-chap encryption rc4-128
exit

! Show L2TP Properties
show group l2tp /Base/grouptest


! Set the L2TP Properties to default value
group l2tp /Base/grouptest
default authentication
exit
group l2tp /Base/grouptest
default all
exit

! Show the parent properties
show group l2tp /Base

! Show the group properties
show group l2tp /Base/grouptest
!
! Show PPTP Properties
show group pptp /Base/grouptest

! Change PPTP Properties
group pptp /Base/grouptest
no authentication pap
no authentication chap
no authentication ms-chap version 1
no authentication ms-chap version 2
no authentication ms-chap encryption none
no authentication ms-chap encryption rc4-40
no authentication ms-chap encryption rc4-128
exit

! Show PPTP Properties
```

```
show group pptp /Base/grouptest
! Set the PPTP Properties to default value
group pptp /Base/grouptest
default authentication
exit

! Show the parent properties
show group pptp /Base
! Show the group properties
show group pptp /Base/grouptest

! Show L2F Properties
show group l2f /Base/grouptest

! Change L2f Properties
group l2f /Base/grouptest
no authentication pap
no authentication chap
exit

! Show L2F Properties
show group l2f /Base/grouptest
group l2f /Base/grouptest
default authentication
exit
! Show L2F Properties
show group l2f /Base
! Show L2F Properties
show group l2f /Base/grouptest
exit
!
! End of the Group Configuration  Script
exit
exit
exit
```

Resulting output script: test4.out

```
!
Output file
test4.out
CES>!
CES>! Smoketest Script
CES>!
CES>enable
Password:
CES#con ter
Enter configuration commands, one per line.  End with Ctrl/z.
CES(config)#!#####################################
CES(config)#! Set ROOT properties
CES(config)#!#####################################
CES(config)#! Set IPSEC Tunnel
CES(config)#ipsec authentication local usernam
CES(config)#ipsec authentication radius passgo-defender
CES(config)#ipsec authentication local rsa-sig
CES(config)#ipsec authentication radius dynamic-securid
CES(config)#ipsec authentication radius username-password
CES(config)#ipsec encryption des56-md5
CES(config)#ipsec encryption hmac-md5
CES(config)#ipsec encryption md5
CES(config)#ipsec encryption sha1
CES(config)#ipsec encryption hmac-sha1
CES(config)#ipsec encryption des40-md5
CES(config)#ipsec encryption 3des-sha1
CES(config)#ipsec encryption des56-sha1
CES(config)#ipsec encryption 3des-md5
CES(config)#ipsec encryption des40-sha1
CES(config)#ipsec encryption ike des56-group1
CES(config)#ipsec encryption ike 3des-group2
CES(config)#ipsec encryption ike 3des-group7
CES(config)#ipsec nat-traversal port 12345
CES(config)#ipsec nat-traversal
CES(config)#
CES(config)#! Set PPTP Tunnel
CES(config)#pptp authentication pap
CES(config)#pptp authentication chap
CES(config)#pptp authentication ms-chap version 1
CES(config)#pptp authentication ms-chap version 2
CES(config)#pptp authentication ms-chap encryption rc4-128
CES(config)#pptp authentication ms-chap encryption rc4-40
```

```
CES(config)#! Set PPTP Tunnel
CES(config)#l2tp authentication pap
CES(config)#l2tp authentication chap
CES(config)#l2tp authentication ms-chap version 1
CES(config)#l2tp authentication ms-chap version 2
CES(config)#l2tp authentication ms-chap encryption rc4-128
CES(config)#l2tp authentication ms-chap encryption rc4-40

CES(config)#! Set L2F Tunnel
CES(config)#l2f authentication pap
CES(config)#l2f authentication chap

CES(config)#! Add networks
CES(config)#network add "testNetwork" ip 1.1.1.1 mask 255.255.255.255
CES(config)#show networks
Networks:
   testNetwork
CES(config)#

CES(config)#! Add domain
CES(config)#domain add TestDomain domain-name test
CES(config)#sh domains TestDomain
Domains for  TestDomain :
   test
CES(config)#
CES(config)#! Add Access hours
CES(config)#access-hours add "TestHours"
CES(config)#show access-hours
Anytime
TestHours
Weekdays
Weekends

CES(config)#
CES(config)#show group
  /Base
  /Base/clitest

CES(config)#! Add group test
CES(config)#group add /Base/grouptest
CES(config)#

CES(config)#! Show groups
CES(config)#show group
```

```
  /Base
  /Base/clitest
  /Base/grouptest
CES(config)#!
CES(config)#! ########################################
CES(config)#! Test Properties of the group
CES(config)#! ########################################
CES(config)#!
CES(config)#! Show General Properties
CES(config)#show group con /Base/grouptest
CONNECTIVITY Settings:
  Access Hours                                          : Anytime
  Address Pool Name                                     : Not Configured
  Call Admission Priority                               : highest
  Contact Information                                   : Not Configured
  Filters                                               : permit all
  Forwarding Priority                                   : low
  Idle Timeout                                          : 00:15:00
  Ipx                                                   : Disabled
  Maximum Number of Login Attempts                      : 0
  Number Logins                                         : 1
  Password Management                                   : Disabled
  Password Maximum Age                                  : 30
  Password Manimum Length                               : 16
  Password Alphabetic                                   : Disabled
  PPP Links Maximum Number                              : 2
  RSVP                                                  : Disabled
  RSVP: Token Bucket Depth                              : 3000
  RSVP: Token Bucket Rate                               : 28
  Static Addresses                                      : Enabled
  User Bandwidth Policy: Committed Rate                 : 56000
  User Bandwidth Policy: Excess Rate                    : 128000
  User Bandwidth Policy: Excess Action                  : MARK
CES(config)#group con /Base/grouptest
CES(config-group/con)#access-hours "TestHours"
CES(config-group/con)#ip address-pool "blah"
% IP Address Pool does not exist
CES(config-group/con)#priority call-admission highest
CES(config-group/con)#contact "You are the contact person"
CES(config-group/con)#priority forwarding high
CES(config-group/con)#idle-timeout 15:15:00
CES(config-group/con)#ipx
CES(config-group/con)#filters "deny all"
CES(config-group/con)#rsvp
```

```
CES(config-group/con)#rsvp token-bucket depth 3000
CES(config-group/con)#rsvp token-bucket rate 28
CES(config-group/con)#no password alphabetic
CES(config-group/con)#no password management
CES(config-group/con)#password max-age 30
CES(config-group/con)#password min-length 8
CES(config-group/con)#ppp-links max-number "2"
CES(config-group/con)#login max-attempts 5
CES(config-group/con)#logins 3
CES(config-group/con)#static-ipaddress
CES(config-group/con)#committed rate 56000
CES(config-group/con)#excess rate 128000
CES(config-group/con)#excess action drop
CES(config-group/con)#exit
% LDAP: Object class violation
CES(config)#
CES(config)#! Default all
CES(config)#group con /Base/grouptest
CES(config-group/con)#default all
CES(config-group/con)#exit
CES(config)#

CES(config)#! Show the parent properties
CES(config)#show group con /Base
CONNECTIVITY Settings:
  Access Hours                                          : Anytime
  Address Pool Name                                   : Not Configured
  Call Admission Priority                               : highest
  Contact Information                                 : Not Configured
  Filters                                               : permit all
  Forwarding Priority                                   : low
  Idle Timeout                                          : 00:15:00
  Ipx                                                   : Disabled
  Maximum Number of Login Attempts                      : 0
  Number Logins                                         : 1
  Password Management                                   : Disabled
  Password Maximum Age                                  : 30
  Password Manimum Length                               : 16
  Password Alphabetic                                   : Disabled
  PPP Links Maximum Number                              : 2
  RSVP                                                  : Disabled
  RSVP: Token Bucket Depth                              : 3000
  RSVP: Token Bucket Rate                               : 28
  Static Addresses                                      : Enabled
```

```
  User Bandwidth Policy: Committed Rate                    : 56000
  User Bandwidth Policy: Excess Rate                       : 128000
  User Bandwidth Policy: Excess Action                     : MARK

CES(config)#! Show the group properties
CES(config)#show group con /Base/grouptest
CONNECTIVITY Settings:
  Access Hours                                             : Anytime
  Address Pool Name                                       : Not Configured
  Call Admission Priority                                  : highest
  Contact Information                                     : Not Configured
  Filters                                                  : permit all
  Forwarding Priority                                      : low
  Idle Timeout                                             : 00:15:00
  Ipx                                                      : Disabled
  Maximum Number of Login Attempts                         : 0
  Number Logins                                            : 1
  Password Management                                      : Disabled
  Password Maximum Age                                     : 30
  Password Manimum Length                                  : 16
  Password Alphabetic                                      : Disabled
  PPP Links Maximum Number                                 : 2
  RSVP                                                     : Disabled
  RSVP: Token Bucket Depth                                 : 3000
  RSVP: Token Bucket Rate                                  : 28
  Static Addresses                                         : Enabled
  User Bandwidth Policy: Committed Rate                    : 56000
  User Bandwidth Policy: Excess Rate                       : 128000
  User Bandwidth Policy: Excess Action                     : MARK
CES(config)#
CES(config)#!
CES(config)#! ####################################
CES(config)#!  Test IPSEC Properties of the Group
CES(config)#! ####################################
CES(config)#!
CES(config)#! Enter ipsec mode for group "/Base/grouptest"
CES(config)#group ipsec "/Base/grouptest"
CES(config-group/ipsec)#exit

CES(config)#! Show ipsec Properties
CES(config)#show group l2f /Base
L2F Settings:
  Authentication PAP                                       : Disabled
  Authentication CHAP                                      : Enabled
```

```
  Client Address                                          : Disabled
  Compression                                             : Enabled
  Primary DNS Address                                     : 0.0.0.0
  Primary WINS Address                                    : 0.0.0.0
  Secondary DNS Address                                   : 0.0.0.0
  Secondary WINS Address                                  : 0.0.0.0

CES(config)#! Set all the values to default
CES(config)#group ipsec "/Base/grouptest"
CES(config-group/ipsec)#banner "Hello World"
CES(config-group/ipsec)#display-banner
CES(config-group/ipsec)#rekey timeout 00:00:01
CES(config-group/ipsec)#rekey data-count 123
CES(config-group/ipsec)#password-storage
CES(config-group/ipsec)#pfs
CES(config-group/ipsec)#compress
CES(config-group/ipsec)#encryption des56-md5
CES(config-group/ipsec)#encryption hmac-md5
CES(config-group/ipsec)#encryption md5
CES(config-group/ipsec)#no encryption sha1
CES(config-group/ipsec)#encryption hmac-sha1
CES(config-group/ipsec)#encryption des40-md5
CES(config-group/ipsec)#encryption 3des-sha1
CES(config-group/ipsec)#no encryption des56-sha1
CES(config-group/ipsec)#encryption 3des-md5
CES(config-group/ipsec)#encryption des40-sha1
CES(config-group/ipsec)#encryption ike 3des-group7
CES(config-group/ipsec)#nortel-client action none
CES(config-group/ipsec)#nortel-client version none
CES(config-group/ipsec)#no nortel-client message
CES(config-group/ipsec)#nortel-client filter "deny all"
CES(config-group/ipsec)#client allowed ALL
CES(config-group/ipsec)#no client policy
CES(config-group/ipsec)#no client screen-saver password
CES(config-group/ipsec)#client screen-saver activation-time 5
CES(config-group/ipsec)#client undefined-networks
CES(config-group/ipsec)#client failover-tuning
CES(config-group/ipsec)#client failover-tuning interval 00:01:00
CES(config-group/ipsec)#client failover-tuning retransmissions 3
CES(config-group/ipsec)#client nat interval 00:00:18
CES(config-group/ipsec)#nat-traversal nat-detect
CES(config-group/ipsec)#no client auto-connect
CES(config-group/ipsec)#no client auto-connect networks
CES(config-group/ipsec)#no client auto-connect domains
```

```
CES(config-group/ipsec)#ip domain-name "test"
CES(config-group/ipsec)#ip address 0.0.0.0
CES(config-group/ipsec)#ip address 0.0.0.0 secondary
CES(config-group/ipsec)#wins address 0.0.0.0
CES(config-group/ipsec)#wins address 0.0.0.0 secondary
CES(config-group/ipsec)#no authentication local rsa-sig
CES(config-group/ipsec)#authentication local username-password
CES(config-group/ipsec)#authentication local rsa-sig server-ca "CN=CLI1
interop, O=contivity, C=US, OU=interop-lab"
% Certificate "CN=CLI1 interop, O=contivity, C=US, OU=interop-lab" does
not exist
CES(config-group/ipsec)#authentication external passgo-defender
CES(config-group/ipsec)#authentication external username-password
CES(config-group/ipsec)#no authentication external dynamic-securid
CES(config-group/ipsec)#authentication external groupid "hello" password
"asdf"
CES(config-group/ipsec)#forced-logoff 00:00:00
CES(config-group/ipsec)#no split tunneling
CES(config-group/ipsec)#split tunnel-network "testNetwork"
CES(config-group/ipsec)#exit
CES(config)#

CES(config)#! Default All
CES(config)#group ipsec "/Base/grouptest"
CES(config-group/ipsec)#def all
CES(config-group/ipsec)#exit
CES(config)#

CES(config)#! Show IPSEC Properties
CES(config)#show group ipsec /Base
IPSEC Settings:
  Rekey Timeout                                          : 08:00:00
  Rekey Data Count                                       : 0
  Perfect Forward Secrecy                                : Enabled
  Banner                                                : Not Configured
  Domain name                                           : Not Configured
  Display Banner                                         : Disabled
  Compression                                            : Enabled
  Primary DNS Address                                    : 0.0.0.0
  Primary WINS Address                                   : 0.0.0.0
  Secondary DNS Address                                  : 0.0.0.0
  Secondary WINS Address                                 : 0.0.0.0
  Allow Clients                                          : ALL
  Allow undefined networks for non-Contivity clients     : Enabled
```

```
  Allow Password Storage on Client                          : Disabled
  ESP - Triple DES with SHA1 Integrity                      : Disabled
  ESP - Triple DES with MD5 Integrity                       : Disabled
  ESP - 56-bit DES with SHA1 Integrity                      : Disabled
  ESP - 56-bit DES with MD5 Integrity                       : Enabled
  ESP - 40-bit DES with SHA1 Integrity                      : Disabled
  ESP - 40-bit DES with MD5 Integrity                       : Disabled
  ESP - NULL (Authentication Only) with SHA1 Integrity    : Disabled
  ESP - NULL (Authentication Only) with MD5 Integrity     : Disabled
  AH - Authentication Only (HMAC-SHA1)                      : Enabled
  AH - Authentication Only (HMAC-MD5)                       : Enabled
  IKE Encryption and Diffie-Hellman Group                   : 56-bit DES
with Group 1
  Client Failover Tuning                                    : Enabled
  Client Failover Tuning Interval                           : 00:01:00
  Client Failover Tuning Max Number of Retransmissions    : 3
  Client NAT Interval                                       : 00:00:18
  Client Auto Connect                                       : Disabled
  Client Auto Connect Type                                  : Any Network
Traffic
  Client Auto Connect Networks                            : Not Configured
  Client Auto Connect Domains                             : Not Configured
  Client Screen Saver Password Required                     : Disabled
  Client Screen Saver Activation Time                       : 5
  Client Policy                                           : Not Configured
  LDAP Authentication  - User Name and Password             : Enabled
  LDAP Authentication  - RSA Digital Signature              : Enabled
  LDAP Authentication  - Default Server Certificate         : Not
Configured
External Authentication - PassGo Technologies Defender   : Disabled
External Authentication - User Name and Password        : Disabled
  External Authentication - Security Dynamics SecurID     : Disabled
  External Authentication - Group ID                      : Not Configured
  External Authentication - Text Password                 : Not Configured
  Nat Traversal                                           : Auto-Detect NAT
  Nortel client requirements Action                       : Not Configured
  Nortel client requirements Version                      : Not Configured
  Nortel client requirements Message                      : Not Configured
  Nortel client requirements Filter                       : Not Configured
  Split Tunneling                                           : Disabled
  Split Tunneling Networks                                : Not Configured
  Forced Logoff                                             : 00:00:00

CES(config)#! Show IPSEC Properties
```

```
CES(config)#show group ipsec /Base/grouptest
IPSEC Settings:
  Rekey Timeout                                              : 08:00:00
  Rekey Data Count                                           : 0
  Perfect Forward Secrecy                                    : Enabled
  Banner                                                   : Not Configured
  Domain name                                              : Not Configured
  Display Banner                                             : Disabled
  Compression                                                : Enabled
  Primary DNS Address                                        : 0.0.0.0
  Primary WINS Address                                       : 0.0.0.0
  Secondary DNS Address                                      : 0.0.0.0
  Secondary WINS Address                                     : 0.0.0.0
  Allow Clients                                              : ALL
  Allow undefined networks for non-Contivity clients         : Enabled
  Allow Password Storage on Client                           : Disabled
  ESP - Triple DES with SHA1 Integrity                       : Disabled
  ESP - Triple DES with MD5 Integrity                        : Disabled
  ESP - 56-bit DES with SHA1 Integrity                       : Disabled
  ESP - 56-bit DES with MD5 Integrity                        : Enabled
  ESP - 40-bit DES with SHA1 Integrity                       : Disabled
  ESP - 40-bit DES with MD5 Integrity                        : Disabled
  ESP - NULL (Authentication Only) with SHA1 Integrity       : Disabled
  ESP - NULL (Authentication Only) with MD5 Integrity        : Disabled
  AH - Authentication Only (HMAC-SHA1)                       : Enabled
  AH - Authentication Only (HMAC-MD5)                        : Enabled
  IKE Encryption and Diffie-Hellman Group                    : 56-bit DES
with Group 1/ Triple DES with Group 7
  Client Failover Tuning                                     : Enabled
  Client Failover Tuning Interval                            : 00:01:00
  Client Failover Tuning Max Number of Retransmissions       : 3
  Client NAT Interval                                        : 00:00:18
  Client Auto Connect                                        : Disabled
  Client Auto Connect Type                                   : Any Network
Traffic
  Client Auto Connect Networks                             : Not Configured
  Client Auto Connect Domains                              : Not Configured
  Client Screen Saver Password Required                      : Disabled
  Client Screen Saver Activation Time                        : 5
  Client Policy                                            : Not Configured
  LDAP Authentication  - User Name and Password              : Enabled
  LDAP Authentication  - RSA Digital Signature               : Enabled
  LDAP Authentication  - Default Server Certificate          : Not
Configured
```

```
  External Authentication - User Name and Password        : Disabled
  External Authentication - Security Dynamics SecurID     : Disabled
  External Authentication - Group ID                      : hello
  External Authentication - Text Password                 : ********
  Nat Traversal                                          : Auto-Detect NAT
  Nortel client requirements Action                       : Not Configured
  Nortel client requirements Version                      : Not Configured
  Nortel client requirements Message                      : Not Configured
  Nortel client requirements Filter                       : Not Configured
  Split Tunneling                                           : Disabled
  Split Tunneling Networks                                : Not Configured
  Forced Logoff                                             : 00:00:00
CES(config)#
CES(config)#
CES(config)#

CES(config)#! Show L2TP Properties
CES(config)#show group l2tp /Base/grouptest
L2TP Settings:
  Authentication PAP                                        : Disabled
  Authentication CHAP                                       : Enabled
  Authentication MSCHAP Version 1                           : Enabled
  Authentication MSCHAP Version 2                           : Enabled
  Authentication MSCHAP Encryption None                     : Enabled
  Authentication MSCHAP Encryption RC4-128                  : Enabled
  Authentication MSCHAP Encryption RC4-40                   : Enabled
  Client Address                                            : Disabled
  Compression                                               : Enabled
  Minimum IPsec Data Protection Level                       : Not Required
  Require IPsec Transport Mode Connections from             : /Base
  Primary DNS Address                                       : 0.0.0.0
  Primary WINS Address                                      : 0.0.0.0
  Secondary DNS Address                                     : 0.0.0.0
  Secondary WINS Address                                    : 0.0.0.0

CES(config)#! Change L2TP Properties
CES(config)#group l2tp /Base/grouptest
CES(config-group/l2tp)#client-address
CES(config-group/l2tp)#default ipsec-data-protection
CES(config-group/l2tp)#default ipsec-credentials
CES(config-group/l2tp)#no compress
CES(config-group/l2tp)#ip address 12.23.23.3
CES(config-group/l2tp)#ip address 12.23.0.45 secondary
CES(config-group/l2tp)#wins address 123.23.23.3
```

```
CES(config-group/l2tp)#wins address 123.2.12.33 secondary
CES(config-group/l2tp)#no authentication pap
CES(config-group/l2tp)#no authentication chap
CES(config-group/l2tp)#no authentication ms-chap version 1
CES(config-group/l2tp)#no authentication ms-chap version 2
% You must enable at least one MS-Chap Version
CES(config-group/l2tp)#no authentication ms-chap encryption none
CES(config-group/l2tp)#no authentication ms-chap encryption rc4-40
CES(config-group/l2tp)#no authentication ms-chap encryption rc4-128
% You must enable at least one encryption setting
CES(config-group/l2tp)#exit

CES(config)#! Show L2TP Properties
CES(config)#show group l2tp /Base/grouptest
L2TP Settings:
  Authentication PAP                                    : Disabled
  Authentication CHAP                                   : Disabled
  Authentication MSCHAP Version 1                       : Disabled
  Authentication MSCHAP Version 2                       : Enabled
  Authentication MSCHAP Encryption None                 : Disabled
  Authentication MSCHAP Encryption RC4-128              : Enabled
  Authentication MSCHAP Encryption RC4-40               : Disabled
  Client Address                                        : Enabled
  Compression                                           : Disabled
  Minimum IPsec Data Protection Level                   : Not Required
  Require IPsec Transport Mode Connections from         : /Base
  Primary DNS Address                                   : 12.23.23.3
  Primary WINS Address                                  : 123.23.23.3
  Secondary DNS Address                                 : 12.23.0.45
  Secondary WINS Address                                : 123.2.12.33

CES(config)#! Set the L2TP Properties to default values
CES(config)#group l2tp /Base/grouptest
CES(config-group/l2tp)#default authentication
CES(config-group/l2tp)#exit
CES(config)#group l2tp /Base/grouptest
CES(config-group/l2tp)#default all
CES(config-group/l2tp)#exit

CES(config)#! Show the parent properties
CES(config)#show group l2tp /Base

L2TP Settings:
  Authentication PAP                                    : Disabled
```

```
  Authentication CHAP                                    : Enabled
  Authentication MSCHAP Version 1                        : Enabled
  Authentication MSCHAP Version 2                        : Enabled
  Authentication MSCHAP Encryption None                  : Enabled
  Authentication MSCHAP Encryption RC4-128               : Enabled
  Authentication MSCHAP Encryption RC4-40                : Enabled
  Client Address                                         : Disabled
  Compression                                            : Enabled
  Minimum IPsec Data Protection Level                    : Not Required
  Require IPsec Transport Mode Connections from          : /Base
  Primary DNS Address                                    : 0.0.0.0
  Primary WINS Address                                   : 0.0.0.0
  Secondary DNS Address                                  : 0.0.0.0
  Secondary WINS Address                                 : 0.0.0.0

CES(config)#! Show the group properties
CES(config)#show group l2tp /Base/grouptest
L2TP Settings:
  Authentication PAP                                     : Disabled
  Authentication CHAP                                    : Enabled
  Authentication MSCHAP Version 1                        : Enabled
  Authentication MSCHAP Version 2                        : Enabled
  Authentication MSCHAP Encryption None                  : Enabled
  Authentication MSCHAP Encryption RC4-128               : Enabled
  Authentication MSCHAP Encryption RC4-40                : Enabled
  Client Address                                         : Disabled
  Compression                                            : Enabled
  Minimum IPsec Data Protection Level                    : Not Required
  Require IPsec Transport Mode Connections from          : /Base
  Primary DNS Address                                    : 0.0.0.0
  Primary WINS Address                                   : 0.0.0.0
  Secondary DNS Address                                  : 0.0.0.0
  Secondary WINS Address                                 : 0.0.0.0
CES(config)#!
CES(config)#! Show PPTP Properties
CES(config)#show group pptp /Base/grouptest
PPTP Settings:
  Authentication PAP                                     : Disabled
  Authentication CHAP                                    : Enabled
  Authentication MSCHAP Version 1                        : Enabled
  Authentication MSCHAP Version 2                        : Enabled
  Authentication MSCHAP Encryption None                  : Enabled
  Authentication MSCHAP Encryption RC4-128               : Enabled
  Authentication MSCHAP Encryption RC4-40                : Enabled
```

```
  Client Address                                          : Disabled
  Compression                                             : Enabled
  Primary DNS Address                                     : 0.0.0.0
  Primary WINS Address                                    : 0.0.0.0
  Secondary DNS Address                                   : 0.0.0.0
  Secondary WINS Address                                  : 0.0.0.0

CES(config)#! Change PPTP Properties
CES(config)#group pptp /Base/grouptest
CES(config-group/pptp)#no authentication pap
CES(config-group/pptp)#no authentication chap
CES(config-group/pptp)#no authentication ms-chap version 1
CES(config-group/pptp)#no authentication ms-chap version 2
% You must enable at least one MS-Chap Version
CES(config-group/pptp)#no authentication ms-chap encryption none
CES(config-group/pptp)#no authentication ms-chap encryption rc4-40
CES(config-group/pptp)#no authentication ms-chap encryption rc4-128
% You must enable at least one encryption setting
CES(config-group/pptp)#exit

CES(config)#! Show PPTP Properties
CES(config)#show group pptp /Base/grouptest
PPTP Settings:
  Authentication PAP                                      : Disabled
  Authentication CHAP                                     : Disabled
  Authentication MSCHAP Version 1                         : Disabled
  Authentication MSCHAP Version 2                         : Enabled
  Authentication MSCHAP Encryption None                   : Disabled
  Authentication MSCHAP Encryption RC4-128                : Enabled
  Authentication MSCHAP Encryption RC4-40                 : Disabled
  Client Address                                          : Disabled
  Compression                                             : Enabled
  Primary DNS Address                                     : 0.0.0.0
  Primary WINS Address                                    : 0.0.0.0
  Secondary DNS Address                                   : 0.0.0.0
  Secondary WINS Address                                  : 0.0.0.0

CES(config)#! Set the PPTP Properties to default values
CES(config)#group pptp /Base/grouptest
CES(config-group/pptp)#default authentication
CES(config-group/pptp)#exit

CES(config)#! Show the parent properties
CES(config)#show group pptp /Base
```

```
PPTP Settings:
  Authentication PAP                                    : Disabled
  Authentication CHAP                                   : Enabled
  Authentication MSCHAP Version 1                       : Enabled
  Authentication MSCHAP Version 2                       : Enabled
  Authentication MSCHAP Encryption None                 : Enabled
  Authentication MSCHAP Encryption RC4-128              : Enabled
  Authentication MSCHAP Encryption RC4-40               : Enabled
  Client Address                                        : Disabled
  Compression                                           : Enabled
  Primary DNS Address                                   : 0.0.0.0
  Primary WINS Address                                  : 0.0.0.0
  Secondary DNS Address                                 : 0.0.0.0
  Secondary WINS Address                                : 0.0.0.0

CES(config)#! Show the group properties
CES(config)#show group pptp /Base/grouptest
PPTP Settings:
  Authentication PAP                                    : Disabled
  Authentication CHAP                                   : Enabled
  Authentication MSCHAP Version 1                       : Enabled
  Authentication MSCHAP Version 2                       : Enabled
  Authentication MSCHAP Encryption None                 : Enabled
  Authentication MSCHAP Encryption RC4-128              : Enabled
  Authentication MSCHAP Encryption RC4-40               : Enabled
  Client Address                                        : Disabled
  Compression                                           : Enabled
  Primary DNS Address                                   : 0.0.0.0
  Primary WINS Address                                  : 0.0.0.0
  Secondary DNS Address                                 : 0.0.0.0
  Secondary WINS Address                                : 0.0.0.0
CES(config)#! Show L2F Properties
CES(config)#show group l2f /Base/grouptest
L2F Settings:
  Authentication PAP                                    : Disabled
  Authentication CHAP                                   : Enabled
  Client Address                                        : Disabled
  Compression                                           : Enabled
  Primary DNS Address                                   : 0.0.0.0
  Primary WINS Address                                  : 0.0.0.0
  Secondary DNS Address                                 : 0.0.0.0
  Secondary WINS Address                                : 0.0.0.0
CES(config)#! Change L2F Properties
CES(config)#group l2f /Base/grouptest
```

```
CES(config-group/l2f)#no authentication pap
CES(config-group/l2f)#no authentication chap
% You must enable at least one Authentication Method
CES(config-group/l2f)#exit
CES(config)#! Show L2F Properties
CES(config)#show group l2f /Base/grouptest
L2F Settings:
  Authentication PAP                                    : Disabled
  Authentication CHAP                                   : Enabled
  Client Address                                        : Disabled
  Compression                                           : Enabled
  Primary DNS Address                                   : 0.0.0.0
  Primary WINS Address                                  : 0.0.0.0
  Secondary DNS Address                                 : 0.0.0.0
  Secondary WINS Address                                : 0.0.0.0
CES(config)#group l2f /Base/grouptest
CES(config-group/l2f)#default authentication
CES(config-group/l2f)#exit
CES(config)#! Show L2F Properties
CES(config)#show group l2f /Base
L2F Settings:
  Authentication PAP                                    : Disabled
  Authentication CHAP                                   : Enabled
  Client Address                                        : Disabled
  Compression                                           : Enabled
  Primary DNS Address                                   : 0.0.0.0
  Primary WINS Address                                  : 0.0.0.0
  Secondary DNS Address                                 : 0.0.0.0
  Secondary WINS Address                                : 0.0.0.0
CES(config)#! Show L2F Properties
CES(config)#show group l2f /Base/grouptest
L2F Settings:
  Authentication PAP                                    : Disabled
  Authentication CHAP                                   : Enabled
  Client Address                                        : Disabled
  Compression                                           : Enabled
  Primary DNS Address                                   : 0.0.0.0
  Primary WINS Address                                  : 0.0.0.0
  Secondary DNS Address                                 : 0.0.0.0
  Secondary WINS Address                                : 0.0.0.0
CES(config)#exit
CES#exit
CES>exit
```

Appendix B
Using the bulk load commands

The **bulk load** command enables an administrator to send a list of commands and parameters to a Nortel VPN Router and have them executed in series. This command allows an administrator with many Nortel VPN Routers to configure them in bulk from a list of settings instead of having to configure each VPN Router manually through the browser interface.

This appendix describes the user commands for using the bulk load utility.



Note: In Version 4.0, the bulk load function was replaced with new commands. You can continue to use the **LOAD** command and any scripts that were developed prior to Version 4.0. For future CLI scripting, use the full CLI capability described in this document.

bulk load command

The **bulk load** command allows an administrator to configure several different aspects of the VPN Router, such as users, branch office connections, and tunnel types.

The **bulk load** command is executed via Telnet using the **load** command. The **load** command has the following syntax:

```
CES(config)# load <filename>
```

As the command executes, any errors encountered will be displayed on the screen. Most errors are reported in the following format:

```
% Error:<error_message> at line number <line_number>: end
```

The line number refers to the `end` label of the command in error.

If errors occur during the execution of a command, they are displayed. Non-error status information is not displayed during the execution of the commands. After a command has been executed, its results can be verified by viewing the corresponding GUI page.

Note: A bulk load file can contain a maximum of 40,000 lines, including blank lines.

Components

The bulk loading feature has two main components: the command file and the **`load`** command.

load command

The **`load`** command is available only through the Telnet or serial interface. Once executed, the command will load the specified command file, and execute the instructions it contains. When completed, the command file will be deleted. Following is the syntax of the **`load`** command:

`CES(config)# load <command_filename>`

Command file

The command file is a text file containing a sequence of commands that are to be executed. The file is located in the /system/command directory on the boot disk. The command file has the following characteristics:

- The command file must conform to the 8.3 naming convention.
- Each command file begins with the string FILE_FORMAT: [*format*].
- Each command is initiated with the string COMMAND: xxxx.
- Each command is terminated with the string END.
- Each command accepts a number of qualifiers. Each qualifier is defined by TYPE: VALUE pairs; for example NAME is the field type, and Joe is the field value.
- The comment character is //.

- The command file must end with a blank line.
- A command file may contain an unlimited number of commands.
- When all commands have been executed, the command file is automatically deleted.



Note: The bulk load command files do not support embedded comments. If you place a comment on the same line as a command or attribute, errors may occur.

file_format command

The **`file_format`** command defines what versions of the bulk load commands are contained in the command file. In Version 3.0, bulk loading file formats 1.0, 2.0, and 3.0 are supported. The FILE_FORMAT command is useful if a bulk load script is to be used on several Nortel VPN Routers with different releases installed. For example, the following command file may be executed on a Nortel VPN Router installed with Versions 2.50, 2.60, and 3.00:

```
file_format: 1.0
command: one
[...]
end
file_format: 2.0
command: two
[...]
end
file_format: 3.0
command: three
[...]
end
```

The Version 2.50 Nortel VPN Router will recognize and execute command 1 and ignore commands 2 and 3. The Version 2.60 Nortel VPN Router will recognize both commands 1 and 2, but will ignore command 3. The Version 3.0 Nortel VPN Router will recognize all three commands. If the command file is only being used on a Version 3.00 Nortel VPN Router, the file format may be set to 1.0, 2.0, or 3.0.



Note: In Version 4.0, the bulk load functionwas replaced with new commands. You can continue to use the **load** command and any scripts that were developed prior to Version 4.0. For future CLI scripting, use the full CLI capability described in Chapter 5, “Creating and using scripts to provision a VPN Router,” on page 255.

User commands

User commands allow an administrator to add or delete user records. They also allow an administrator to add or delete user groups. The supported user commands are:

ADD_GROUP
ADD_USER
DELETE_GROUP
DELETE_USER
MODIFY_GROUP
PURGE_GROUP
RESET_USER_CERTS

ADD_GROUP

The **ADD_GROUP** command is used to add a group to the Nortel VPN Router database.

```
COMMAND: ADD_GROUP
GROUP: [Group name - Required]
END
```

ADD_USER

The **ADD_USER** command is used to add a user or user group. A user record must contain authentication credentials (such as UID and password, DN, and so forth.) before the user is added to the database.

```
COMMAND: ADD_USER
GROUP: [Group name]
NAME: [User name - Required]
STATIC_ADDR_IP: [Static IP address]
STATIC_ADDR_MASK: [Static IP address mask]
IPSEC_UID: [IPSec User ID - Required if not using
certificates]
IPSEC_PSW: [IPSec password - Required if not using
certificates]
IPSEC_SUBJECTDN: [Subject distinguished name - Required if
using certificates and not IPSEC_ALTNAME]
IPSEC_ALTNAME: [Subject alternative name - Required if using
certificates and not IPSEC_SUBJECTDN]
IPSEC_TYPE: [Subject name type {Email/DNS/IP} - Required
with certificates and IPSEC_ALTNAME]
IPSEC_ISSUERCA: [Issuer certificate authority - Required
with certificates]
SERVER_CERT: [Server Certificate - Default: Inherit from
group]
RESTRICTED: [Control User Tunnel {True/False} -
Default:False]
END
```

DELETE_ALL

The **DELETE_ALL** command deletes all users in the database.



Caution: This command should only be executed by the Nortel VPN Router administrator because all other accounts are removed.

```
COMMAND: DELETE_ALL
END
```

DELETE_USER

The **DELETE_USER** command is used to delete a specified user record from the database. You must include a user name. If you do not specify a group, the /Base group is assumed.

```
COMMAND: DELETE_USER
GROUP: [Group name]
NAME: [User name - Required]
END
```

DELETE_GROUP

The **DELETE_GROUP** command is used to delete a specified group and its users.

```
COMMAND: DELETE_GROUP
GROUP: [Group name - Required]
END
```

MODIFY_GROUP

The **MODIFY_GROUP** command is used to modify existing user groups. Any set of these attributes may be included in this command. Any attribute not specified inherits the value from its parent group.

```
COMMAND: MODIFY_GROUP
GROUP: [Group name - Required]
// Connectivity Attributes
FILT_NAME: [Name of existing filter]
CALL_PRI: [Call admission priority {Low/Medium/High/Highest}]
FORWARD_PRI: [Forwarding priority {Low/Medium/High/Highest}]
NUM_LOGINS: [Number of logins]
STATIC_ADDR: [Static addresses {Enable/Disable}]
IDLE_TO: [Idle timeout period (hh:mm:ss format)]
FORCED_LO_TIME: [Forced logout timeout (hh:mm:ss format)]
SPLIT_TUN: [Split tunneling {Enable/Disable}]
SPLIT_TUN_NET: [Split tunnel network name]
ADDR_POOL: [Address pool name or 'Default' for default pool]
// Bandwidth Policy
BW_COMMIT_RATE: [Committed Bandwidth Rate (bps)]
BW_EXCESS_RATE: [EXCESS Bandwidth Rate (bps)]
BW_EXCESS_ACTION: [EXCESS Rate Action {Drop/Mark}]
// IPSEC Attributes
DIG_SIG: [RSA Digital Signature {Enable/Disable}]
UNAMEPW: [User Name/Password Authentication {Enable/Disable}]
SERVER_CERT: [Default server certificate]
ESP_3SHA1: [ESP - Triple DES with SHA1 Integrity {Enable/Disable}]
ESP_3MD5: [ESP - Triple DES with MD5 Integrity {Enable/Disable}]
ESP_56SHA1: [ESP - 56-bit DES with SHA1 Integrity {Enable/Disable]
ESP_56MD5: [ESP - 56-bit DES with MD5 Integrity {Enable/Disable}]
ESP_40SHA1: [ESP - 40-bit DES with SHA1 Integrity {Enable/Disable}
ESP_40MD5: [ESP - 40-bit DES with MD5 Integrity {Enable/Disable}]
ESP_NULLSHA1: [ESP - NULL (Authentication Only) with SHA1 Integrity
{Enable/Disable}]
ESP_NULLMD5: [ESP - NULL (Authentication Only) with MD5 Integrity
{Enable/Disable}]
AH_SHA1: [AH - Authentication Only (HMAC-SHA1) {Enable/Disable}]
AH_MD5: [AH - Authentication Only (HMAC-MD5) {Enable/Disable}]
SCRSVR_PSW: [Client screen saver password required Enable/Disable}]
SCRSVR_INT: [Client screen saver interval]
PSW_ON_CLI: [Allow password storage on client {Enable/Disable}]
PFS: [Perfect forward security {Enable/Disable}]
```

```
COMPRESSION: [Compression {Enable/Disable}]
REKEY_TO: [Rekey timeout (hh:mm:ss format)]
REKEY_DATACNT: [Rekey datacount (in KB)]
DOMAIN: [Domain name]
PRI_DNS: [Primary DNS address]
PRI_WINS: [Primary WINS address]
SEC_DNS: [Secondary DNS address]
SEC_WINS: [Secondary WINS address]
END
```

PURGE_GROUP

The **PURGE_GROUP** command is used to delete all users in a specified group. If you do not specify a group, the command purges all users in the /Base group.

```
COMMAND: PURGE_GROUP
GROUP: [Group name - Required]
END
```

Branch office commands

Branch office commands allow an administrator to add or delete branch office connections, including control tunnel connections. These commands also allow administrators to add and delete branch office groups. The supported branch office commands are:

ADD_BRANCHGROUP
ADD_CONNECTION
DELETE_ALLBRANCH
DELETE_BRANCHGROUP
DELETE_CONNECTION
MODIFY_BRANCHGROUP
PURGE_BRANCHGROUP

ADD_CONNECTION

The **ADD_CONNECTION** command defines a branch office control connection with specific attributes. The connection must contain authentication information before it is created. Once a connection is created with the required attributes, it is automatically enabled. This command has been modified for the Nortel VPN Router Version 3.0

```
COMMAND: ADD_CONNECTION
GROUP: [Group name]
NAME: [Connection name - Required]
SYSTEM_IP: [VPN Router management IP address - Required for
Restricted tunnel]
```



Note: Using a SYSTEM _IP value other than the actual management IP address, will create a NAT SET for the Management IP.

```
LOCAL_ENDPOINT: [Local interface IP address - Required]
REMOTE_ENDPOINT: [Remote interface IP address - Required]
RESTRICTED: [Control Tunnel {True/False} - Default:False]
FILT_NAME: [Tunnel filter name - Required]
ROUTING: [Routing type {Static/Dynamic} - Default:Static]
TUNNEL: [Tunnel type {IPSEC,PPTP,L2TP} - Default:IPSEC]
// Static Routing
NET_NAME: [Local acContivitysible network - Required for
Static Routing]
NAT_NAME: [NAT Translation (Optional for Static Routing)]
SUBNET: [Remote AcContivitysible Net Subnet - Required for
Static Routing]
MASK: [Remote AcContivitysible Net Subnet mask - Required
for Static Routing]
REM_NET_COST: [Remote network cost - Default:10]
REM_NET_STATE: [Remote network state - {Enable/Disable}
Default: Enable]
// Dynamic Routing
OSPF_STATE: [OSPF state {Enable/Disable} (Dynamic Routing)
Default:Disable]
AREA_ID: [Area ID (Dynamic Routing) - Default:0.0.0.0]
OSPF_COST: [OSPF cost (Dynamic Routing) - Default:10]
RIP_STATE: [Rip state {Enable/Disable} (Dynamic Routing) -
Default: Disable]
```

```
// IPSec Authentication
IPSEC_PSW: [IPSec password - Required if not using
certificates]
IPSEC_SUBJECTDN: [Subject distinguished name - Required if
using certificates and not IPSEC_ALTNAME]
IPSEC_ALTNAME: [Subject alternative name - Required if using
certificates and not IPSEC_SUBJECTDN]
IPSEC_TYPE: [Subject name type {Email/DNS/IP} - Required
with certificates and IPSEC_ALTNAME]
IPSEC_ISSUERCA: [Issuer certificate authority - Required
with certificates]
SERVER_CERT: [Server Certificate - Required with
certificates]
SERVER_ALTNAME: [Server Certificate Alternate name]
// PPTP/L2TP Authentication
TUNNEL_AUTH: [MSChap V2 Authentication {RC4-128,RC4-40,
Unencrypt} - (PPTP & L2TP tunnel types)]
LOCAL_UID: [Tunnel authentication - local user ID - (PPTP &
L2TP tunnel types) - Required for PPTP/L2TP]
PEER_UID: [Tunnel authentication - peer user ID - (PPTP &
L2TP tunnel types) - Required for PPTP/L2TP]
PEER_PSW: [Tunnel authentication - peer password - (PPTP &
L2TP tunnel types)]
COMPRESSION: [PPTP & L2TP compression {Enable/Disable} -
(PPTP & L2TP tunnel types)]
ENC_STATE_MODE: [PPTP & L2TP Compression/Encryption
stateless mode {Enable/Disable} - (PPTP & L2TP tunnel
types)]
// L2TP specific authentication parameters
CONCENTRATOR: [L2TP Concentrator (L2TP tunnel type)]
L2TP_IPSEC_XPORT: [L2TP IPSEC Transport {None, 3DES, 56DES,
40DES, AH} - (L2TP tunnel type only)]
END
```

ADD_BRANCHGROUP

The **ADD_BRANCHGROUP** command creates a branch office group as specified. A group name is required.

```
COMMAND: ADD_BRANCHGROUP
GROUP: [Group name - Required]
END
```

DELETE_CONNECTION

The **DELETE_CONNECTION** command deletes the specified connection from the branch office group.

```
COMMAND: DELETE_CONNECTION
NAME: [Connection name - Required]
GROUP: [Group name - Default:/Base]
END
```

MODIFY_CONNECTION

The **MODIFY_CONNECTION** command is used to add a new remote accessible network entry to an existing branch office connection.

```
COMMAND: MODIFY_CONNECTION
GROUP: [Branch Office group - Default:/Base]
NAME: [Name of existing Branch Office connection to modify -
Required]
SUBNET: [Remote Network subnet - Required]
MASK: [Remote Network subnet mask - Required]
REM_NET_COST: [Remote network cost - Default:10]
REM_NET_STATE: [Remote network state - {Enable/Disable}
Default:Enable]
END
```

MODIFY_BRANCHGROUP

The **MODIFY_BRANCHGROUP** command is used to modify existing branch office groups. All values that are not specified will inherit values from its parent group.

```
NOTE: COMMAND: MODIFY_BRANCHGROUP
GROUP: [Name of existing Branch Office group to modify
-Required]
//Connectivity Attributes
CALL_PRI: [Call admission priority {Low/Medium/High/
Highest}]
FORWARD_PRI: [Forwarding priority {Low/Medium/High/Highest}]
IDLE_TO: [Idle timeout period (hh:mm:ss format)]
// Bandwidth Policy
BW_COMMIT_RATE: [Committed Bandwidth Rate (bps)]
BW_EXCESS_RATE: [EXCESS Bandwidth Rate (bps)]
BW_EXCESS_ACTION: [EXCESS Rate Action {Drop/Mark}]
// IPSEC Attributes
ESP_3SHA1: [ESP - Triple DES with SHA1 Integrity {Enable/
Disable}]
ESP_3MD5: [ESP - Triple DES with MD5 Integrity {Enable/
Disable}]
ESP_56SHA1: [ESP - 56-bit DES with SHA1 Integrity {Enable/
Disable}]
ESP_56MD5: [ESP - 56-bit DES with MD5 Integrity {Enable/
Disable}]
ESP_40SHA1: [ESP - 40-bit DES with SHA1 Integrity {Enable/
Disable}]
ESP_40MD5: [ESP - 40-bit DES with MD5 Integrity {Enable/
Disable}]
ESP_NULLSHA1: [ESP - NULL (Authentication Only) with SHA1
Integrity {Enable/Disable}]
ESP_NULLMD5: [ESP - NULL (Authentication Only) with MD5
Integrity {Enable/Disable}]
AH_SHA1: [AH - Authentication Only (HMAC-SHA1) {Enable/
Disable}]
AH_MD5: [AH - Authentication Only (HMAC-MD5) {Enable/
Disable}]
VEND_ID: [Vendor ID {Enable/Disable}]
PFS: [Perfect forward security {Enable/Disable}]
COMPRESSION: [Compression {Enable/Disable}]
REKEY_TO: [Rekey timeout (hh:mm:ss format)]
REKEY_DATACNT: [Rekey datacount (in KB)]
```

```
// RIP Attributes
RIP_TRANSMIT: [Rip Transmit {OFF,V1,V2}]
RIP_RECEIVE: [Rip Receive {OFF,V1,V2}]
IMPORT_DEF_ROUTE: [Import Default Route {Enable/Disable}]
EXPORT_DEF_ROUTE: [Export default routes metric {Enable/
Disable}]
EXPORT_STATIC_ROUTE: [Export static routes metric {Enable/
Disable}]
EXPORT_BO_STATIC_ROUTE: [Export branch office static routes
metric (Enable/Disable}]
EXPORT_OSPF_ROUTE: [Export OSPF e static routes metric
(Disable, 1-15}]
POISON_REV: [Poison Reverse {Enable/Disable}]
RIP_AUTH: [Rip Authentication {None/Simple/MD5}]
//
```



Note: The following value does not accept the inherited keyword. The RIP_AUTH value controls the inheritance of this value.

```
//
RIP_PASS: [RIP authentication password]
// OSPF Attributes
OSPF_PRI: [OSPF Priority]
OSPF_DEAD_INT: [OSPF dead interval]
OSPF_HELLO_INT: [OSPF hello interval]
OSPF_REXMIT_INT: [OSPF retransmit interval]
OSPF_XMIT_DELAY: [OSPF transmission delay]
OSPF_AUTH: [OSPF Authentication {None/Simple/MD5}]
```



Note: The following values do not accept the inherited keyword. The OSPF_AUTH value will control the inheritance of these values.

```
OSPF_PASS: [OSPF Authentication Password]
MD5_PASS: [OSPF MD5 password]
MD5_KEY: [OSPF MD5 Key]
END
```

Nortel VPN Router configuration commands

Nortel VPN Router Configuration commands allow the administrator to configure Nortel VPN Router attributes such as network definitions, NAT, address pools, filters, automatic backup, syslog forwarding, SNMP settings, and DHCP servers.

Network definition commands

Three bulk load commands are used to manage network definitions:

CREATE_NETWORK
DELETE_NETWORK
MODIFY_NETWORK

CREATE_NETWORK

The **CREATE_NETWORK** command is used to add a new network definition.

```
COMMAND: CREATE_NETWORK
NET_NAME: [Name of new network definition - Required]
SUBNET: [New IP address - Required]
MASK: [New subnet mask - Required]
END
```

DELETE_NETWORK

The **DELETE_NETWORK** command is used to delete an existing network definition.

```
COMMAND: DELETE_NETWORK
NET_NAME: [Name of existing network to delete - Required]
END
```

MODIFY_NETWORK

The **MODIFY_NETWORK** command is used to add new subnets to an existing network definition.

```
COMMAND: MODIFY_NETWORK
NET_NAME: [Name of existing network to modify - Required]
SUBNET: [New IP address - Required]
MASK: [New subnet mask - Required]
END
```

NAT commands

Three bulk load commands are used to configure NAT settings: **CREATE_NAT**, **DELETE_NAT**, and **MODIFY_NAT**.

CREATE_NAT

The **CREATE_NAT** command is used to create a new NAT set.

```
COMMAND: CREATE_NAT
NAT_NAME: [Name of new NAT set - Required]
NAT_TYPE: [Translation Type {Static/Pooled/Port} - Required]
IN_START_IP: [Internal starting IP address - Required]
IN_END_IP: [Internal ending IP address - Required]
EX_START_IP: [External starting IP address - Required]
EX_END_IP: [External ending IP address - Required for Pooled
NAT type]
END
```

DELETE_NAT

The **DELETE_NAT** command is used to delete an existing NAT set.

```
COMMAND: DELETE_NAT
NAT_NAME: [Name of existing NAT set to delete - Required]
END
```

MODIFY_NAT

The **MODIFY_NAT** command is used to add a new rule to an existing NAT set.

```
COMMAND: MODIFY_NAT
NAT_NAME: [Name of existing NAT set to modify - Required]
NAT_TYPE: [Translation Type {Static/Pooled/Port} - Required]
IN_START_IP: [Internal starting IP address - Required]
IN_END_IP: [Internal ending IP address - Required]
EX_START_IP: [External starting IP address - Required]
EX_END_IP: [External ending IP address - Required for Pooled
NAT type]
END
```

Address pool commands

Two bulk load commands are used to configure address pools: **CREATE_POOL and DELETE_POOL**.

CREATE_POOL

The **CREATE_POOL** command is used to create a new address pool.

```
COMMAND: CREATE_POOL
NAME: [Name of new address pool]
IP_START: [Starting IP address - Required]
IP_END: [Ending IP address - Required]
MASK: [Subnet mask]
END
```

DELETE_POOL

The **DELETE_POOL** command is used to delete an existing address pool.

```
COMMAND: DELETE_POOL
IP_START: [Starting IP address - Required]
IP_END: [Ending IP address - Required]
END
```

Filter commands

Several bulk load commands are used to create and configure filters and filter rules:

ADD_RULE
CREATE_ADDRESS
CREATE_FILTER
CREATE_PORT
CREATE_RULE
DELETE_FILTER
DELETE_RULE

CREATE_FILTER

The **CREATE_FILTER** command allows for the creation of a new named filter. The filter may be created to allow or disallow certain management traffic. These fields are not required.

```
COMMAND: CREATE_FILTER
FILT_NAME: [Filter name - Required]
// Allow management traffic for…
HTTP_SVC: [HTTP local service {Enable/Disable}]
SNMP_SVC: [SNMP local service {Enable/Disable}]
FTP_SVC: [FTP local service {Enable/Disable}]
TELNET_SVC: [TELNET local service {Enable/Disable}]
PING_SVC: [Ping local service {Enable/Disable}]
RADIUS_SVC: [Radius local service {Enable/Disable}]
FIREWALL_SVC: [Firewall local service {Enable/Disable}]
FTP_SVR: [FTP remote server {Enable/Disable}]
DHCP_SVR: [DHCP remote server {Enable/Disable}]
RADIUS_SVR: [Radius remote server {Enable/Disable}]
DNS_SVR: [DNS remote server {Enable/Disable}]
END
```

DELETE_FILTER

The **DELETE_FILTER** command allows for the deletion of an existing filter.

```
COMMAND: DELETE_FILTER
FILT_NAME: [Filter name - Required]
END
```

The **ADD_RULE** command allows an existing rule to be added to an existing filter.

```
COMMAND: ADD_RULE
FILT_NAME: [Filter name - Required]
RULE_NAME: [Rule name - Required]
END
```

The **CREATE_RULE** command allows for the creation of a new rule definition.

```
COMMAND: CREATE_RULE
RULE_NAME: [Rule name - Required]
ADDR_NAME: [Address Name- Default:Any]
ACTION: [Rule action {Permit/Deny} - Default:Deny]
DIRECTION: [Direction {Inbound/Outbound} - Default:Inbound]
PROTOCOL: [Protocol Name - Default:Ip]
SRC_PORT: [Source Port Name - Default:Any]
DEST_PORT: [Destination Port Name - Default:Any]
END
```

CREATE_ADDRESS

The **CREATE_ADDRESS** command creates a new address definition to be used by a filter rule.

```
COMMAND: CREATE_ADDRESS
ADDR_NAME: [Address Name - Required]
IP_ADDR: [IP Address - Required]
MASK: [Address mask - Required]
END
```

CREATE_PORT

The **CREATE_PORT** command creates a new port definition to be used by a filter rule.

```
COMMAND: CREATE_PORT
PORT_NAME: [Port Name - Required]
PORT: [Port number - Required]
END
```

DELETE_RULE

The **DELETE_RULE** command deletes an existing rule definition. This command will fail if the rule is being used by a filter.

```
COMMAND: DELETE_RULE
RULE_NAME: [Rule name - Required]
END
```

Automatic backup commands

Two bulk load commands are available to configure the automatic backup feature:

ADD_FTPSERVER
DELETE_FTPSERVER

ADD_FTPSERVER

The **ADD_FTPSERVER** command is used to configure a new automatic backup server.

```
COMMAND: ADD_FTPSERVER
FTP_IP: [FTP host IP address - Required]
FTP_UID: [User ID for FTP host - Required]
FTP_ENABLE: [Enable Auto-backup Host - Default:Enable]
FTP_PSW: [Password for FTP host - Default: ""]
FTP_INTERVAL: [Time between backups (hours) - Default: 5]
FTP_PATH: [Path where files are stored - Default: \]
FTP_SERVER: [FTP Server {1/2/3} - Default: 1]
END
```

DELETE_FTPSERVER

The **DELETE_FTPSERVER** command is used to remote an existing automatic backup server.

```
COMMAND: DELETE_FTPSERVER
FTP_SERVER: [Existing FTP Server {1/2/3} - Required]
END
```

SYSLOG forwarding commands

Two bulk load commands are available to configure the syslog forwarding feature:

ADD_SYSLOG
DELETE_SYSLOG

ADD_SYSLOG

The **ADD_SYSLOG** command is used to setup a system log forwarding server.

```
COMMAND: ADD_SYSLOG
SLOG_IP [Host IP address - Required]
SLOG_MSGLEVEL: [Urgent/Normal/Detailed/All - Default:
Normal]
SLOG_FACILITY: [Syslog Facility {KERN/LOCAL[0-7]} -
Default:KERN]
SLOG_PORT: [Syslog port - Default: 514]
SLOG_ENABLE: [Enable Syslog Server - Default:Enable]
SLOG_SERVER: [Syslog Server {1/2/3/4} - Default: 1]
END
```

DELETE_SYSLOG

The **DELETE_SYSLOG** command is used to remove an existing system log forwarding server.

```
COMMAND: DELETE_SYSLOG
SLOG_SERVER: [Existing Syslog Server {1/2/3/4} - Required]
END
```

SNMP commands

Three bulk load commands are used to configure SNMP:

ADD_SNMPHOST
CONFIG_TRAP
DELETE_SNMPHOST

ADD_SNMPHOST

The **ADD_SNMPHOST** command is used to add and configure either SNMP-Get or Trap hosts.

```
COMMAND: ADD_SNMPHOST
SNMP_TYPE: [Get/Trap - Required]
SNMP_IP: [SNMP host IP address - Required]
SNMP_COMMUNITY: [SNMP Community name]
SNMP_ENABLE: [Enable SNMP Host - Default:Enable]
END
```

CONFIG_TRAP

The **CONFIG_TRAP** command is used to configure which conditions will cause traps.

```
COMMAND: CONFIG_TRAP
TRAP_DESCRIPTION: [Trap Description - Required]
TRAP_INTERVAL: [Time between trap checks (hh:mm:ss)]
TRAP_ENABLE: [Enable SNMP Trap - Default:Enable]
END
```

DELETE_SNMPHOST

The **DELETE_SNMPHOST** command is used to remove an existing SNMP-Get or Trap host.

```
COMMAND: DELETE_SNMPHOST
SNMP_TYPE: [Get/Trap - Required]
SNMP_IP: [SNMP host IP address - Required]
END
```

DHCP commands

Three bulk load commands are used to configure DHCP:

CONFIG_DHCP
CONFIG_REMOTE_POOL
DELETE_DHCP

CONFIG_DHCP

The **CONFIG_DHCP** command is used to setup the DHCP servers on the VPN Router.

```
COMMAND: CONFIG_DHCP
DHCP_TYPE: [DHCP servers to use {Any/Specified}]
DHCP_IP: [DHCP server IP address - Required if DHCP_SERVER
is specified]
DHCP_SERVER: [Specified DHCP server to modify {Primary/
Secondary/Tertiary} - Default:Primary]
CACHE_SIZE: [DHCP cache size]
IMMEDIATE_ADDR_REL: [Immediate address release {Enable/
Disable}]
END
CONFIG_REMOTE_POOL
The CONFIG_REMOTE_POOL command is used to set the type of
remote pool used by the VPN Router, either DHCP or Address
Pools.
COMMAND: CONFIG_REMOTE_POOL
POOL_TYPE: [Pool type to use {DHCP/Address Pool} - Required]
END
```

DELETE_DHCP

The **DELETE_DHCP** command is used to remote an existing DHCP server.

```
COMMAND: DELETE_DHCP
DHCP_SERVER: [Existing DHCP server to remove {Primary/
Secondary/Tertiary} - Required]
END
```

Licensing commands

Licensing of certain features will be supported in bulk load Version 3.0. The following two commands allow you to enable and disable a paid feature on the Nortel VPN Router:

DISABLE_PAID_FEATURE
ENABLE_PAID_FEATURE

DISABLE_PAID_FEATURE

The **DISABLE_PAID_FEATURE** command allows you to specify the licensing key to disable a paid feature on the Nortel VPN Router.

```
COMMAND: DISABLE_PAID_FEATURE
PAID_KEY: [Licensing key for the feature to be disabled]
END
```

ENABLE_PAID_FEATURE

The **ENABLE_PAID_FEATURE** command allows a user to specify the licensing key to enable a paid feature on the Nortel VPN Router.

```
COMMAND: ENABLE_PAID_FEATURE
PAID_KEY: [Licensing key for the feature to be enabled]
END
```

Usage notes

Deletion of groups

The **DELETE_GROUP** and **DELETE_BRANCHGROUP** commands can cause the LDAP server in use by the Nortel VPN Router to become unreachable while the group is being deleted. This can happen if the group being deleted has a large number of users or branch office connections defined (for example, more than 50). Deleting each user or branch office connection individually, using the **DELETE_USER** or **DELETE_CONNECTION** command lessens the load on the LDAP server, but it may increase the time required to execute the commands.

Required fields for user and branch records

You must specify an authentication method and details when using the **ADD_CONNECTION** and **ADD_USER** commands. Valid authentication information can be specified using any one of the following combinations of attributes:

- Text Password
- Subject Distinguished Name (DN), a valid issuer certificate authority (CA), and a valid server certificate
- Subject Alternative Name, Subject Alternative Name Type, a valid issuer certificate authority (CA), and a valid server certificate



Note: Server certificates may be inherited from a user's group for **ADD_USER**.

Group name syntax

For many of the user and branch office commands, you must specify the name of the group that you are manipulating. The syntax of the group name is very important. Group names are specified in relative distinguished name (RDN) format, leaving out the '/Base' specifier. For example:

```
/Base/Engineering' is specified as:
Group: ou=Engineering
/Base/Engineering/Software' is specified as:
Group: ou=Software, ou=Engineering
/Base/Field/Boston/Sales' is specified as:
Group: ou=Sales, ou=Boston, ou=Field
```

Certificate distinguished name order

The Distinguished Name for certificates must be entered in the same order as they appear in the certificate. For Example:

```
cn=Joe, ou=My Org Unit, o=Some Org, c=US
```

is not the same as:

```
cn=Joe, o=Some Org, ou=My Org Unit, c=US
```

Index

A

aaa 748
aaa accounting network radius 746
aaa accounting session update 747
aaa accounting timeout 748
aaa accounting timeout enable 750
aaa accounting update 751
aaa authentication administrator 666
aaa authentication fwua 668
aaa authentication ipsec 669
aaa authentication l2f 671
aaa authentication l2tp 672
aaa authentication ldap-server 790
aaa authentication pptp 673
aaa authorization network radius 752
access-hours for groups 275
access-hours global settings 456, 527
access-list permit/deny 1737
accounting radius-server 753
accounting radius-server host 754
action 278
action nexthop 279
activate 1581
address 282
add-rule - current filter set 280
add-rule - MF classifier 1789
administration group-manage 283
administration switch-manage 285
administration uid 287
administration users-manage 288, 288
adminname 553
aggregation 1644
antireplay enable 290
area 1600
arp 165
arp timeout 1090
asbr 1602
async 177
async-over-tcp enable 166
async-over-tcp local-ip-address 168, 172
async-over-tcp local-tcp-listen-port 174
async-over-tcp num-of-ticks 179
async-over-tcp originator 177
async-over-tcp peer-ip-address 170
async-over-tcp peer-tcp-listen-port 176
audible alarm 180
ault 2021
authentication (Branch Office Group RIP or Branch Office Group OSPF) 292
authentication (Group IPsec Tunnel) 293
authentication (L2TP, PPTP, L2F) 295
authentication ldap-server base-dn 791
authentication ldap-server contivity-group 793
authentication ldap-server default-group 794
authentication ldap-server digital-certificate 795
authentication ldap-server domain-delimiter 797
authentication ldap-server filter 798
authentication ldap-server host 799

authentication ldap-server ip-address 802
authentication ldap-server ldap-filter 803
authentication ldap-server net-mask 805
authentication ldap-server password 806
authentication ldap-server remove-suffix 808
authentication ldap-server subject-dn 809
authentication ldap-server timeout 811
authentication ldap-server uid 812
authentication ldap-server username-password 814
auto-answer 1254
auto-save-logging enable 182
auto-save-logging max-files 184
auto-summary 2005
auto-vlink 1604

B

banner 297
baud-rate 1255
bgp 2007, 2007
bgp always-compare-med 2007, 2007
bgp client-to-client reflection 2008
bgp cluster-id 2010
bgp multiple-paths 2013
bgp public 2014
bgp redistribute-internal 2015
bgp router-id 2017
bo-conn 486
bo-group 298
boot system 98
bootfile 840
Bulk Load Command 2139

C

ca-allow-all enable 911
ca-import enable 912
capture 1743
capture add 1745
capture enable 1748
capture save 1751
capture start 1752
capture stop 1754
ca-trusted enable 914
cd 68
circuit-id 1377
circuit-id - ATM interface 1334
class 1484
clear accounting 756
clear arp-cache 100
clear capture 1756
clear flow-cache 987
clear ip route 69
clear logging events 101
client 300
client auto-connect 303
client auto-connect networks 304
client dynamic-dns enable 306
client failover-tuning 307
client failover-tuning interval 309
client failover-tuning retransmissions 310
client nat interval 311
client policy 312
client screen-saver activation-time 314
client screen-saver password 315
client-address 302
client-policy 529
clip enable 1208
clip ip 1209
clip ip interface-type 1211
clip ip services 1213
clip ip state 1215

clock rate 1992
clock set 557
clock source 1464, 1994
clock timezone 558
clock-type 1918
cmp 675
committed rate 316
compat-3-6 1605
compress - branch office settings 488
compress - group settings 318
compress-files enable 560
configure terminal 102
connect - Dial Serial 1256
connect - ISDN 1290
connection 319
conn-type 489
console mode 186
contact 320
controller 1466
controller 56k 1996
controller atm 1335
conventions, text 45
copy 103
copy ip ospf-lsdb-table 1635
copy ip route-table 1636
cost 1485
counter disconnect 1920
counter fast-contact 1921
counter fast-poll 1922
counter no-response 1923
counter remote-busy 1924
counter slow-contact 1925
counter slow-poll 1926
country - Certificate Request Configuration mode 915
create - Certificate Request Configuration mode 916
create diskette 562
create recovery 564
create safe-mode-config 565
critical-interface-group 1584
crl 918
crl optimize 921
crl optional 922
crl retrieval 676
crl search-base host port attribute 923
crl search-base host port bind-dn 925
crl search-base host port enable 928
crl search-base host port object-class 930
crl search-base host port password 932
crl search-base host port ssl-enable 934
crl update 936
crypto ca allow 937
crypto ca configure 919, 939
crypto ca identity 940
crypto exp 188
crypto import 941
crypto password 942
crypto server configure 943
crypto server request 945
crypto trusted 946

D

data-collection-interval 189
dead-interval 322
debug atm 1337
debug dhcp 841
debug interface fastethernet pppoe 1222
default 323
default language 567

default-group 947
default-information originate 2018
delete 105
demand 677, 1538
demand add 1539
demand delay 1540
demand enable 1541
description - ATM interface 1339
description - ATM subinterface 1340
description - DHCP 843
description - Ethernet interface 1091
description - frame relay subinterface 1487
description - PPP 1378
description (802.1Q VLAN subinterface) 1121
destination-address 1790
df-bit 325
dial 1536
dial-prefix-string 1258
diffserv-marking 1792
dir 71
direction - filter rule 327
direction - packet capture 1757
disable - IPX 1625
disable - Privileged EXEC mode 106
display-banner 328
distribute-list - OSPF 1607
distribute-list - RIP 1567
dlci 1489
dlsw 1898
dlsw clear circuit 1875
dlsw debug_level 1986
dlsw ips-trace enable 1988
dlsw local-peer 1878, 1878
dlsw local-peer backlevel-flowcontrol 1879
dlsw local-peer enable 1881
dlsw local-peer mac-translation 1883, 1883
dlsw local-peer unconfigured-peer enable 1884
dlsw mac-translation 1885
dlsw remote-peer 1886
dlsw remote-peer circuit-inactivity 1890
dlsw remote-peer cost 1891
dlsw remote-peer enable 1892
dlsw remote-peer receive-initial-pacing 1893
dlsw remote-peer rfc1795 1895
dlsw timer circuit-ack-timeout 1896
dlsw timer explorer-delay 1897
dlsw timer explorer-timeout 1898
dlsw timer explorer-wait-timeout 1899
dlsw timer idle-timeout 1900
dlsw timer tcp-connect-retry 1901
dlsw timer test-timeout 1902
dns-proxy enable 568
domain add 530
dot1q enable 1122
dot1q interface untag egress 1124
dot1q interface untag ingress 1125
dot1q interface vlan-id 1127
dscp-values 1794
dsl operating-mode 1342
duplex 1092

E

enable 190, 1927
enable - IPX 1626
enable - Privileged EXEC mode 73
enable password 190
enable-ping 190
encapsulation (ATM subinterface) 1344
encapsulation (frame relay interface) 1490
encapsulation (frame relay subinterface) 1492

encapsulation (PPP interface) 1380
encapsulation dot1q 1129
encapsulation sdlc 1928
encryption 331
encryption ike 333
enrollment url 948
erase config-file 569
event-log size 191
exception backup 571
excess action 336
excess rate 337
excluded-address 844
exit 1542
exit - any mode or telnet 74
exit - current mode 339
exit - global configuration mode 193
exit - Privileged EXEC mode 107
export bo-static-metric 340
export default-metric 341
export ospf-metric 342
export static-metric 343
external-metric 1609

F

filter - 802.1q subinterface 1130
filter - ATM interface 1346
filter - interface 1094
filter - packet capture 1762
filter - PPP interface 1381
filter - tunnel 490
filter add 346
filter rule add 348
filters (Group Connectivity Configuration 344
fips 679
firewall 988, 994
firewall alg 990, 991
firewall anti-spoof 993
firewall cone-nat 994
firewall connection number 995
firewall hairpinning 997
firewall logging 998
firewall scan-detection 1001
firewall tunnel-filter 1003
firewall tunnel-management-filter 1004
firewall user-authentication 680
forced-logoff (group connectivity and branch office group connectivity) 350, 385
forced-logoff (Privileged EXEC) 108
fragment 1494
frame-relay bc 1495
frame-relay be 1496
frame-relay cir 1498
frame-relay connection-type 1499
frame-relay debug 1501
frame-relay lmi-n391dte 1503
frame-relay lmi-t391dte 1504
frame-relay lmi-type 1506
frame-relay subinterface 1507
framing 1468
ftp-coredump 575
ftp-coredump enable 577
ftp-server enable 682
ftp-server port 195, 196, 198

G

group - branch office connection 491
group - user account group 353
group (Global Configuration Command) 351
grouppoll 1930

H

hardware-address 847
hello-interval 355
help - EXEC mode 75
help - global configuration mode 199
help - Privileged EXEC mode 110
host 848
hostname - DNS name for gateway 200
hostname - system host 578
hours name 1549
http enable 683
http port 203, 206
https 206, 684
https private port 206

I

identification enable 686
idle-timeout - admin session 579
idle-timeout - connection 356
import default-route 357
included-address 850
initial-contact enable 358
interface 1511, 1546
interface - PPP 1383
interface - PPPoE 1223
interface atm 1348
interface bri 1292
interface bri enable 1293, 1295
interface dial 1260
interface dial enable 1261
interface fastethernet 1095
interface gigabitethernet 1097
interface group 1586
interface-group 1548
interleave 1510
inverse-arp 1513
invert data 1469
ip address - current interface 1160
ip address - DNS on private network 360
ip address - management address 581
ip address (802.1Q VLAN) 1132, 1138
ip address dhcp 1134
ip address type 1136
ip address-pool - enable for dial-in and PPP 361
ip address-pool - source 542
ip address-src 362
ip as-path access-list 2021
ip community-list 2024
ip default-network 1726
ip default-route-preference 1727
ip dhcp proxy-server blackout-interval override 545
ip dhcp server pool 851
ip domain-name - DNS domain 582
ip domain-name - IPsec tunnel 364
ip forward-protocol dhcp-relay 1659, 1661
ip helper-address 1662
ip http server 208
ip load-sharing 1651
ip local 1514
ip local - ATM subinterface 1349
ip local address-type - ATM subinterface 1352
ip multicast-relay boundary 1161
ip name-server 583
ip ospf - frame relay subinterface 1516
ip ospf - interface 1163
ip ospf (802.1Q VLAN) 1138
ip ospf authentication-key 1165
ip ospf cost 1166
ip ospf dead-interval 1168

ip ospf hello-interval 1169
ip ospf message-digest-key 1171
ip ospf network 1172
ip ospf poll-interval 1174
ip ospf priority 1175
ip ospf retransmit-interval 1177
ip ospf transmit-delay 1178
ip radius source-interface 687
ip remote 1518
ip remote - ATM subinterface 1353
ip remote address-type - ATM subinterface 1355
ip rip - frame relay subinterface 1519
ip rip - interface 1180
ip rip (802.1Q VLAN) 1140
ip rip authentication mode 1181
ip rip cost 1183
ip rip export-bo-static-metric 1186
ip rip export-default-metric 1187
ip rip export-ospf-metric 1189
ip rip export-static-metric 1190
ip rip import-default 1192
ip rip poison-reverse 1194
ip rip receive version 1195
ip rip send version 1197
ip route 1729
ip vrrp 1141, 1198
ip vrrp backup 1142, 1200
ip vrrp backup disable 1145, 1201
ip vrrp backup enable 1144, 1203
ip vrrp master 1146, 1204
ipsec authentication - group mode 688
ipsec authentication - IPsec tunnel 493
ipsec encryption 689
ipsec encryption ike 691
ipsec fail-over 693
ipsec issuer-ca - branch office 494
ipsec issuer-ca - IPsec 365
ipsec load-balance 694
ipsec nat-traversal 696
ipsec nat-traversal port 698
ipsec nat-traversal-bo 697
ipsec relative-dn 496
ipsec server-ca 498
ipsec server-ca (User Configuration) 366
ipsec subject-alt-name - branch office connection 499
ipsec subject-alt-name - groups 368
ipsec subject-dn - branch office connection 500
ipsec subject-dn - groups 369
ipsec uid (User Configuration) 370
ipsec uid pwchange enable 372
ipsec-transport 373
ipx 374
ipx interface 1630
ipx public-network-address 1628
isakmp-retransmission interval 375
isakmp-retransmission max-attempts 377
isdn auto-answer 1296
isdn auto-spid-detection enable 1298
isdn auto-switch-detect 1299
isdn bandwidth-monitor enable 1301
isdn country-code 1303
isdn manual-tei 1305
isdn microcode 1306
isdn not-end-to-end 1308
isdn phone 1309
isdn public 1311
isdn spid1 1312
isdn spid2 1314
isdn switch-type 1316

K

keepalive interval 378
keepalive ondemand-conn 379
key - Certificate Request Configuration mode 950
kill 111

L

l2f authentication 699
l2f nas-uid 701
l2f uid (User Configuration) 380
l2tp authentication - branch office connection 502
l2tp authentication - l2tp tunnel 702
l2tp concentrator 503
l2tp ipsec-data-protection 504
l2tp lac-uid 704
l2tp stateless-mode 506
l2tp uid (User Configuration) 382
ldap 209
ldap-server external 818
ldap-server external host 820
ldap-server internal 823
ldap-server source 826
lease 853
length 1765
license 584
line-buildout 1471
linecode 1472
line-encoding 1931
line-power-detection enable 1318
line-speed 1932
llc2 ack-delay-time 1904
llc2 busy-time 1906
llc2 enable 1907
llc2 idle-time 1909
llc2 lantype 1910
llc2 lpf-time 1913
llc2 max-received-window 1911
llc2 max-retry 1912
llc2 rej-time 1914
llc2 t2timeout 1916
lmac lsap 1933
load 211
local-endpoint 507
local-gateway 508
locality - Certificate Request Configuration mode 951
local-network 510
log-file-lifetime 212
logging 215, 470, 472, 586
logging capture-filter entity add 456, 456
logging capture-filter entity remove 458, 458
logging capture-filter severity add 461, 461
logging capture-filter severity remove 463, 463
logging display-filter entity add 465, 465
logging display-filter entity remove 467, 467
logging display-filter severity add 470, 470
logging display-filter severity remove 472, 472
logging history 213
logging save-log 215
login max-attempts 383
logins 384
logout 217
ls 76

M

mac-crc-included 1357
mac-pause 1099
mac-pause threshold 1100
mac-pause ticks 1101
map-class frame-relay 1521

match 2028
match as-path 2026
match community 2028
match ip address 2030
maximum-paths 1653
menu-access-level 1263
microcode 1264
microcode reload 1266
microcode reload bri 1320
mkdir 113
mode 1267
modem-command-string 1269
modem-initialization-string 1271
modem-termination-string 1272
more 114
move-rule - filter rule 387
move-rule - MF class 1795
mtu (Branch Office Connection Configuration) 511
mtu (Interface Configuration) 1102
mtu enable 513
multicast-boundary interface 1668
multicast-relay congestion-threshold 1670
multicast-relay enable 1672
multiple 2032
multiple-paths 2032

N

nailed-up 388
name - Certificate Request Configuration mode 952
nat 514
nat-traversal 389, 1006
neighbor 2033, 2034, 2037, 2039, 2042, 2043, 2045, 2048, 2051, 2056, 2058, 2059, 2061
neighbor advertisement-interval 2034
neighbor allow-as-in 2036
neighbor default-originate 2037
neighbor distribute-list 2039
neighbor ebgp-multihop 2041
neighbor enable 2042
neighbor filter-list 2043
neighbor loop-detection 2047
neighbor next-hop-self 2045
neighbor password 2048
neighbor remote-as 2050
neighbor retry-interval 2051
neighbor route-map 2053
neighbor route-reflector-client 2055
neighbor send-community 2056
neighbor timers 2061
neighbor update-source 2059
neighbor weight 2062
netobj 1007
netobj-group 1010
network 2065
network - IPX interface 1632
network - OSPF 1610
network - RIP 1570
network (VRRP) 1588
network add 532
next-server 856
no bo-group 391
no crypto ca enroll 953
no crypto server certificate renew 954
no group 392
no uid lockout 400
nortel-client action 394
nortel-client filter 396
nortel-client message 397
nortel-client version 399

ntp 588
ntp authentication-key 589
ntp broadcast server 590
ntp multicast server 591
ntp server 592

O

openSSL enable 955
option 857
option client-identifier 860
option default-router 861
option dns-server 863
option domain-name 864
option netbios-name-server 865
option netbios-node-type 867
organization - Certificate Request Configuration mode 958
org-unit - Certificate Request Configuration mode 957
ospf maximum-paths 1654, 1655

P

password - management 401
password-storage 403
PCAP 1741
performance-report-message 1474
persistent 1768
pfs 404
phone 1274
ping 1549
ping - general use 78
ping-address 217
ping-interval 219
poison-reverse 405
policy nat 1012
policy nat enable 1014
policy nat interface 1015
policy object 1017
policy security 1019
pollframe 1934
port 406
ppp authentication chap 1384
ppp authentication pap 1386
ppp ip default-route (ATM subinterface) 1388
ppp ip local (ATM subinterfaces) 1390
ppp ip local (dial interfaces) 1392
ppp ip local (serial interfaces) 1394
ppp ip ospf 1396
ppp ip primary-dns-obtain enable 1398
ppp ip remote (ATM subinterfaces) 1399
ppp ip remote (dial interfaces) 1401
ppp ip remote (serial interfaces) 1403
ppp ip rip 1405
ppp ip secondary-dns-obtain enable 1407
ppp ipcp vj-connect-id-compression-negotiation 1408
ppp ipcp vj-max-slots 1410
ppp ipcp vj-negotiation 1412
ppp lcp address-control-field-compression 1413
ppp lcp echo-fault-threshold 1415
ppp lcp echo-interval 1417
ppp lcp protocol-field-compression 1418
ppp lcp-ncp interface-debug 1420
ppp local authentication chap 1422
ppp local authentication pap 1424
ppp local password 1426
ppp local username 1428
ppp multilink high-threshold-duration 1430
ppp multilink high-threshold-percent 1431
ppp multilink incoming enable 1433
ppp multilink low-minimum-duration 1435

ppp multilink low-threshold-duration 1437
ppp multilink low-threshold-percent 1439
ppp multilink minimum-links 1440
ppp multilink outgoing enable 1442
ppp password 1444
ppp public 1446
ppp remote authentication pap 1447
ppp remote password 1449
ppp remote username 1451
ppp username 1453
ppp-links max-number 407
pppoe admin-state enable 1224
pppoe cost 1226
pppoe enable 1228
pppoe idle-timeout 1229
pppoe ip local 1231
pppoe ip tcp adjust-mss enable 1233
pppoe on-demand enable 1234
pppoe ppp authentication 1236
pppoe ppp ipcp
vj-connect-id-compression-negotiation 1238
pppoe ppp ipcp vj-max-slots 1239
pppoe ppp ipcp vj-negotiation 1241
pppoe ppp lcp echo-fault-threshold 1242
pppoe ppp lcp echo-interval 1243
pppoe ppp lcp protocol-field-compression 1245
pppoe ppp username 1246
pppoe service-name 1248
pptp authentication 515, 706
pptp uid (User Configuration) 409
priority 410, 1524, 1551
priority call-admission 411
priority forwarding 413
promiscuous 1770
prompt 220
protocol 1797
proxy ldap-server pwd-lifetime 831
proxy ldap-server pwd-timestamp-attr 830
proxy ldap-server server-type 829
proxy-xid 1935
public - ATM subinterface 1359
public - frame relay subinterface 1526
public - interface 1104
publications
hard copy 49
pwd 81

Q

qos admission-control 1799
qos bandwidth-management 1801
qos bandwidth-rates 1802
qos egress-dscp-map enable 1804
qos egress-queuing-mode 1806
qos egress-traffic-conditioning 1808
qos ingress-dscp-map enable 1810
qos ingress-traffic-conditioning 1812
qos mf-class - Global Configuration 1817
qos mf-class - Interface Configuration 1815
qos mf-class add 1818
qos mf-class enable 1820
qos mf-class rule 1821
qos mf-class rule add 1823
qos non-tunnel-traffic-ratio 1824
qos over-subscription-ratio 1827
qos shaping 1829
qos shaping-state enable 1831
qos statistics reset 1832
qos traffic-conditioning enable 1834

R

radius service 707
radius-accounting private enable 709
radius-accounting public enable 710
radius-client 711
radius-client host 713
radius-client port 714
radius-server 757
radius-server authentication 758
radius-server domain-delimiter 761
radius-server group 762
radius-server group domain-delimiter 766
radius-server group enable 764
radius-server group group-level enable 767
radius-server group maximum-transmit-attempts 769
radius-server group response-timeout-interval 770
radius-server group suffix-remove enable 772
radius-server interface 775
radius-server key 776
radius-server suffix-remove 779
radius-server suppress-service-type enable 780
radius-server timeout 782
receive version 414
recover reference-number 961
recvwindow 1936
redial 1553
redistribute 2066
redistribute - RIP 1571
redistribute - routes 1612
reformat diskette 594
rekey data-count 415
rekey timeout 417
reload 117
reload at 120
reload cancel 123
reload in 125
reload no-sessions 128
remote-endpoint 517
remote-endpoint host 518
remoteip 1771
remote-network 520, 1555
remove-rule 418, 1836
rename 131
renew 962
reset - ISDN 1322
reset - modem and serial port 1276
reset ssl-vpn 721
restart ssl-vpn 723
restrict 221
retransmit-interval 419
retrieve backup 596
retrieve software 132
revoke now 963
rip maximum-paths 1655
rmac rsap 1937
rmdir 134
route-map 2068
route-policy enable/disable 1739
router bgp 2071
router car 1646
router ospf 1615
router rip 1573
router static 1731
router vrrp 1589, 1590
route-reflector enable 2070
router-id 1613
route-unreachable 1557
routing 521
rsvp 421

rsvp token-bucket 422
rule (Firewall Policy Configuration) 1021, 1147
rule (NAT Policy Configuration) 1025
rule description (NAT Policy Configuration) 1029
rule service (NAT Policy Configuration) 1030
rule status (NAT Policy Configuration) 1032

S

safe-mode duration 223
safe-mode enable 225
save current config-file 598
scheduler manageability 599
sdlc activation-sequence 1938
sdlc counter idle-time 1940
sdlc counter non-productive 1941
sdlc counter write-port 1942
sdlc debug 1944
sdlc interframe-fill enable 1945
sdlc link-station polladdress 1946
sdlc max-received-window 1947
sdlc polladdress 1948
sdlc primary-full-duplex 1949
sdlc role 1950
sdlc secondary-full-duplex 1952
sdlc send-rej 1953
sdlc timer idle-line 1954
sdlc timer non-productive 1955
sdlc timer write-port 1956
send version 423
sendwindow 1958
serial-port baud-rate 1277
serial-port mode 1279
server 425
server-name 868
service 1034
service dhcp enable - Ethernet interface 1106
service dhcp enable - global 870
service dhcp restart 871
service-group 1038
service-NAT Policy Configuration 1037
set 2075
set as-path 2073
set authorization-code 964
set ca-default-group 965
set community 2075
set ip next-hop 2078
set issuer 966
set issuer-dn 967
set key-size 968
set local-preference 2079
set metric 2080
set origin 2081
set port 969
set reference-number 971
set subject-dn 972
set weight 2083
show 480
show (ipsec|l2f|l2tp|pptp) 717
show access-hours 534
show accounting radius-server 783
show admin settings 601
show arp 135
show authentication ldap-server 832
show authentication radius-server 784
show bo-conn 523
show bo-group 427
show capture 1773
show client-policy 535
show clip 1216
show clip services 1218

show clock 602
show compress-files 603
show config-files 605
show controller 1476
show controller 56k 1998
show critical-interface 1591
show crypto 231
show crypto ca certificates 973
show crypto certificates 976
show crypto enrollment 977
show crypto password 978
show crypto server certificate renew 980
show current-config-file 606
show data-collection-interval 136
show demand 1558
show dhcp-relay config 1663
show dhcp-relay config interface 1664
show dhcp-relay config statistics 1665
show dlsw capabilities 1971
show dlsw circuits 1973
show dlsw directory 1975
show dlsw mac-table 1977
show dlsw peers 1978
show dlsw port 1981
show dlsw sdlc 1984
show domains 536
show dot1q 1151
show dot1q statistics 1153
show dsl interface atm 1360
show ecmp 1657
show event-log size 137
show exception backup 607
show file systems 82
show filters 428
show firewall 1040
show firewall user-authentication 715
show flash contents 83
show frame-relay lmi 1527
show frame-relay pvc 1529
show ftp-coredump 609
show groups 430
show health 139
show hosts 610
show interface atm 1362
show interface atm statistics 1364
show interface bri 1323
show interface bri statistics 1326
show interface dial 1281
show interface dial statistics 1283
show interface fastethernet 1107
show interface gigabitethernet 1110
show interface groups 1592
show interface pppoe 1249
show interface serial 1455
show interface serial ppp 1456
show interface serial statistics 1458
show interfaces 1044
show ip as-path access-list 2084, 2102
show ip bgp 2085
show ip bgp community 2088
show ip bgp neighbors 2089
show ip bgp networks 2094
show ip bgp redistribute-routes 2096
show ip bgp redistribution 2095
show ip bgp regexp 2098
show ip bgp summary 2098
show ip community-list 2102
show ip default-route-preference 1732
show ip dhcp proxy-server 545
show ip dhcp server 872

show ip int 1205
show ip local pool 547
show ip name-server 611
show ip ospf 1616
show ip ospf border-routers 1618
show ip ospf database 1619
show ip ospf interface 1620
show ip ospf neighbor 1621
show ip ospf virtual-links 1623
show ip rip 1574
show ip rip database 1575
show ip rip interface 1576
show ip rip redistribution 1578
show ip route 1638
show ip route-map 2103
show ip static 1734
show ip vrrp 1594
show ldap-server 834
show license 613
show log-file-lifetime 140
show logging capture-filter 474, 474
show logging capture-filter entity 478, 478
show logging capture-filter entity all 475, 475
show logging capture-filter severity 481, 481
show logging capture-filter severity all 480, 480
show logging config 142
show logging events 145
show logging history 150
show logging security 151
show logging syslog 154
show microcode 1285, 1328
show multicast-relay 1673
show multicast-relay status interfaces 1675
show multicast-relay status statistics 1676
show netobjs 1046
show networks 538
show ntp 614
show policy nat 1047
show policy security 1049
show qos admission-control 1837
show qos bandwidth-management 1838
show qos bandwidth-rates 1840
show qos interfaces 1841
show qos mf-class 1843
show qos statistics 1845
show radius-server group 786
show reload 85
show router car 1647
show rules (Firewall Policy Configuration) 1051
show rules (NAT Policy Configuration) 1053
show rules (QoS) 1849
show running-config 263
show safe-mode 157
show scheduler 616
show serial-port 158
show services 86
show services - Firewall and NAT 1055
show services - gateway 86
show sessions 88
show snmp get-host 878
show snmp host 879
show snmp identity 880
show snmp mib 881
show snmp-traps trap-groups 883
show snmp-traps trap-hosts 886
show software version 159
show ssl cipher 724
show ssl option des-cbc-padding 727
show ssl server-cert 726
show ssl-vpn 728

show status statistics admin 617
show status statistics hardware 620
show status statistics interfaces 624
show status statistics network 627
show status statistics resources 634
show status statistics routing 640
show status statistics security 642
show status statistics system 645
show syslog-host 652
show system accelerator 653
show system accelerator statistics 656
show system forwarding 160
show tunnel-guard policy 1060, 1061
show tunnel-guard server-port 1062
show users 432
show version 90
shutdown - ATM interface 1367
shutdown - ATM subinterface 1368
shutdown - current interface 1111
shutdown - dial and serial port 1286
shutdown - ISDN 1330
snmp-ifspeed 888
snmp-server contact 889
snmp-server enable traps attack 890
snmp-server enable traps hardware 891
snmp-server enable traps ietf 896
snmp-server enable traps server 898
snmp-server enable traps service 900
snmp-server get-host 901
snmp-server host 903
snmp-server location 904
snmp-server management 905
snmp-server mib 906
snmp-server name 908
snmp-server port 233, 235
source-address 1850
speed 1113
split 433, 435
split inverse-tunnel-network network-name 433
split tunneling 435
split tunnel-networks 436
split-dns enable 659
ssl cipher 729
ssl encryption 836
ssl https-port 731
ssl option des-cbc-padding enable 733
ssl server-cert 735
ssl-vpn csfw-implied-rule enable 739
ssl-vpn enable 736
ssl-vpn init 737
ssl-vpn paste-config 740
ssl-vpn-cli 742
start 1959
state 524
state - Certificate Request Configuration mode 981
static-ipaddress (Group Connectivity Configuration) 438
static-ipaddress (User Configuration) 439
static-subnet-mask 440
stop 1961
subinterface (802.1Q VLAN) 1154
subinterface (ATM) 1370
subinterface enable (802.1Q VLAN) 1156
subject-dn 982
synchronization 2104
system accelerator auto-recovery enable 660
system accelerator enable 662
system forwarding gratuitous-arp enable 237
system forwarding nexthop-forward enable 239
system forwarding proxy-arp branch-office-tunnels enable 240

system forwarding proxy-arp physical-interfaces enable 241
system forwarding tunnel-to-tunnel-traffic BO-to-BO enable 243
system forwarding tunnel-to-tunnel-traffic EU-to-BO enable 245
system forwarding tunnel-to-tunnel-traffic EU-to-EU enable 246
system-log-to-file enable 248

T

tcp-mss 1114
tcp-mss enable 1116
tcp-udp-destination-port 1852
tcp-udp-source-port 1855
technical publications 49
telnet enable 718
telnet port 249, 251
terminal paging 91
text conventions 45
threshold 1649
timeout 1560
timer disconnect 1962
timer fast-contact 1963
timer fast-poll 1964
timer no-response 1965
timer rnr-limit 1966
timer slow-contact 1968
timer slow-poll 1969
timer turn-around 1970
timers basic 1579
timers bgp 2105
timeslot 1478
trace ip 92
traffic-shape rate 1532
transmit-data-monitor 2000
transmit-delay 442
trigger 1561
trigger - Demand 1561
trigger - packet capture 1777
trigger traffic 1561
tunnel protocol 719
tunnel-guard agent-query-timeout 1065, 1067, 1068
tunnel-guard enable 1069
tunnel-guard fail-action 1071
tunnel-guard recheck-interval 1074
tunnel-guard server-port 1083
tunnel-type 525
tx-ringsize 1480, 1989
type 1779

U

use address 443
use destination_address 1857
use dest-port 444
use diffserv_marking 1858
use dscp 1860
use nexthop-addr 446
use protocol - for current filter rule 447
use protocol - for QoS rule 1862
use source_address 1864
use src-port 449
use tcp_udp_destination_port 1866
use tcp_udp_source_port 1868
use tunnel-guard filter 1085
use tunnel-guard policy 1087
user add 450
userid 1782

V

validate 252
vendor-id 452
verify system 663
virtual-circuit (ATM) 1371

W

wait 1564
who 94
wins address 453
wrapping 1784