Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers

Release 6.3
03-300431
Issue 10
August 2015

© 2015 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface

with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya and Avaya Aura® are registered trademarks of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 21
Purpose 21
Intended audience 21
Document changes since last issue 21
Safety labels and security alert labels 22
SAT Command syntax 22
Contention between simultaneous commands 23
Busyout and release commands 24
Alarm and error categories 24
Common SAT command parameters 25
Common output field descriptions 26
Error messages 27
Common Error Codes 28
Related resources 30
Documentation 30
Training 30
Viewing Avaya Mentor videos 31
Support 31
Warranty 31
Chapter 2: Maintenance command descriptions 32
aar analysis 32
list aar analysis 32
aar route-chosen 33
list aar route-chosen 33
access-endpoint 34
busyout access-endpoint 34
release access-endpoint 35
status access-endpoint 35
test access-endpoint 36
administered-connection 37
disable administered-connection 37
enable administered-connection 37
status administered-connection 38
aesvcs 38
reset aesvcs link 38
status aesvcs cti-link 38
status aesvcs interface 39
status aesvcs link 40
test aesvcs-server 40
alarms 41

display alarms ... 41
test alarms ... 44
analog-testcall ... 46
test analog-testcall ... 46
announcement ... 47
erase announcement ... 47
list announcement ... 47
announcement-board ... 48
disable announcement-board ... 48
enable announcement-board ... 48
arp ... 49
netstat arp ... 49
ars analysis ... 50
list ars analysis ... 50
ars route-chosen ... 51
list ars route-chosen ... 51
attendant ... 52
status attendant ... 52
audio-group ... 53
list audio-group ... 53
list usage audio-group ... 54
audits ... 54
clear audits ... 54
status audits ... 54
bcms ... 61
monitor bcms ... 61
board ... 65
busyout board ... 65
release board ... 65
reset board ... 66
test board ... 66
boot-image ... 67
get boot-image ... 67
set boot-image ... 68
bp ... 68
change bp ... 68
bri-port ... 69
status bri-port ... 69
bulletin-board ... 76
display bulletin-board ... 76
cabinet ... 76
add cabinet ... 76
change cabinet ... 78

display cabinet..... 78
list cabinet..... 78
status cabinet..... 79
calltype route-chosen..... 81
list calltype route-chosen..... 81
campon-busyout..... 83
campon-busyout..... 83
capacity..... 83
display capacity..... 83
carrier..... 93
recycle carrier..... 93
cdr-link..... 94
busyout cdr-link..... 94
release cdr-link..... 95
status cdr-link..... 95
test cdr-link..... 97
circuit-packs..... 97
change circuit-packs..... 97
display circuit-packs..... 99
clan-all..... 99
status clan-all..... 99
clan-ip..... 100
status clan-ip..... 100
clan-port..... 101
status clan-port..... 101
cleared-alarm-notif..... 101
status cleared-alarm-notif..... 101
communication-interface links..... 102
change communication-interface links..... 102
display communication-interface links..... 102
communication-interface processor-channels..... 102
change communication-interface processor-channels..... 102
display communication-interface processor-channels..... 104
conference..... 104
status conference..... 104
configuration..... 132
list configuration..... 132
list configuration media-gateway..... 134
list configuration power-supply..... 135
list configuration software-versions..... 135
list configuration stations..... 136
craft2..... 137
enable craft2..... 137

disable craft2 137
cti-link 137
busyout cti-link 137
change cti-link 138
list cti-link 140
list usage cti-link 140
release cti-link 141
test cti-link 141
customer-alarm 142
test customer-alarm 142
data-module 142
busyout data-module 142
release data-module 143
status data-module 143
test data-module 144
directory 145
list directory 145
disabled-MOs 145
list disabled-MOs 145
disabled-tests 146
display disabled-tests 146
ds1-facility 146
busyout ds1-facility 146
test ds1-facility 147
ds1-loop 148
test ds1-loop 148
eda-external-device-alrm 149
list eda-external-device-alrm 149
test eda-external-device-alrm 149
emergency 150
set emergency 150
environment 151
status environment 151
test environment 153
errors 154
clear errors 154
display errors 155
ess 159
disable ess 159
enable ess 160
status ess clusters 161
status ess port-networks 163
ethernet-options 166

get ethernet-options..... 166
list ethernet-options..... 167
set ethernet-options..... 167
events..... 168
display events..... 168
extended-user-profile..... 169
change extended-user-profile..... 169
display extended-user-profile..... 170
extension-type..... 170
list extension-type..... 170
failed-ip-network-region..... 171
display failed-ip-network-region..... 171
test failed-ip-network-region..... 171
fiber-link..... 172
add fiber-link..... 172
busyout fiber-link..... 173
change fiber-link..... 174
display fiber-link..... 176
list fiber-link..... 176
reset fiber-link..... 177
test fiber-link..... 178
file..... 179
remove file..... 179
filexfer..... 179
disable filexfer..... 179
enable filexfer..... 180
firmware-counters..... 180
clear firmware-counters..... 180
firmware download..... 181
change firmware download..... 181
disable firmware download..... 183
display firmware download..... 183
status firmware download..... 184
test firmware download..... 185
firmware station-download..... 185
change firmware station-download..... 185
disable firmware station-download..... 186
display firmware station-download..... 186
status firmware station-download..... 186
test firmware station-download..... 188
hardware-group..... 189
cancel hardware-group..... 189
resume hardware-group..... 189

status hardware-group ... 190
test hardware-group ... 191
health ... 193
monitor health ... 193
status health ... 194
history ... 196
list history ... 196
notify history ... 198
initcauses ... 198
display initcauses ... 198
integ-annc-board ... 200
list usage integ-annc-board ... 200
integ-annc-brd-loc ... 200
change integ-annc-brd-loc ... 200
ip-board ... 201
status ip-board ... 201
ip-codec-set ... 202
change ip-codec-set ... 202
ip-interface ... 209
change ip-interface ... 209
list ip-interface ... 210
ip-network-region ... 212
change ip-network-region ... 212
list ip-network-region ... 212
status ip-network-region ... 212
duplicate ip-network-region ... 213
ip-route ... 214
list ip-route ... 214
netstat ip-route ... 215
refresh ip-route ... 216
ipserver-interface ... 216
add ipserver-interface ... 216
busyout ipserver-interface ... 217
change ipserver-interface ... 217
display ipserver-interface ... 221
get forced-takeover ipserver-interface ... 222
list ipserver-interface ... 223
list measurements ipserver-interface ... 223
release ipserver-interface ... 224
remove ipserver-interface ... 225
reset ipserver-interface ... 225
set ipserver-interface ... 226
test ipserver-interface ... 226

ip-stations ... 226
reset ip-stations ... 226
ip-synchronization ... 228
status ip-synchronization ... 228
isdnpri-testcall ... 230
clear isdnpri-testcall ... 230
list isdnpri-testcall ... 231
status isdnpri-testcall ... 231
test isdnpri-testcall ... 233
journal-link ... 234
status journal-link ... 234
journal-printer ... 235
busyout journal-printer ... 235
release journal-printer ... 235
test journal-printer ... 236
led ... 236
test led ... 236
license ... 237
test license ... 237
link ... 238
busyout link ... 238
clear link ... 238
status link ... 238
test link ... 241
locations ... 241
list locations ... 241
logging-levels ... 242
change logging-levels ... 242
display logging-levels ... 242
login-id ... 243
reset login-id ... 243
logins ... 243
status logins ... 243
maintenance ... 244
reset maintenance ... 244
test maintenance ... 244
marked-ports ... 245
list marked-ports ... 245
mct-history ... 245
list mct-history ... 245
measurements ... 247
list measurements aca ... 247
list measurements clan ethernet ... 247

list measurements clan ppp 248
list measurements clan sockets 249
list measurements ds1 250
list measurements ip codec 252
list measurements ip dsp-resource 253
list measurements ip signaling-groups 265
list measurements ip voice-stats 266
list measurements tone-receiver 275
media-gateway 278
add media-gateway 278
change media-gateway 281
display media-gateway 282
list media-gateway 282
reset media-gateway 284
status media-gateway 284
test media-gateway 286
media-processor 286
set media-processor 286
status media-processor 288
status media-processor board 289
meet-me-vdn 291
reset meet-me-vdn 291
mg-announcements 291
status mg-announcements 291
mg-return 292
enable mg-return 292
mis 293
busyout mis 293
release mis 293
modem-pool 294
release modem-pool 294
test modem-pool 294
moh-analog-group 295
list moh-analog-group 295
monitored-station 296
list monitored-station 296
mst 296
clear mst 296
disable mst 296
display mst 297
list mst 297
multimedia 299
list multimedia 299

night-service 300
list night-service attendant 300
list night-service hunt-group 300
list night-service trunk-group 300
node-names 301
display node-names 301
nr-registration 302
disable nr-registration 302
enable nr-registration 303
status nr-registration 303
options 306
set options 306
off-pbx-telephone 308
status off-pbx-telephone station 308
list off-pbx-telephone station-mapping 309
packet-interface 310
reset packet-interface 310
status packet-interface 311
test packet-interface 312
periodic-scheduled 312
status periodic-scheduled 312
pin 314
change pin 314
reset pin 314
ping 315
ping 315
pkt 317
clear pkt 317
test pkt 318
pms-down 318
list pms-down 318
pms-link 319
busyout pms-link 319
release pms-link 320
status pms-link 320
test pms-link 321
pnc 322
set pnc 322
status pnc 322
pnc interchange 325
reset pnc interchange 325
port 326
busyout port 326

clear port ... 327
display port ... 327
mark port ... 328
release port ... 328
test port ... 329
port-network ... 329
reset port-network ... 329
status port-network ... 330
power-shutdown ... 334
get power-shutdown ... 334
pri-endpoint ... 334
busyout pri-endpoint ... 334
release pri-endpoint ... 335
status pri-endpoint ... 335
test pri-endpoint ... 336
processor-ip-interface ... 337
busyout processor-ip-interface ... 337
release processor-ip-interface ... 337
status processor-ip-interface ... 337
profile-base ... 338
display profile-base ... 338
psa ... 338
status psa ... 338
public-unknown-numbering ... 339
change public-unknown-numbering ... 339
display public-unknown-numbering ... 340
list public-unknown-numbering ... 340
registered-ip-stations ... 342
list registered-ip-stations ... 342
remote-access ... 343
status remote-access ... 343
remote-office ... 344
add remote-office ... 344
change remote-office ... 345
display remote-office ... 345
list remote-office ... 345
remove remote-office ... 346
status remote-office ... 346
route-table ... 346
refresh route-table ... 346
security-violations ... 347
monitor security-violations ... 347
session ... 349

enable session 349
set-data 349
list set-data 349
shell 350
go shell 350
signaling-group 351
display signaling-group 351
list signaling-group 353
set signaling-group 354
status signaling-group 354
test signaling-group 356
skill-status 357
list skill-status 357
socket-usage 358
monitor socket-usage 358
status socket-usage 358
sp-link 359
busyout sp-link 359
release sp-link 360
status sp-link 360
test sp-link 360
ssh-keys 361
reset ssh-keys 361
station 362
add station 362
busyout station 362
change station 362
list station 363
release station 363
status station 364
test station 375
survivable-processor 375
list survivable-processor 375
suspend-alm-orig 376
disable suspend-alm-orig 376
enable suspend-alm-orig 377
list suspend-alm-orig 378
switch-node 378
status switch-node 378
switch-node-clock 379
set switch-node-clock 379
synchronization 379
change synchronization 379

disable synchronization ... 380
display synchronization ... 381
enable synchronization ... 382
list synchronization ... 382
set synchronization ... 383
status synchronization ... 383
test synchronization ... 384
sys-link ... 385
list sys-link ... 385
status sys-link ... 386
test sys-link ... 387
system ... 388
monitor system ... 388
reset system ... 391
system-parameters duplication ... 394
change system-parameters duplication ... 394
display system-parameters duplication ... 395
system-parameters ip-options ... 396
change system-parameters ip-options ... 396
display system-parameters ip-options ... 396
system-parameters ipserver-interface ... 396
change system-parameters ipserver-interface ... 396
display system-parameters ipserver-interface ... 398
system-parameters maintenance ... 398
change system-parameters maintenance ... 398
display system-parameters maintenance ... 404
system-parameters port-networks ... 404
change system-parameters port-networks ... 404
tdm ... 405
busyout tdm ... 405
release tdm ... 405
set tdm ... 405
test tdm ... 406
terminal ... 407
erase terminal ... 407
test-number ... 408
disable test-number ... 408
enable test-number ... 408
test-schedule ... 408
display test-schedule ... 408
testcalls ... 410
list testcalls ... 410
tftp-server ... 413

change tftp-server 413
display tftp-server 413
time 413
display time 413
set time 414
tone-clock 415
set tone-clock 415
test tone-clock 415
trace 416
list trace media-gateway 416
list trace ras 417
list trace station 417
list trace tac 418
list trace vdn 418
list trace vector 419
trace-route 419
trace-route ip-address 419
traffic 421
monitor traffic 421
translation 422
save translation 422
trunk 423
busyout trunk 423
monitor trunk 424
release trunk 424
status trunk 425
test trunk 427
trunk-group 428
list trunk-group 428
tsc-administered 428
status tsc-administered 428
test tsc-administered 429
tti 430
status tti 430
tti-ip-stations 431
list tti-ip-stations 431
user-profile 431
change user-profile 431
display user-profile 432
duplicate user-profile 434
export user-profile 434
import user-profile 435
list user-profiles 436

remove user-profile 437
user-profile-by-category 437
add user-profile-by-category 437
change user-profile-by-category 438
display user-profile-by-category 438
val 438
reset val 438
val-ip 439
status val-ip 439
video-bridge 439
status video-bridge 439
Chapter 3: Linux bash commands 441
Introduction 441
acpfindvers 441
almcall 441
almclear 442
almdisplay 443
almenable 443
almnotif 444
almsnmpconf 444
almsummary 445
almsuppress 445
authtype 445
autosat 446
cmpasswd 446
cmuseradd 446
cmuserdel 447
cmusermod 447
corevector 448
custalmopt 449
defsat 449
dhelp 449
disp_dup_log 450
displaydenialevents 450
dkill 450
dsat 451
environment 451
fasttop 451
filesync 452
ftpserv 454
fwdlreason 454
hardware_info 455
listhistory 455

loaddisplang..... 456
loadpwd..... 456
locktrans..... 457
logclear..... 458
logecho..... 458
logfilter..... 458
loginreport..... 459
logv logc logw..... 460
modserv..... 462
mv_lastlog..... 463
mv_status..... 463
ping..... 463
pingall..... 464
productid..... 464
raid_status..... 465
restartcause..... 466
rm_download_files..... 467
rtrenice..... 468
sat..... 468
save_trans..... 468
server..... 468
setnic..... 469
start..... 470
statapp..... 470
statuslicense..... 471
stop..... 472
sudo..... 472
swversion..... 472
systat..... 473
testcustalm..... 474
testinads..... 474
testinadsport..... 474
testled..... 475
tlscertmanage..... 475
topsting..... 476
uname..... 477
unlocktrans..... 477
unused_login_audit..... 478
update_activate..... 478
update_deactivate..... 478
update_info..... 478
update_remove..... 479
update_show..... 479

update_unpack..... 480
userlock..... 480
vilog..... 481
webssl..... 481
wlog..... 481
xlnrecovery..... 482
Chapter 4: IPSI commands..... 483
IPSI commands..... 483
Command interpreter..... 483
IPSI Clock..... 483
IPSI/Network diagnostics..... 484
Query/display Server IP Addresses..... 484
Ethernet services port configuration commands..... 484
exit (or quit)..... 485
help (or ?)..... 485
ipsilogin..... 485
ipsisession..... 485
ipsiversion..... 486
loadipsi..... 486
loadstbyipsis..... 487
logout..... 488
reset..... 488
resetipsi..... 488
resetbyipsis..... 489
set control gateway..... 489
set control interface..... 490
set diffserv..... 490
set port duplex..... 490
set port flowcontrol..... 491
set port negotiation..... 491
set port speed..... 491
set services gateway..... 492
set services interface..... 492
set time slot occupancy notification..... 493
set vlan priority..... 493
set vlan tag..... 493
show arp..... 493
show control interface..... 494
show control stats..... 494
show firmware version..... 494
show host..... 494
show internet stats..... 494
show ip stats..... 495

show network stats..... 495
show port..... 495
show qos..... 496
show route..... 496
show route stats..... 496
show servers..... 496
show services interface..... 496
show services stats..... 497
show tcp stats..... 497
ssh-keygen..... 497
telnet..... 498
trace route..... 499
Appendix A..... 500
PCN and PSN notifications..... 500
PCN and PSN notifications..... 500
Viewing PCNs and PSNs..... 500
Signing up for PCNs and PSNs..... 501

Chapter 1: Introduction

Purpose

This document provides information regarding the Avaya Aura® Communication Manager commands that monitor, test, and maintain hardware components of an Avaya server or gateway system. The commands help the user to test, troubleshoot, and fix problems that could severely disrupt call processing.

Many commands can be run from the Communication Manager web interface. For more information on using the web interface, see *Administering Avaya Aura® Communication Manager* (03-300509) on the Avaya Support website, http://support.avaya.com.

System Access Terminal (SAT) commands apply to a number of servers and gateways and display different results depending on the configuration of the system. Some commands apply to certain servers and not others.

Intended audience

The information in this book is intended for use by Avaya technicians, provisioning specialists, business partners, and customers, specifically:

- Trained Avaya technicians
- A maintenance technician dispatched to a customer site in response to a trouble alarm or a user trouble report
- A maintenance technician located at a remote maintenance facility
- The customer's assigned maintenance technician

The technician is expected to have a working knowledge of telecommunications fundamentals and of the particular Avaya Server and Gateway to the extent that the procedures in this book can be performed, in most cases, without assistance.

Document changes since last issue

The following changes have been made to this document since the last issue:

- Added H.323 Stations via TLS to the display capacities field descriptions — Page 11 table of display capacity.

- Added Link Encryption Type and Mutual Authentication to the add media-gateway field descriptions table of add media-gateway.
- Updated monitor security-violations.
- Added Network region to the status station field descriptions, page 1 — General Status and Hospitality Status table of status station.
- Added Authentication Type to the status station field descriptions — IP Endpoints Data, page 7 of status station.

Safety labels and security alert labels

Observe all caution, warning, and danger statements to help prevent loss of service, equipment damage, personal injury, and security problems.

Caution:

A caution statement calls attention to a situation that can result in harm to software, loss of data, or an interruption in service.

Warning:

A warning statement calls attention to a situation that can result in harm to hardware or equipment.

Danger:

A danger statement calls attention to a situation that can result in harm to personnel.

Security alert:

A security alert calls attention to a situation that can increase the potential for unauthorized use of a telecommunications system.

SAT Command syntax

Each command consists of an action, an object upon which the action is performed, and required or optional qualifiers which modify the execution of the command. For example, in the command `test station extension [ short | long ]`

- **test** is the action.
- **station** is the object.
- **extension** is a required qualifier.
- **[short | long]** are the optional qualifiers. **|** indicates either-or (either short or long).

Command words may be abbreviated. A partially entered word is recognized when enough letters are entered to distinguish it from other valid entries. For example, the command `test alarms long clear` may be entered as `t al l c`.

If not enough letters are entered, the screen displays a selection of command words or qualifiers that match the abbreviation.

You can drop the leading zeroes from numerical entries. For example, cabinet number 03 may be entered as `3`.

Press or click on the **HELP** key to display every available command or every valid qualifier for the command.

The length of the hardware location differs for the various types of commands:

- `display cabinet` requires a cabinet number location (i.e., `display cabinet 12`)
- `display media-gateway` requires a gateway number location (i.e., `display media-gateway 233`)
- `test port` requires a location entry of either
  - the cabinet number plus the carrier letter plus the port number (i.e., `test port 12c13`)
  - the gateway number plus the media module number plus the port location (i.e., `test port 5V90613`)

Contention between simultaneous commands

The following limits apply to maintenance and administration activities:

- Up to 15 users can be logged into the system at the same time.
- Up to 5 maintenance commands can be run concurrently.
- Up to 10 administration commands can be run concurrently.
- In general, you can use only one command at a time on a maintenance object or other system entity. This restriction applies to the following commands:
  - `busyout`
  - `change`
  - `clear`
  - `recycle`
  - `release`
  - `remove`
  - `set`
  - `test`

- When an action command is acting on a circuit pack, the specified circuit pack and each maintenance object located on it are unavailable for other commands.
- Most commands require the use of shared system resources in order to run. When required resources are already in use, the command aborts. only one such command can run at a time.
- Display-only commands generally do not conflict with any other commands:
  - `display`
  - `status`
  - `get`
  - `monitor`

Busyout and release commands

The `busyout` command places the object of the command in a maintenance busy state. In the busyout state:

- The object is removed from active service and is not available for use by call processing.
- Services which are dependent on the busied out component are dropped. If the component supports a link, the link is dropped.
- No scheduled or periodic background tests are run on the object while it is busied out. Demand maintenance tests can be run on the object, but some tests require that the object be released to complete.
- A warning alarm with error type 18 is logged against each busied out object.
- To prevent the busyout of a particular bus, you should move dedicated tone time slots to another bus (the other half of the duplicated bus).

To display a list of every busied-out maintenance object in the system:

1. Type the command `display errors`.
2. Type `error type 18` in the **Error Type** field on the Hardware Errors Report screen.

The **`release`** command releases the maintenance object from the maintenance busyout server and puts it back into service if the health of the object allows. If a **`release`** command is entered for an object that is not busied out, the command aborts.

Alarm and error categories

Use `display alarms` and `display errors` to generate reports for certain groups of maintenance objects.

Use the **Category** field of the input screen to restrict the report to maintenance objects in a specific category. The **HELP** key displays a list of categories. Other fields on the input screen allow you to further customize the alarm and error report.

Common SAT command parameters

The following table contains descriptions for common command input parameters.

Parameter	Meaning
PN#	1–2 digit port network number. Use **list cabinet** to find which port networks are located in each cabinet.
schedule	Use **schedule** to specify a start time to execute the command. When the command is executed, the output is sent to the system printer. **schedule** is available for the **display**, **list**, and **test** commands. • Enter **list common-queue** to display the commands that are currently queued for execution. • Enter **remove common-queue** *job#* to cancel a queued command. This command requires that the system printer is administered.
group#	The 1–3 digit trunk-group number.
group#/member#	The group number followed by a slash and a 1–3 digit member number of an individual trunk.
extension	The extension number assigned to the port or other maintenance object. The number of digits in an extension is determined by the system dial plan.
next	The next available number in the sequence.
repeat #	The number of times a test sequence is to be repeated.
short long	The type of test sequence to run for the maintenance object. The test sequence varies for each maintenance object. The short test sequence is always non-destructive and is the default. **Caution:** For some maintenance objects, **long** is destructive to call service.
clear	Used with **test** commands. **clear** repeats the test sequence until any active alarms against the maintenance object are cleared by the passing of tests or until any test in the test sequence fails. If no alarms are active, the test sequence is run once. • **long clear** clears every alarm against the maintenance object if no errors are encountered. • **short clear** clears only alarms that are pertinent to the tests in the short test sequence.

Table continues…

Parameter	Meaning
	Caution: If every test passes, **`long clear`** clears every error counter. If firmware counters are cleared while an actual problem exists, customer service may degrade due to calls being routed over faulty components.

Common output field descriptions

Output field	Field description
Port	Port location identifier. The port length differs for the various types of commands: • a port circuit requires a full-length address (i.e., 1c1502) • a control carrier component, such as an IPSI, is designated as 01B. In critical-reliability systems, port network connectivity is duplicated a two independent sets of PNC: components: **A-PNC** and **B-PNC**.
Maintenance Name	The name of the maintenance object as it appears in the alarm and error logs.
Alt. Name	The alternate name depends upon the type of the object. for example: • Station MO, Alt. Name = nnnnn (extension). • Trunk MO, Alt. Name = nn/n (trunk-group# / member#). • Personal CO MO, Alt. Name = P/23 (P/ personal CO line group #).
Test No.	The identification number of the test that is being run on the maintenance object as part of a `test` command. Descriptions of each test and related error codes appear under each maintenance object. For specific maintenance object information, see *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03–300430.
Result	One of the following results: • PASS: The command successfully completed. For a **`test`** command, no errors were detected by the test. • ABORT: The command was prevented from completing. See Common Error Codes on page 28. • FAIL: A serious error was detected by the test. See Common Error Codes on page 28. • NO BOARD: The system does not detect a circuit pack in the location specified on the command line. • CONFLICT: Another user was testing this maintenance object.

Table continues…

Output field	Field description
	• EPN-DOWN: The EPN holding the maintenance object is inaccessible. The expansion archangel (EA) link may be down. • DISABLED: The maintenance object or test was disabled by the `disable` command. • NOT ASSIGNED: The location specified does not have a circuit pack administered to it. • EXTRA BOARD: This can appear for these circuit packs: - Maintenance test - Announcement - Call Classifier - Tone Detector - Speech Synthesis Each of these circuit packs has restrictions on how many can be in the system or port network, depending on the system configuration. Remove the extra circuit pack(s).
Error Code	Indicates the reason for a FAIL or ABORT result. For `test` commands that return a test result, consult the tables of test error codes under the relevant maintenance object in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers,* 03–300430. For `busyout`, `release`, and `reset` commands, see Common Error Codes on page 28.

Error messages

Error Message	Meaning
`All maintenance resources busy; try again later`	Every available maintenance resource is currently in use.
`Board not inserted`	The specified board is not inserted in the system.
`Command resources busy; Press CANCEL to clear, and then resubmit`	There is a resource problem. Restart the command.
`Error encountered; can't complete request`	The command cannot be executed, perhaps because of corrupt software. Follow normal escalation procedures.
`Hardware-group command aborted with cancel command entered from another terminal`	The **`test hardware-group`** command which is running in the foreground was successfully canceled with the **`cancel hardware-group`** command from another terminal.

Table continues…

Error Message	Meaning
'login id': 'command' has a command conflict	The command is in conflict with another currently executing command. The login id of the conflicting user and the conflicting command is shown.
Port/Board invalid	The format for the board location is incorrect.
PN is not available	The PN in which the specified board resides is not available.
save translations has a command conflict	An update of the standby server is in progress.

Common Error Codes

Error Code	Command Result	Description/Recommendation
	ABORT	System resources are unavailable to run the command. Try the command again at one-minute intervals up to 5 times.
0	ABORT	Internal system error. Retry the command at one-minute intervals up to 5 times.
1005	ABORT	A DS1 interface circuit pack could not be reset because it is currently supplying the online synchronization reference. Use **set sync** to designate a new DS1 interface circuit pack as the online reference, then try the reset again.
1010	ABORT	An attempt was made to busyout an object that was already busied out.
1011	ABORT	An attempt was made to release an object that was not first busied out.
1015	ABORT	A reset of this circuit pack requires that every maintenance object on it be in the out-of-service state. Use **busyout board** to place every object on the circuit pack in the out-of-service state, and try the reset again.
1026	ABORT	The specified TDM bus cannot be busied out because the control channel or system tones are being carried on it. Use **set tdm PC** to switch the control channel and system tones to the other TDM bus.
1426	ABORT	The port cannot be released because the gateway has the Emergency Transfer Mode set. The user must use the command line interface of the gateway to clear the mode.
2012	ABORT	Internal system error.

Table continues…

Error Code	Command Result	Description/Recommendation
2500		
2100	ABORT	System resources to run this command are unavailable. Try the command again at one-minute intervals up to 5 times.
62524 62525 62526	ABORT	Maintenance is currently active on the maximum number of maintenance objects that the system can support. A common cause is that the system contains a large number of administered stations or trunks with installed circuit packs that are not physically connected. Resolve as many alarms as possible on the station and trunk MOs, or busyout these MOs to prevent maintenance activity on them. Then try the command again.
	NO BOARD	The circuit pack is not physically installed.
	EXTRA BD	This result can appear for the following circuit packs: • Maintenance/Test • Announcement • Call Classifier • Tone Detector • Speech Synthesis Each of these circuit packs has restrictions on how many can be installed in the system or in a port network, depending on system configuration. Remove any extra circuit packs.
1	FAIL	For **reset** commands, the circuit pack was not successfully halted. Replace the circuit pack.
2	FAIL	For **reset** commands, the circuit pack was not successfully restarted after being halted. Replace the circuit pack.
	FAIL	See the applicable maintenance object information in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers (03–300430)*.
	PASS	The requested action successfully completed. If the **reset** command was used, the circuit pack is now running and should be tested.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Document number	Title	Description	Audience
Maintenance and Troubleshooting			
03–400430	*Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers*	Alarms and error descriptions for maintenance objects associated with Communication Manager.	Technicians, system administrators, Communication Manager maintenance personnel at customer-end.
03–400432	*Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers*	Procedures to monitor, test, and maintain an Avaya Server or Gateway system. It covers many of the faults and troubles that can occur and provides simple procedures to correct them.	Technicians, system administrators, Communication Manager maintenance personnel at customer-end.
03-602013	*Avaya Aura® Communication Manager SNMP Administration and Reference*	Describes the SNMP administration and the MIB group.	Technicians, system administrators, Communication Manager maintenance personnel at customer-end.

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
ATI01672	Avaya Aura® Communication Manager Fundamentals
ATI02348	Avaya Aura® Communication Manager Implementation

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support web site, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support web site, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. On the Avaya Support website at http://support.avaya.com, search for notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to help answer questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Maintenance command descriptions

aar analysis

list aar analysis

Use **list aar analysis** to view the parameters that the Automatic Alternate Routing (AAR) table uses to route a call.

Syntax

```
list aar analysis [start] [route] [location n|all] [node] [to-node] [count] [schedule]
```

start This is an optional parameter. The digit string from which the system starts listing the aar analysis data.

route This is an optional parameter. The route number that Communication Manager uses for the dialed string. The parameter value can be one of the following:

- 1 to 2000
- r1 to r32
- p1 to p2000

location This is an optional parameter. The location of the extension. The parameter value can be one of the following:

- 1 to 2000
- all

node This is an optional parameter. The first node in the list that you want the system to display. The parameter value can be in the range of 1 to 999.

to-node This is an optional parameter. The last node in the list that you want the system to display. The parameter value can be in the range of 1 to 999.

count This is an optional parameter. The number of stations that you want the system to display.

schedule This is an optional parameter. The time at which you want the system to print the output.

Field descriptions

Field	Description
Location	The location of the extension.
Dialed String	The dialed string that matches with the dialed string entry in the AAR Digit Analysis table.
Total Min Max	The minimum and maximum number of digits that you have administered to match with the dialed string.
Route Pattern	The route pattern that Communication Manager uses for the dialed string.
Call Type	The type of call for each dialed string.
Node Number	The destination node number in a private network when the system uses Node Number Routing or Distributed Communication System (DCS).
ANI Reqd	The value of this field denotes if R2–MFC and Russian MF ANI calls require ANI.

aar route-chosen

list aar route-chosen

Use the **list aar route-chosen** command to check the parameters that the Automatic Alternate Routing (AAR) table uses to route a call to a number. Using AAR, the system automatically selects the most desirable and least expensive route for calls over the trunk facilities at the customer's end.

Syntax

```
list aar route-chosen x [location n|all][partition n][schedule]
```

x The dialed number.

location *n* Optional. The location number. The parameter value includes:

- **1** to **2000**
- **all**

The default value is **all**.

partition *n* Optional. The partition group number. The parameter value ranges from **1** to **8**.

schedule Optional. The start time for the command.

Field descriptions

Field	Description
Location	The location entered on the command line.
Partitioned Group Number	The partitioned group number entered on the command line. The default value is **1**.
Dialed String	The dialed string matching with the dialed string entry in AAR Digit Analysis table.
Total Min Max	The minimum and maximum lengths matching with the minimum and maximum length entries from the AAR Digit Analysis table.
Route Pattern	The pattern number used to route the call.
Call Type	The call type matching with the call type entry from the AAR Digit Analysis table. For more information on this field, see the **change aar analysis** command in *Administering Avaya Aura® Communication Manager Screen Reference* (03-602878).
Node Number	The node number matching with the node number entry from the AAR Digit Analysis table.
Actual Outpulsed Digits by Preference	The digits transmitted when you choose each of the preferences in the route pattern.

access-endpoint

busyout access-endpoint

Use the **busyout access-endpoint** command to busy out an access endpoint.

For more details on busyout commands, see Busyout and release commands on page 24.

⚠ Caution:

busyout access-endpoint command drops an active call on the endpoint.

Syntax

```
busyout access-endpoint extension
```

extension The extension of the access endpoint that needs to be busied out.

release access-endpoint

Use the **release access-endpoint** command to release all ports from the busy state. Communication Manager performs the periodic and scheduled tests and completes the background initialization testing on the released ports.

The **Port** field displays the port address of the released access endpoint.

For more information about busyout and release commands, see Busyout and release commands on page 24.

Syntax

```
release access-endpoint extension
```

extension The extension of the access endpoint that needs to be released.

status access-endpoint

Use the **status access-endpoint** command to check the operational status of an access endpoint.

Syntax

```
status access-endpoint extension
```

extension The extension of the access endpoint.

Field descriptions

Field	Description
Extension	The extension number of the access endpoint.
Port	The physical location of the port, including cabinet, carrier, slot, and circuit, to which the access endpoint is connected. **Note:** For the wideband access endpoint, the location is the starting port.
Communication Type	The type of communication that the channel supports. Values of this field include: • 56k-data • 64k-data • voice-band-data • voice-grade-data • wideband

Table continues…

Field	Description
Width	The width of the access endpoint. For communication types 56k-data, 64k-data, voice-band-data, and voice-grade-data, the width is **1**. For communication type wideband, the width is the number of DS0s that make up the access endpoint.
Service State	The operational status of the access endpoint channel. Values of this field include: • in-service or active • in-service or idle • out-of-service • maintenance-busy • disconnected
Connected Ports	The location of any facility or endpoint to which this access endpoint is connected.

test access-endpoint

Use the **test access-endpoint** command to perform the hardware diagnostic tests on all the port circuits associated with an access endpoint.

Syntax

```
test access-endpoint extension  [ short | long | repeat n | clear ]
```

extension The extension of the access endpoint. The number of digits is determined by the dial plan.

short Perform a series of non-destructive diagnostic tests.

long Perform a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and non-destructive tests.

repeat *n* The number of times to repeat the test sequence.

clear Repeat the test sequence until the alarm is cleared or until a single test in the sequence fails.

Examples

```
test access-endpoint  25012
test access-endpoint  45002  sh
test access-endpoint  45892  l
test access-endpoint  24389  sh r 4
test access-endpoint  34899  l r 6
test access-endpoint  93483  r 2
test access-endpoint  10022  c
```

administered-connection

disable administered-connection

Use the **disable administered-connection** command to stop scheduled and periodic testing and to stop processing of inline errors for all or selected administered connections.

To view the administrative information for administered connections, use the **list administered-connection** and **display administered-connection** commands.

Syntax

```
disable administered-connection  [ a-c#  | all ]
```

a-c# The number assigned to the administered connection during administration.

all Disable all administered connections.

Example

```
disable administered-connection all
disable administered-connection a-c1
disable administered-connection a-c2
```

enable administered-connection

When maintenance is disabled using the **disable administered-connection** command, use the **enable administered-connection** command to re-enable scheduled and periodic testing and inline error processing on a specified administered connection or every administered connection.

Using administered connection commands, you can isolate the results of certain maintenance processes by preventing interference.

To view administrative information for administered connections, use the **list administered-connection** and **display administered-connection** commands.

Syntax

```
enable administered-connection a-c # | all
```

a-c# The number of the administered connection assigned during administration.

all Enable all the administered connections.

status administered-connection

Use the **status administered-connection** command to see the operational status of an administered connection.

Syntax

```
status administered-connection a-c #
```

a-c# The number of the administered connection assigned during administration.

status administered-connection field descriptions

Field	Description
Connection Number	The number assigned to the administered connection.
Enabled	The status that shows whether the administered connection is enabled.
Originator	The extension of the access or data endpoint that initiates the connection.
Destination	The destination address used to route the administered connection.

aesvcs

reset aesvcs link

Use the **reset aesvcs link** command to reset an AESVCS link. This command closes the socket connection and the AES server attempts to reconnect.

For more information on links, see the **status link** command.

Syntax

```
reset aesvcs-link n/n
```

n/n The AESVCS server number and the AESVCS link number.

Example

```
reset aesvcs link 01/01
```

status aesvcs cti-link

Use the **status aesvcs cti-link** command to see the status of all the CTI links associated to AES servers on the AE Services Administration page of the IP Services screen administered using

the **change ip-services** command. These links provide connectivity to ASAI adjuncts, which are connected to an Ethernet LAN.

For more details on links, see the **status link** command.

Syntax

```
status aesvcs cti-link
```

status aesvcs cti-link field descriptions

Field	Description
CTI Link	The CTI link number. The field value range is 1–16.
Version	The negotiated ASAI protocol version.
Mnt Busy	The status indicating whether maintenance is busy. Values include y/n. If the value is y, the link has been busied out using the **busyout cti-link** command. Use the **release cti-link** command to release the busied out link.
AE Services Server	The name of the AES server on the AE Services Administration page of the IP Services screen administered using the **change ip-services** command.
Service State	The status of the TCP/IP tunnel connection and CTI link. Values include **down/established**.
Msgs Sent	The number of ASAI messages sent during a specified 30-minute window collection period.
Msgs Rcvd	The number of ASAI messages received during a specified 30-minute window collection period.

status aesvcs interface

Use **status aesvcs interface** command to see the status of the interfaces on which Communication Manager checks for AESVCES server connections.

Syntax

```
status aesvcs interface
```

status aesvcs interface field descriptions

Field	Description
Local Node	The name of the AESVCS interface as administered on the IP Services screen using the **change ip-services** command.
Enabled	The status whether the interface is enabled, as set on the Enabled field on the IP Services screen using the **change ip-services** command.
Number of Connections	The number of active AESVCS server connections on the interface.

Table continues…

Field	Description
Status	The current status of the interface: • Disabled — the *Enabled* field is set to `n` on the IP Services screen administered using the **`change ip-services`** command for the interface. • Intfce-down — the interface is not functioning and cannot accept incoming communications. • Listening — the interface is running and AESVCS servers can connect over it.

status aesvcs link

Use the **`status aesvcs link`** command to see the status of all the active sockets associated with AES servers. The sockets are administered on the AE Services Administration page of the IP Services screen using the **`change ip-services`** command.

For more information on links, see the **`status link`** command.

Syntax

```
status aesvcs link
```

status aesvcs link field descriptions

Field	Description
Srvr/Link	The AES server ID from the AE Services Administration page and the AE Services link number. The field value range is 1–16.
AE Services Server	The name of the AES server.
Remote IP	The IP address of the AESVCS link (AESV-LNK) connection on the AES server.
Remote Port	The TCP/IP port of the AESVCS link connection on the AES server.
Local Node	The node name of the interface on which the AES server is connected and the v6 addresses of the node.
Msgs Sen	The number of ASAI messages sent during the 30-minutes moving window collection period.
Msgs Rcvd	The number of ASAI messages sent during the 30-minutes moving window collection period.

test aesvcs-server

Use the **`test aesvcs-server`** command to run diagnostic tests on the specified AESVCS server and any associated AESVCS links (AESV-LNK).

Syntax

```
test aesvcs-server 1-16  [ short | long ] [ repeat # | clear ] [schedule]
```

1–16	The AES server number 1–16.
short	Perform a series of non-desctructive diagnostic tests.
long	Perform a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and non-destructive tests.
repeat #	The number of times to repeat the test.
clear	Repeat the test sequence until any active alarms against the AES server are cleared by the passing of tests, or until any test in the sequence fails.
schedule	Specify a start time for the command.

Example

```
test aesvcs-server  4 long repeat 3
```

alarms

display alarms

Use the **display alarms** command to see the hardware alarm report. Use this report to select the alarms to be displayed.

The system creates the hardware alarm reports from the logs of the maintenance subsystem that monitors the system hardware and logs problems as errors or alarms. The type of alarm indicates the impact of the problem. Following are the types of alarms:

- **Warning alarm** — Indicates a problem that is important to log or external to the system, but does not cause a noticeable degradation of service.
- **Minor alarm** — Indicates a problem that can disable a local area of the system and noticeably degrade the system.
- **Major alarm** — Indicates a problem that widely degrades the system and seriously impairs service. The system places a call to INADS.

A resolved alarm is a problem that has been corrected, and the alarmed component of the system is functioning correctly again. The system stamps resolved alarms with the date and time the problem was corrected. The system handles any errors associated with the alarms as **resolved**.

Syntax

```
display alarms [ schedule ]
```

schedule Specify a start time for the command.

display alarms field descriptions

Field	Description
Alarm Types	Enter `y` or `n` in the alarm type fields to specify the type of alarm to display on the report. You can choose a combination of: • active or inactive alarms • major, minor, or warning alarms • resolved or unresolved alarms
Interval	Enter `m`, `h`, `d`, `w` or `a` to display alarm records for the last month, last hour, last day, last week, or all. • **From:** Display alarm records from the time specified by *mm/dd/hh:mm*, where *mm* is the month, *dd* is the day, *hh* is the hour and *mm* is the minute. If no **From** date is defined, the report includes every alarm active since a month prior to the current time. • **To:** Display alarm record to the time specified by *mm/dd/hh/mm*, where *mm* is the month, *dd* is the day, *hh* is the hour, and *mm* is the minute. If no **To** date is entered, any alarm that is active after the From date is used.
Equipment Type	Identify the equipment type that you want on the report. If there is no input to these fields, the system defaults to every type. • **Gateway:** Display every alarm associated with a particular gateway. • **Cabinet:** Display every alarm associated with a particular cabinet. • **Port Network:** Display every alarm associated with a particular port network. • **Board Number:** Display every alarm associated with a particular circuit pack. Alarms for a circuit pack are referenced by port location (cabinet-carrier-slot). If the cabinet number is omitted, default is 1. • **Port:** Display every alarm associated with a particular port on a circuit pack. Alarms for a port circuit are referenced by port location (cabinet-carrier-slot-circuit). If the cabinet number is omitted, default is 1. • **Category:** Enter a category to restrict the report to maintenance objects in a specific category. The **Help** key displays a list of categories. • **Extension:** Alarms associated with an extension number. • **Trunk (group/member):** Display every alarm associated with a particular trunk group or trunk-group member.

Input for display alarms

Enter **`display alarms`** to display the Alarm Reports options screen. Select different options on this screen for the type of report you want to see and press **Enter**.

Table 1: Alarm Report field descriptions

Field	Description
Port	The location of the alarmed object. • For installed circuit packs, the location is as **cabinet-carrier-[slot]-[circuit]**. • For port network-related objects, the location is as **PN UUB**, where **UU** is the port network number and **B** is the bus (**A** or **B**) • For fiber link-related objects, the location is as **x a-pnc** where **x** is the fiber link number and **a** is the PNC side (**A** or **B**). This is the same identifier that is used by the alarm log.
Maintenance Name	Name of the MO as it is in the alarm and error logs.
On Brd	**y** indicates that the fault is on the associated circuit pack. **n** indicates that the fault is located on an off-board element that is connected to the circuit pack.
Alt. Name	Alternate name depends upon the type of the object. For example: • Station MO, Alternate Name = **nnnnn** (extension) • Trunk MO, Alternate Name = **nn/n** (trunk-group#/member #) • Personal CO line MO, Alternate Name = **P/xx** (P/personal CO line group #)
Alarm Type	Major, Minor, or Warning. This is an indicator of the seriousness of the alarm.
Service State	Service state of the station and trunk ports: • **RDY** — ready for service • **OUT** — out of service • **IN** — in service • **[Blank]** — No associated service state
Ack	Headings 1 and 2 identify the first and second OSS telephone numbers, respectively. The entries in the column below ACK indicate the acknowledged alarm state: • **y** — alarm has been acknowledged • **n** — alarm has not been acknowledged • **c (cleared)** — alarm was first acknowledged, then resolved and cleared • **[Blank]** — no attempt was made to report the alarm If the user disables the alarm origination with **`change system-parameters`**

Table continues…

	maintenance, then the Ack field is blank regardless of the true acknowledged state of the alarm.
Date Alarmed	Day, hour, and minute of alarm.
Date Resolved	Day, hour, and minute of resolution. 0 for active alarms.

Feature interactions for display alarms

If the alarm origination is disabled by **change system-parameters maintenance**, the Ack field is blank regardless of the true acknowledge state for the alarm.

If `second-as-backup` is entered in the Alarm Origination to OSS Numbers field, the column under the heading **2** will be blank for the alarms that the switch has not attempted to send to the second OSS telephone number. For the alarms that the switch has attempted to send to the second OSS telephone number, the column will be `y`, `n`, or `c`, depending on the acknowledgment status of the alarm. After the call to the first OSS telephone number is successful, for the alarms that the switch has attempted to send to OSSN2, the column will be consistent with the column under heading **1**.

test alarms

Use **test alarms** to test the hardware associated with active alarms in the alarms log.

test alarms provides a query screen to help the user narrow the selection of alarmed objects. Once the screen is filled out, press **Enter** to test the hardware associated with the selected alarm log entries. The results in standard test output and status information are on the message line as the command progresses.

Several alarms may be logged against a single maintenance object, each alarm representing a different problem. Even if there are multiple entries in the alarm log for a single object, **test alarms** tests each physical object once.

Syntax

```
test alarms [ auto-page ] [ failures ] [ step ] [ short  |  long ] [ repeat  #  | clear ]
```

auto-page Continue testing and displaying test results by providing a new screen every time the SAT screen is filled with test results. The screen does not scroll to accommodate new results.

If the auto-page option is not specified, when the SAT screen is filled with test results testing stops until the user enters the **Page** key to continue or the **Cancel** key to halt the testing.

failures Show failures on the SAT screen. All passes will not be displayed on the output screen. Hardware failures, aborts, conflicts, and PN-down failures.

step Step to the next or previous alarm without testing the current alarm. Alarm information is displayed with a prompt for a keypress. Enter:

- **CANCEL** to abort the command
- **ENTER** to test the currently displayed alarm

- **NEXT ALARM** (function key) to move to the next alarm
- **PREV ALARM** (function key) to move to the previous alarm without testing the currently displayed alarm

Press **NEXT ALARM** (function key) or **PREV ALARM** (function key) at any time during the command, even during test results. If the **NEXT ALARM** or **PREV ALARM** is pressed during a test, the test is aborted, testing of the current alarm stops, and the next alarm or previous alarm is displayed. If the first alarms is displayed, and the **PREV ALARM** is pressed, then the last alarm is displayed. If the last alarm is currently displayed, and **NEXT ALARM** is requested, the first alarm is displayed.

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test, between 1 and 100.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

test alarms options

After entering **`test alarms`**, you are presented with an options screen for alarm selection. The following fields are displayed on the test alarms screen.

Table 2: test alarms field descriptions — Hardware Test Alarm Query

Field	Description
ALARM TYPES	The type of alarm or combination of alarms to be tested, specified by `y` or `n` in the alarm type fields.
REPORT PERIOD	Test alarms for records for the last hour (*h*), last day (*d*), last week (*w*) or all (*a*).
From	Specifies error records starting from the time specified by *mm/dd/hh/mm* (month/day/hour/minute). If no *From* date is entered, errors from the earliest record in the log are displayed.
To	Specifies every error record up to the time specified by *mm/dd/hh/mm*. If no *To* date is entered, every error up to the current date is displayed.
Equipment Type	To limit the report to a specific group of components, enter the location of a type of equipment in one of the following fields. If no entry is made, errors for the entire system are displayed. • **Gateway** — Enter the gateway number. • **Cabinet** — Enter the cabinet number. • **Port Network** — Enter the port network number. • **Board Number** — Enter the cabinet-carrier-slot address of the circuit pack (for example, 11c04). If the cabinet number is omitted, it defaults to 1.

Table continues…

Field	Description
	• **Port** — Enter the cabinet-carrier-slot-circuit address of the port (for example, 11c0408). If the cabinet number is omitted, the system will default to 1. • **Category** — Enter a category to restrict the report to maintenance objects in a specific category. The **HELP** key displays a list of categories. • **Extension** — Enter the extension number of a port. • **Trunk (group/member)** — Enter a trunk-group number, or a trunk-group and member number separated by a slash (for example, 78 or 78/1).

test alarms output

The responses, with normal output, on a test-by-test basis with one line of data displayed for each test result. With the failures option, only the tests that failed.

Table 3: test alarms field descriptions — Alarm Entry

Field	Description
Port	The location of the alarmed object (cabinet-carrier-slot-circuit). This is the same identifier as used by the alarm log.
Maintenance Name	The name of the MO as it is displayed in the alarm and error logs.
On Board	Whether the fault detected is on the associated circuit pack, or an off board element connected to the circuit pack.
Alt Name	Extension numbers or trunk-group numbers.
Alarm Type	Major, minor, or warning. This is an indicator to the seriousness of the alarm raised.
Service State	RDY (ready for service), OUT (out of service), or IN (in service). This is the current service state of the station and trunk ports shown.

analog-testcall

test analog-testcall

Use **`test analog-testcall`** to use the Automatic Transmission Measurement System (ATMS) to originate test calls over analog trunks. ATMS collects performance measurements on the test call and compares them to administered thresholds. Detail and summary reports of these measurements are generated with **`list testcalls`**.

You can specify testing of an entire trunk group or an individual trunk using either group or member addresses or port and circuit pack location. The type of test call, the number of the testing line on

the far-end switch and various other parameters must be administered on the Trunk Group screen before the command can execute.

The **test analog-testcall** test aborts when attempting a test call on these trunk groups:

- ISDN-PRI
- SIP
- DID
- Any incoming trunk group (transmission tests can only be run on outgoing trunks)

ATMS, **test analog-testcall**, and the measurement reports are described in Automatic Transmission Measurement System (ATMS) in 'Automatic Transmission Measurement System' in *Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers (03–300432)*.

Syntax

```
test analog-testcall  trunk# / member# | port location | board location full |
supervision |  no-selftest | no-return-loss | no-st-or-rl [ repeat # ] [ schedule ]
```

announcement

erase announcement

Use the **erase announcement** command to delete the announcement files from a gateway location, whether the announcement files are backed up to a compact flash or internal flash. For example, when you run the command **erase announcement** *6v9*:

- If the backup device in the gateway location 6v9 is the internal flash on a gateway, all the announcement files on the internal flash (as well as the RAM) are erased.
- If the backup device in the gateway location 6v9 is a Compact Flash inserted in a G430 or G450 Release 2 (or later), all the announcement files in the **/annc/backup** directory on the Compact Flash (as well as the RAM) are erased.

Syntax

```
erase announcment [gateway number] [module number]
```

list announcement

Use the **list announcement** command to see announcement information listed by the extension.

Syntax

```
list announcement [ext x][to-ext x][count n][type x][schedule]
```

ext *x*	List information for a specific extension. Also use **`list announcement`** *x*.
to-ext *x*	When used with the parameter ext *x*, lists information for all announcement beginning with one extension and ending with another.
count *n*	Lists *n* number of announcements.
type *x*	Lists all announcements of a specific type.
schedule	Specify a start time for the command.

announcement-board

disable announcement-board

Use the **`disable announcement-board`** command to disable an announcement board on your system.

The **Maximum TN2501 VAL Boards** and **Maximum Media Gateway VAL Sources** fields on the system-parameters customer-options screen must be set properly in order to enable/disable announcement-board. For information on administering announcement boards, see *Administering Avaya Aura® Communication Manager* (03-300509).

Syntax

```
disable announcement-board x
```

enable announcement-board

Use the **`enable announcement-board`** command to enable an announcement board on your system.

The **Maximum TN2501 VAL Boards** and **Maximum Media Gateway VAL Sources** fields on the system-parameters customer-options screen must be set properly in order to enable/disable announcement-board. For information on administering announcement boards, see *Administering Avaya Aura® Communication Manager* (03–300509).

Syntax

```
enable announcement-board x
```

arp

netstat arp

Use **netstat arp** to:

- Display the C-LAN circuit pack's Address Resolution Protocol (ARP) table
- Help troubleshoot, isolate, and correct duplicate IP addresses within the network

Syntax

```
netstat arp [ unsorted  |  ip-sort | mac-sort | ck-dup ][ all | baord board-location]
```

unsorted ARP data in the order it was received.

ip-sort ARP data by IP address.

mac-sort ARP data by MAC address.

ck-dup ARP entries that contain duplicated IP addresses. This is the default parameter.

The output of **netstat arp** shows as many pages as are required to display all of the data received from the C-LAN boards.

netstat arp field descriptions

Field	Description
Seq Num	A switch-generated, sequential reference number
Dup Status	Displays DUP if a duplicated IP address is found
Board Location	Location of the TN799DP (C-LAN) circuit pack
Maint Name	Maintenance name of the circuit pack
IP Address	IP address
MAC Address	MAC address
Arp/ErrType	• **Other** — The IP address and the MAC address for the entry are dissociated. This can be ignored. • **Invalid** — The IP and MAC address for this entry are disassociated. This can be ignored. • **Dynamic** — needs further investigation. • **Static** — needs further investigation. • **BRD BUSY** — the CLAN-BD has been busied out. • **LPBCK IP** — Loopback query failed, typically because the RSCL is down. • **SNMPFAIL** — SNMP query to the board failed.

Table continues…

Field	Description
	• **Timeout** — SNMP query timeout.

ars analysis

list ars analysis

Use **list ars analysis** to view the parameters that the Automatic Route Selection (ARS) table uses to route a call.

Syntax

```
list ars analysis [start] [route] [location n|all] [node] [to-node] [count] [schedule]
```

start This is an optional parameter. The digit string from which the system starts listing the ars analysis data.

route This is an optional parameter. The route number that Communication Manager uses for the dialed string. The parameter value can be one of the following:

- 1 to 2000
- r1 to r32
- p1 to p2000

location This is an optional parameter. The location of the extension. The parameter value can be one of the following:

- 1 to 2000
- all

node This is an optional parameter. The first node in the list that you want the system to display. The parameter value can be in the range of 1 to 999.

to-node This is an optional parameter. The last node in the list that you want the system to display. The parameter value can be in the range of 1 to 999.

count This is an optional parameter. The number of stations that you want the system to display.

schedule This is an optional parameter. The time at which you want the system to print the output.

Field descriptions

Field	Description
Location	The location of the extension.
Dialed String	The dialed string that matches with the dialed string entry in the ARS Digit Analysis table.
Total Min Max	The minimum and maximum number of digits that you have administered to match with the dialed string.
Route Pattern	The route number that Communication Manager uses for the dialed string.
Call Type	The type of call for each dialed string.
Node Number	The destination node number in a private network when the system uses Node Number Routing or Distributed Communication System (DCS).
ANI Reqd	The value of this field denotes if R2–MFC and Russian MF ANI calls require ANI.

ars route-chosen

list ars route-chosen

Use **list ars route-chosen** to see the parameters used by ARS to route a call to a specific number.

Syntax

```
list ars route-chosen x [ location n | all ] [ partition n ] [ schedule ]
```

x	Dialed number
location *n*	Optional. The location number. The parameter value includes • **1** to **2000** • **all**
partition *n*	Optional. The partition group number. The parameter value ranges from **1** to **8**.
schedule	Optional. Specify a start time for the command.

list ars route-chosen field descriptions

Field	Description
Location	Entries are displayed for phones dialing from the specified location. The default is all.
Partitioned Group Number	Partitioned Group Number as entered on the command line. The default is 1.
Dialed String	The matched entry in the ARS Digit Analysis table.
Total Min Max	Minimum and maximum length of the string matched in the ARS Digit Analysis table.
Route Pattern	Route pattern used to route the call.
Call Type	The call type as matched on the AAR Digit Analysis table. See **change ars analysis** in the *Administering Avaya Aura®Communication Manager Screen Reference (03-602878)* for full explanation of this field.
Node Number	Node number as matched on the ARS Digit Analysis table.
Location	Entries are displayed for phones dialing from this location. If there are no matching entries in the telephone's location, Communication Manager tries the entries for location all.
Actual Outpulsed Digits by Preference	Digits outpulsed when you choose each of the preferences in the chosen route pattern.

attendant

status attendant

Use **status attendant** to see the operational state of the specified attendant console.

Syntax

```
status attendant  console #
```

console # Console number assigned to the attendant.

Description

This information can help in trouble diagnosis and in locating facilities to which the attendant console is connected.

status attendant field descriptions

Field	Description
Console Number	Number assigned to the attendant
Port	Port location of the attendant (cabinet-carrier-slot-circuit)
Service State	In-service/idle, in-service/active, out of service, or disconnected
Usage State	Idle or active
Maintenance Busy State	**y/n** Is maintenance testing the object?
Connected Ports	Port locations to which the attendant is communicating (cabinet-carrier-slot-circuit).

audio-group

list audio-group

Use **list audio-group** to list all audio groups and see how many members (audio sources) are in each group.

For more information on the Audio Groups screen, see *Administering Avaya Aura®Communication Manager (03-300509)*.

Syntax

```
list audio-group { [ 1-Max ] ( number n | ( to-number  n ) | count n ) } [ schedule ]
```

1-Max audio group number to list.

number *n* to-number *n* range of audio group numbers to list.

count *n* number of audio groups to see on the page.

schedule Specify a time for the command to run.

list audio-group field descriptions

Field	Description
Group	Number of the Audio Group
Name	Name of the Audio Group
Number of Sources	Number of members (audio group sources) in the audio group

list usage audio-group

Use **list usage audio-group** to see all extensions that refer to the specified audio group.

For more information on the Announcements/Audio Sources screen, see *Administering Avaya Aura® Communication Manager*.

Syntax

```
list usage audio-group n  [ schedule ]
```

n	Audio group number.
schedule	Specify a time to run the command.

audits

clear audits

Use **clear audits** to clear cumulative and peak hour data collected for each data relation audit. The **clear audits** command clears old data to display the data that is collected since the last **clear audits** when **status audits** is run.

Syntax

```
clear audits [cumulative] [peak-hour]
```

cumulative	The data collected for the peak hour since the last reboot or the last time the **clear audits** command was run.
peak-hour	The data collected since the last reboot or the last time the **clear audits** command was run.

status audits

Use **status audits** to see the results of Data Relation Audits that are built into the switch. Data Relation Audits check for inconsistencies between selected data items in the switch and report inconsistencies. Data Relation Audits are useful during development and testing phases of projects to discover software errors. On field, Data Relation Audits help the switch to recover from data corruption before the service is interrupted.

The status audits command displays the date and time that the requested interval begins, the number of times that the full sequence of audits executes (audit cycles), and status information about each audit that detected a problem or aborted during the interval. The status information contains:

- The name of the audit.
- The number of times an audit ran and corrected an error.
- The number of times an audit ran and detected an irreparable error.
- The number of times an audit ran and aborted.
- For cumulative: The date and time that the audit first detected a problem.
- For cumulative: The time of the most recent error detected by the audit.

Audit data information cumulates from the last reboot or the last **clear audits** cumulative command, and for peak hours since the last reboot or the last **clear audits** command.

The status audits screen does not automatically update, but reflects the system at the time of request.

Syntax

```
status audits [cumulative] [peak-hour]
```

cumulative The data collected for the peak hour since the last reboot or the last time the **clear audits** command was run.

peak-hour The data collected since the last reboot or the last time the **clear audits** command was run.

status audits field descriptions

Field	Descriptions
Start Date	• For cumulative: The date and time of the last reboot or the last time the **clear audits** cumulative command was run. • For peak-hour: The date and time of the beginning of the peak hour since the last reboot or when the last **clear audits** command is run.
# of Audit Cycles Completed	The number of audit cycles completed in the specified interval (0–999999). Asterisks indicate numbers that exceed 999999. The switch executes audits in a set order. After all audits are executed, the switch restarts the sequence. Individual audit values can be larger if the switch is partially through another audit cycle. Audit cycle numbers do not apply to these audits that execute as part of scheduled maintenance.

Table continues…

Field	Descriptions
Audit Name	The audit name that detected an error or aborted. A few audits do not run in the normal audit sequence. Instead, they execute as part of scheduled maintenance and are marked with “(SCH)” following the audit name.
# Cycles Fixed Data	The number of times the audit was run in a specified interval and found a fixable problem. Asterisks are used from numbers that exceed 65534.
# Cycles Could Not Fix Data	The number of times the audit was run in a specified interval and found a problem that could not be fixed. The audited switch data is inconsistent when this happens. Asterisks are used for numbers that exceed 65534.
# Cycles Audit Aborted	The number of times that the audit was run in a specified interval and aborted due to an internal error. Asterisks are for numbers that exceed 65534.
First Error	The date and time when the audit first detected fixed data, could not fix data, or aborted problems since the last **clear audits** cumulative command.
Most Recent Error	The date and time when the audit last detected fixed data, could not fix data, or aborted problems since the last **clear audits** cumulative command.

Table of audits

Time-available Maintenance Audits shows the names of the audits that are run as part of time available maintenance, the audit number (pname) and a short description of each audit. These audits are run using Iname MO_DR_AUDIT (8192). These audits can be run using the **test mo** command with Iname 1892, pname “audit number”, and test number 0.

Audit name	Audit number	Description
AAP-MSG	585	AAP message buffer audit
AC-ISG	607	AC state audit
ADJUSR	595	Adjunct user record audit
ADMTRM	559	Administration terminal audit
ANUR-A	589	Announcement user record audit
AN-ADM	574	Announcement group administration audit
AN-CALLS	572	Announcement group calls audit
AN-QUE	577	Announcement group queue audit
AQSA	545	ACB queue slot allocation audit
ASLINK	606	ASAI link status audit
ASYLED	605	ASAI yellow LED audit

Table continues…

Audit name	Audit number	Description
ATACT	558	Attendant active audit
ATAV	557	Attendant availability
AT-ADM	529	Attendant group administration audit
AT-CALLS	515	Attendant group calls audit
AT-QUE	523	Attendant group queue audit
ATSC-AUD	561	ISDN-PRI TSC UUI buffer audit
AUR-A	540	Attendant user record audit
AU-CIDP	596	Announcement user cid/port audit
BR-CALLS	629	Bridged extensions audit
BRDG-LK	625	Bridging button lock audit
BUTLK	560	Button lock audit
CALK	569	Coverage answer member lock audit
CATT	527	Attendant connections audit
CD-PN-TAB	622	CD_Pn_tab audit
CDM	528	Data module connections audit
CLDIR	631	Clear Directory DEMAND-ONLY audit
CNF-A	637	conference record audit
CO-ADM	530	Coverage group administration audit
CO-CALLS	516	Coverage group calls audit
CR_AUDIT	513	Call processing data audit
CSR-A	544	Connection service record audit
CSTAT	512	Stations connections audit
CTRK	526	Trunk connections audit
DA-CALLS	583	DAP call record audit
DA-CR	628	DAP call records audit
DA-MSG	628	DAP message buffer audit
DE-ADM	531	Data extension group audit
DE-CALLS	517	Data extension group calls audit
DIR	630	Integrated directory audit
DMLK	563	Data module lock audit
DMTM-A	640	Multimedia data index audit
DUR-A	543	Data user record audit
DXLK	567	Data extension member lock audit
EAL-VCTOKEN	644	EAL SVC Objects audit
EI-TAB	620	Expansion Interface table audit

Table continues…

Audit name	Audit number	Description
EMMC-LL	657	EMMC: EMMC_T linked list audit
FHT	554	Facility status hundreds table audit
FSM-TIMER	632	fsm (fac_st) timer audit
FTED	553	Facility status tracked user audit
FTING	552	Facility tracking user audit
FTSRA	593	Fiber time-slot record allocation audit
GIP-TIMER	611	GIP Timer audit
H248TERM-DR	659	H248 term data relation audit
HTLK	568	Hunt member lock audit
HU-ADM	532	Hunt group administration audit
HU-CALLS	518	Hunt group calls audit
HU-QUE	524	Hunt group queue audit
IAP-CALLS	590	IAP call record audit
IAP-URB	591	IAP user record audit
IGAR	654	IGAR: UM<->CM data relations audit
IM-HMM	579	HMM image table audit
INST-LNK	604	Instigator/down-link user link audit
IP-EPT-TAB	651	IP EPT table audit
IPBW-AUD	653	IP bandwidth audit for CAC
IPSI-HMM	650	IPSI clock/pktint audit
ISGR-A	594	ISG call record audit
LIP-TIMER	626	LIP timer audit
LOG-A	570	MDM error/alarm log audit
MAP-HMM	580	HMM map status table audit
MIS-FAC	587	MIS facility state audit
MM-A	636	meet-me user CID audit
MMIP-EPT-TAB	655	MM IP EPT table audit
MP-ADM	575	Modem pool group administration audit
MP-CALLS	573	Modem pool group call audits
MP-CHL-TAB	661	Medpro channel table audit
MSAP-MSG	600	MSAP message buffer audit
MSAP-PCALLS	623	MASI path call record audit
MSAP-REC	601	MSAP local record audits
MSGQ-HMM	582	HMM map request queue audit
MS-CALLS	588	MISAP call record audit

Table continues…

Audit name	Audit number	Description
MTM-A	638	Multimedia complex audit
MTMU-A	641	Multimedia user CID audit
MUSIC-AUD	634	Multiple music audit
MUV	555	Message user verification audit
MWIA	550	Message waiting indicator audit
MWL-NOAP	599	Message waiting lamp no AP audit
NR-IGAR	656	IGAR: CM net region audit
PA-ADM	533	Paging group administration audit
PA-CALLS	519	Paging group calls audit
PCLK	566	PCOL member lock audit
PC-ADM	535	Personal CO line group administration audit
PC-CALLS	521	Personal CO line group calls audit
PE-CALLS	608	PRI endpoint calls audit
PINC-TAB	614	Packet Inter-Port Network Connection Sub-table audit
PI-ADM	534	Pickup group administration audit
PK-ALERT	586	Pickup alert audit
PKT-VCTOKEN	643	Packet SVC objects audit
PLIP-LNK	602	LIP link audit
PN-HMM	578	HMM pname table audit
PRI-CR	598	PRI call record audit
PRI-TBUF	592	TSCUUI buffer audit
PUR-A	541	Phantom user record audit
SBS-MTM-A	652	SBS trk MTM index audit
SDSBUF	581	Service dispatcher stim buffer audit
SDSID	571	Service dispatcher SID audit
SE-ADM	538	Terminating extension group administration audit
SE-CALLS	537	Terminating extension group calls audit
SMTM-A	639	Multimedia station index audit
STNLK	562	Station lock audit
SUR-A	539	Station user record audit
S-INC-TAB	613	Service inter-port network connection sub-table audit
S-LD-TAB	635	Service port listen disconnect sub-table audit
S-PT-TAB	612	Service port connection sub-table audit
S-TAB	619	Service table audit
TDM-VCTOKEN	642	TDM SVC objects audit

Table continues…

Audit name	Audit number	Description
TEGLK	565	TEG member lock audit
TKLK	564	Trunk lock audit
TONE-TS	610	Tone time slot sub-table audit
TR-ADM	536	Trunk group administration audit
TR-CALLS	522	Trunk group calls audit
TR-QUE	525	Trunk group queue audit
TR-SID	514	Touch tone receiver audit
TR-TAB	621	Touch tone receiver table audit
TSC-PRI	520	ISDN-PRI TSC resource audit
TSRA	547	Time slot record allocation audit
T-TS-TAB	615	Tone Time Slot connection sub-table audit
TTI-AWOH	616	TTI/AWOH audit
UGMA	551	User group membership audit
UPUSR-LNK	603	Up-link user link record audit
URMB	548	User record maintenance busy audit
VDNMM-CALLS	658	VDN MM EMMC: Call Audit
VDN-AUD	633	VDN Call Count Audit
XMOBILE-UPGRADE	649	XMOBILE type upgrade audit
MGMC-AUD	542	MGMC Message table audit

Scheduled Maintenance audits

This table shows the names of audits that run as part of scheduled maintenance, the audit number (pname) and a short description of each audit. These audits are run using Iname MO_SCH_AUDIT (8193). These audits can be run with the **`test mo`** command with Iname 8193, pname “audit number” and test number 0.

Audit name	Audit number	Description
BRG-REC	647	Bridge call audit
BUTC	609	Button memory compaction audit
LABEL-AUD	660	Custom button label audit
MWL	556	Message Waiting Lamp audit
NUMBER-MAPPING	648	XMOBILE mapping tables audit
PRI-USR	597	PRI user record audit
SSUR-FREE	662	Shared station user record free list audit
SUR-FREE	624	Station user record free list audit
MWL-NOAP	599	MSG Message Waiting Lamp audit

bcms

monitor bcms

Use **monitor bcms** to see a summary of Basic Call Management System (BCMS) conditions for agents and splits. The online status report is automatically updated every 30 seconds. You can also update the online status report on demand by pressing **UPDATE**. Press **CANCEL** and terminate the login to cancel monitor bcms.

Syntax

```
monitor bcms split  split# | system split# |  skill skill# | vdn vdn#
```

split *split#* Status of a particular split and the number of the split (ACD hunt group number).

system *split#* Status of the split queue and cumulative split information for every split measured by BCMS, and the numbers of the split (ACD hunt group numbers) separated by spaces and/or split number ranges separated by a hyphen (-).

skill *skill#* Status of a particular skill group and the number of the group.

vdn *vdn#* Vector directory number

Example

```
monitor bcms system
monitor bcms split 1
```

monitor bcms field descriptions

Field	Description
Date	The current date and time. Updated every 30 seconds or when UPDATE is pressed.
SPLIT NAME	The name of the split being reported. If no name is administered, the split extension appears as “EXTxxxxx”. Splits appear in split number order.
CALLS WAIT	The number of calls currently waiting in this split’s queue. Direct Agent Calls are preceded by an asterisk. This field is real-time status data.
OLDEST CALL	The amount of time that the oldest call has waited in queue. Real-time status data.
AVG SPEED ANS	The average time required for an answer in this split during the current period, including time in queue and time ringing at the agent’s voice terminal. Intraflow calls (those that overflow from one ACD split to another split) will not have queue time from previous splits included in the average. The calculation is: **Total Answer Time/Total Automatic Call Distribution (ACD) Calls**. This is measurement data and includes only completed calls.
AVAIL AGENT	The number of agents in this split currently available to receive an Automatic Call Distribution (ACD) call from this split. Real-time status data.

Table continues…

Field	Description
ABAND CALLS	The number of calls abandoned during the current period. This is measurement data.
AVG ABAND TIME	The average time abandoned calls waited in queue before abandoning during the current period. The calculation is: **Total Abandon Time/Total Calls Abandoned**. This is measurement data and includes only completed calls.
ACD CALLS	The number of ACD calls handled by this split during the current period. This includes calls that intraflow into the split. This is measurement data.
AVG TALK TIME	The average talk time for ACD calls handled by this split during the current period. This does not include ring time at the agents' voice terminal. The calculation is: **Total ACD Talk Time/Number of ACD Calls**. This is measurement data and includes only completed calls.
AVG AFTER CALL	The average After Call Work (ACW) time for ACD calls handled by this split during the current period. ACD calls with no ACW time are included in the average. Time spent on direct incoming or outgoing calls while in ACW are not included in the average. The calculation is: **(Total ACW Time – Total ACW Incoming Time – Total ACW Outgoing Time)/Total ACD Calls**. This is measurement data and includes only completed calls.
% IN SERV LEVL	Percent in Service Level for a particular skill. It is the percentage of calls that were offered to the skill that were answered within the administered Service Level time according to the service agreement (for example, 80% of the calls within 20 seconds. If all calls were answered in that time, the value for the IN SERV LEVL would be 100%). The administered service level is defined on the hunt group form.

monitor bcms split field descriptions

Field	Description
Split	The number of the split requested. This is translation data.
Split Name	The name of the split requested. If no name exists, `EXT xxxxx` appears.
Date	The current date and time, updated every 30 seconds or when the UPDATE key is pressed.
Calls Waiting	The number of calls currently waiting in this split's queue. Direct Agent Calls are preceded by an asterisk. This is real-time status data.
Oldest Call	The time in **minutes:seconds** that the current oldest call has waited in this split's queue. This is real-time status data.
Staffed	The number of agents currently logged into this split. This is real-time status data.
Avail	The number of agents currently available to receive an ACD call in this split. Agents are in the Auto-in or Manual-in work modes and are not currently on a call. If the agent is on another split's call or in ACW for another split, this agent is not listed as available and will not be recorded here. This is real-time status data.

Table continues…

Field	Description
ACD	The number of agents in this split currently on an Automatic Call Distribution (ACD) call for this split. This includes ACD calls handled by this split that arrive as coverage from another split. This also includes outbound calls (Outgoing Call Manager) distributed through the ACD. If an agent puts an ACD call on hold, but does not enter another state (for example, the agent does not enter the AVAIL state), the agent is still seen as in the ACD state. This is real-time status data.
ACW	The number of agents in this split currently in After Call Work (ACW) split. This is real-time status data.
AUX	The number of agents in this split currently in AUX work for this split. If an agent is on another split's call or in ACW for another split, this agent is not considered in AUX work and is not recorded here. This is real-time status data.
Extn	The number of agents in this split currently on non-ACD calls, incoming or outgoing directly to/from their extensions. If the agents are also in ACW or AUX they are recorded as Extn rather than ACW or AUX. This is real-time status data.
Other Split	The number of agents in this split on another split's call or in ACW for another split. Used if agents belong to multiple splits. This is real-time status data.
Agent	The name of the agent associated with the extension. If no name exists this field is blank.
EXT	The agent's extension. This field is translation data.
STATE	The current state of the agent for this split. Possible states are Avail, ACD, ACW, AUX, Extn In, Extn Out, OtherSplit, and Unstaff. This is real-time status data.
TIME	The clock time at which the agent entered the current state. This is real-time status data.
ACD CALLS	The number of ACD calls (inbound and outbound), that the agent has completed for this split during the current period (half-hour or one-hour). If the maximum number of 255 calls exceeded, 255 appears. This is measurement data.
EXTN IN CALLS	The number of non-ACD incoming calls that the agent has received and completed during the current period, maximum 255. This is measurement data.
EXTN OUT CALLS	The number of outgoing non-ACD calls that the agent has completed during the current period, maximum 255. This is measurement data.

monitor bcms vdn field descriptions

Field	Description
Date	The current date and time (updated every 30 seconds or when Update is pressed).
VDN NAME	The name of the VDN being reported. If the VDN does not have a name administered, this field displays `EXT ##` where **##** is the VDN extension.

Table continues…

Field	Description
CALLS WAIT	The number of calls that encountered this VDN and have not been answered, abandoned, outflowed, or forced busy/disc. Includes calls in queues, in vector processing, and ringing at an agent telephone.
OLDEST CALL	The time the oldest call currently waiting has waited in the VDN. Timing starts when the call enters the VDN.
ACD CALLS	The number of completed ACD calls answered in a BCMS-measured split. The split may have been reached via the queue-to-main, check backup, route-to, messaging split, or adjunct routing commands. Includes Direct Agent calls (EAS only).
AVG SPEED ANS	The average speed of answer for ACD and connect calls (see CONN CALLS below) that have completed for this VDN during the current period. This includes the time in vector processing, in a split queue, and time ringing. The calculation is: **Total Answer Time / (Total ACD Calls + Total CONNect CALLS)** Answer time for a call is recorded when the call ends. For example, if a call originates in interval *x*, is answered in interval *y*, and ends in interval *z*, the associated answer and talk times are recorded in interval *z*.
ABAND CALLS	The number of calls to this VDN that have abandoned before being answered during the current period. This includes VDN calls that were routed to an attendant, telephone, or announcement, and abandoned before being answered.
AVG ABAND TIME	The average time abandoned calls waited before abandoning during the current period. The calculation is: **Total Abandon Time / Total Calls Abandoned**
AVG TALK / HOLD	The average talk time for ACD calls completed by this VDN during the current period. This does not include ring time, but it does include any time the caller spent on Hold. The calculation is: **Total Talk Time / ACD Calls**
CONN CALLS	The number of completed calls that were routed to a telephone, attendant, announcement, messaging split, or call pickup and were answered there.
FLOW OUT	The number of calls that were routed to another VDN or to a trunk, including successful look-ahead attempts.
CALLS BUSY / DISC	The number of calls that were forced busy or forced disconnect during the current interval. This value includes: • Calls that encountered a busy or disconnect vector step • Calls disconnected by a stop vector step • Calls forwarded to a split with a full queue • Calls forwarded to a split with no available agents and no queue This value does not include abandoned calls.

Table continues…

Field	Description
% IN SERV LEVL	The percent of calls offered that completed and were answered within the acceptable service level defined on the VDN screen. The calculation is: **(accepted * 100) / calls offered** *calls offered* is defined as: **acdcalls + flowout calls + abandoned + connect + busy / disc** *accepted* is the number of ACD and CONNect calls that were answered within the administered service level. This field is blank if no calls were recorded for this time interval. This field is also blank if no Acceptable Service Level has been administered on the VDN screen.

board

busyout board

Use **busyout board** to busyout all the ports associated with the specified circuit pack or media module.

Note:

In a port network with duplicated TN2602AP circuit packs, only the standby circuit pack can be busied out.

Syntax

```
busyout board location
```

location Physical location of the circuit pack or media module.

Example

```
busyout board 01c11
busyout board 1v3
```

release board

Use **release board** to activate administered maintenance objects on the circuit pack at specified locations.

Syntax

```
release board  location
```

location Physical location of the circuit pack or media module.

Example

```
release board  1a05
```

reset board

Reset every administered port on the specified circuit pack or media module.

Caution:

Note that **reset board** can disrupt service and may cause extraneous alarms. Effects of a reset vary depending upon the type of object being reset and upon whether the component is duplicated. See the *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)* for the relevant maintenance object for details.

Syntax

```
reset board  location [repeat x ]
```

location Physical location of the circuit pack or media module.

repeat # The number of times to repeat the command. The default is 1.

Description

Use **reset board** to perform a software reset of every administered port on the specified circuit pack or media module. Every port must be busied out before the port board is reset. In critical-reliability systems (duplicated PNC), a reset of an Expansion Interface, Switch Node Interface, Switch Node Clock, or DS1 Converter circuit pack on the active PNC is not permitted. Busyout the standby components before entering the reset.

Example

```
reset board 1a04
reset board 1e13  repeat 4
```

test board

Execute tests on specified circuit pack or media module.

Note:

Some of the tests can be disabled by administration.

Important:

You cannot perform the destructive long tests on a Switch Node Interface (SNI) board unless the board has been busied out.

Syntax

```
test board  location  [ repeat # ]
```

location Physical location of the circuit pack or media module.

repeat # (Optional) The number of times to repeat the command. The default is 1.

short Run short test sequence.

long Run long test sequence.

clear Repeats the test sequence until any active alarms against the maintenance object are cleared by the passing of tests, or until any test in the sequence fails.

Description

Use **test board** to perform a set of hardware diagnostic tests on a specified circuit pack. The system first validates that the board exists at the specified location. Then, based on the logical type of board (for example, Analog, Digital, Hybrid), a series of tests performs diagnostics on the board and then returns results of the tests along with any possible error codes.

The default is to run the short test sequence once.

Example

```
test board  01a01
test board  1v4
```

boot-image

get boot-image

Use **get boot-image** to view the two firmware image parameters on the TN2501AP circuit pack.

Syntax

```
get boot-image  location
```

location Physical location of the circuit pack (cabinet, carrier, slot).

get boot-image field descriptions

Field	Description
Board Type	For VAL, this field is TN2501
FW Vintage	Firmware vintage number
HW Signature	Hardware signature number

Table continues…

Field	Description
Suffix	Circuit pack suffix code letter
Date	Date on which the firmware file was created or transferred to the circuit pack
Timestamp	Time at which the firmware file was created or transferred to the circuit pack
CRC Checksum	Cyclic Redundancy Check (data integrity algorithm)
Active Image	• **y** indicates the active firmware image file • **n** indicates the inactive firmware image file To change the active image file, use **set boot-image**
Reboot Image	• **y** indicates that this image becomes active after a system reset • **n** indicates that this image becomes inactive after a system reset

set boot-image

Use **set boot-image** to direct the system to use one of the two possible firmware image files on the TN2501AP circuit pack.

Note:

After you enter **set boot-image**, reset the circuit pack to activate the firmware image.

Syntax

```
set boot-image [ board  location ]  image  1 | 2
```

board *location*	Physical location of the circuit pack
image *1*	Use Image 1 firmware file
image *2*	Use Image 2 firmware file

bp

change bp

The Avaya INIT login controls business partner access via the **change bp** command.

Syntax

```
change bp
```

change bp field descriptions

Field	Description
Enable Use of dadmin login	Ater a new installation, this field is set to `yes` by default. If the value of this field is `yes`, then profile 2 can be used by a login spelled as dadmin if it is enabled in the license and subject to other existing constraints. If the field is set to `no`, then profile 2 is disabled. This field cannot grant access for dadmin if it is disabled in the license, but can inhibit access if dadmin is enabled in the license.
PIN is set/unset	This display-only field indicates whether a PIN has been established for the login (set) or not (unset). If the PIN is unset, then the next SAT access to that login will require the PIN to be established.
Enable Use of craft2 login	This field works the same as the field for the dadmin login, except that it applies to the second craft login when it is enabled by dadmin.

bri-port

status bri-port

Use **`status bri-port`** to see the service state, maintenance state, and layer 1 state of an ISDN-BRI port. There is also information about the point-to-point signaling links carried over the port. For more information, see the 'BRI-PORT (ISDN-BRI Port)' section in the *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*.

Syntax

```
status bri-port  location
```

location Location of the BRI port

status bri-port field descriptions

Field	Description
Port	The location of the ISDN-BRI port.
Service State	Whether the ISDN-BRI port is **in-service** or **out-of-service**.
Maintenance Busy	Whether maintenance testing is currently being performed on the port.

Table continues…

Field	Description
Layer 1 State	The operational state of the physical connection (Layer 1) of the ISDN link carried over the port: • **activated** — Layer 1 frames are being passed between the port and BRI endpoints • **pend-activation** — The port is in service, the layer 1 interface device is turned on and layer 1 frames are being sent from the port, but the BRI endpoints are not responding • **deactivated** — The layer 1 interface device on the BRI has been turned off due to the port being out of service.
TEI Value	The Terminal Endpoint Identifier (TEI) is a layer 2 addressing parameter used by the switch to exchange information with BRI endpoints over the point-to-point signaling link. The TEI is a number from 1 to 127.
	The operational state of the point-to-point signaling link (Layer 2): • **assigned** — The link is currently in the AWAIT_EST (Await Establish) state at layer 2. If the BRI endpoint supports TEI allocation procedures, those procedures have been successfully executed and a TEI has been assigned to the endpoint by the switch. • **established** — The link is in the MF_EST_NORM (Multi-Frame Established Normal) state at layer 2. The switch has successfully started the link and is now capable of exchanging layer 3 frames with the endpoint. If the endpoint does not support SPID initialization procedures, the voice extension of the endpoint associated with the link is also displayed. This is the normal state for a link in a point-to-point wiring configuration. • **L3-established** — The link is in the MF_EST_NORM state at layer 2 and SPID initialization procedures have been successfully completed. The voice extension of the endpoint associated with the link is also displayed. This is the normal state for a link in a multipoint wiring configuration. • **hyperactive** — Traffic on this link has exceeded the threshold and the link has been suspended.
Endpt Extension	The extension of the voice/data endpoint associated with the link. This field is blank if the link is not in the **established** or **L3-established** state.
Endpt SPID	The SPID (Service Profile Identifier) administered for the voice/data endpoint. This field is blank if the link is not in the **established** or **L3-established** state.
Service SPID	If the link is associated with the Service SPID this field displays **yes** and the Endpoint Extension field is blank. Otherwise this field is blank. Service SPID is a feature used by service technicians to check building wiring between the switch and the BRI endpoint.

Interpreting results of status bri-port

The following table helps interpret the results of **`status bri-port`**. Find the combination of the output field values in your report and follow the actions for the type of endpoint connected to the port.

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
BRI, ASAI	0-126	Assigned	blank	blank	This is a transitory state for BRI endpoints and ASAI adjuncts. The switch is attempting to establish the link. 1. Check the endpoint and wiring by following the SPID Facility test's procedure described in BRI-SET, Various Adjuncts in the *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*. 2. Repeat **`status bri-port`** to determine that the Layer 2 state of the signaling link is either **L3-established** (for ASAI adjuncts and BRI endpoints supporting MIM initialization) or **established** (for fixed TEI BRI endpoints and automatic TEI BRI endpoints not supporting MIM initialization). If it is not, follow normal escalation procedures. (A MIM or management information message is a level-3 message that conveys management and maintenance information between a communications system and a BRI terminal.)
ASAI	0-63	Established	blank	blank	This is a transitory state for ASAI adjuncts. ASAI signaling is connected at Layer 2 but the Layer 3 Restart procedure has not been completed between switch and adjunct. 1. Check the adjunct by following the recommended repair procedures of the manufacturer. 2. Repeat **`status bri-port`** and determine whether the L2 state of the signaling link is **L3-established**. If it is not, follow normal escalation procedures.
BRI	0-126	Established	ext#	blank	This is the normal state for non-MIM initializing, fixed, and automatic TEI BRI endpoints.

Table continues…

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
BRI, ASAI	64-126	Established	blank	blank	This is a transitory state for automatic TEI BRI endpoints that support MIM initialization. 1. Verify that SPID administration on the switch and the endpoint are consistent. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. 2. Try replacing the endpoint. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, follow normal escalation procedures.
BRI-	64–126	L3–Established	ext#	blank	This is the normal state for automatic TEI BRI endpoints that support MIM initialization.
BRI	0–126	L3–Established	blank	blank	An invalid SPID is assigned to link. Change the SPID value in the BRI endpoint to match the SPID administered to the BRI endpoint on the port. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, follow normal escalation procedures.
BRI	0–126	L3–Assigned	ext#	blank	This is a transitory state for BRI endpoints that support MIM initialization. 1. Wait 5 seconds and repeat the command. If the state has not changed, continue with Step 2. 2. Make sure SPID administration on the switch and endpoint are consistent. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, go to Step 3. 3. Try replacing the endpoint. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is

Table continues…

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
					not, follow normal escalation procedures.
BRI	0–126	L3–Assigned	ext#	yes	This is a transitory state for BRI endpoints that support MIM initialization when a SPID Facility test has been used to initialize the station. 1. Wait 5 seconds and repeat the command. If the state has not changed continue with Step 2. 2. Make sure SPID administration on the switch and endpoints are consistent. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, go to Step 3. 3. Try replacing the endpoint. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, follow normal escalation procedures.
ASAI BRI	0-126	Hyperactive	ignore	ignore	Link has sent too many messages per unit time. Signaling has been suspended. After 60 seconds, the system attempts to put the link into service. If a link remains in this state while there is no activity at the BRI endpoint, take the following steps: 1. Make sure SPID administration on the switch and endpoints are consistent. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, go to Step 2. 2. Try replacing the endpoint. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, follow normal escalation procedures.
ASAI	0-126	L3-Restarting	ext#		The switch has sent a Restart message to the adjunct but has not yet received a Restart Acknowledgment message from the adjunct.

Table continues…

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
ASAI	0-126	L3-Restarted	ext#		After receiving a Restart Acknowledgment message, the switch has sent a Heartbeat message to the adjunct and is waiting for a response.
ASAI	0-126	L3-Established	ext#		This is the normal state for ASAI adjunct.
BRI-	64–126	L3–Established	ext#	blank	This is the normal state for automatic TEI BRI endpoints that support MIM initialization.
BRI	0–126	L3–Established	blank	blank	An invalid SPID is assigned to link. Change the SPID value in the BRI endpoint to match the SPID administered to the BRI endpoint on the port. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, follow normal escalation procedures.
BRI	0–126	L3–Assigned	ext#	blank	This is a transitory state for BRI endpoints that support MIM initialization. 1. Wait 5 seconds and repeat the command. If the state has not changed, continue with Step 2. 2. Make sure SPID administration on the switch and endpoint are consistent. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, go to Step 3. 3. Try replacing the endpoint. Repeat **`status bri-port`** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, follow normal escalation procedures.
BRI	0–126	L3–Assigned	ext#	yes	This is a transitory state for BRI endpoints that support MIM initialization when a SPID Facility test has been used to initialize the station. 1. Wait 5 seconds and repeat the command. If the state has not changed continue with Step 2. 2. Make sure SPID administration on the switch and endpoints are consistent.

Table continues…

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
					Repeat **status bri-port** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, go to Step 3. 3. Try replacing the endpoint. Repeat **status bri-port** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, follow normal escalation procedures.
ASAI BRI	0-126	Hyperactive	ignore	ignore	Link has sent too many messages per unit time. Signaling has been suspended. After 60 seconds, the system attempts to put the link into service. If a link remains in this state while there is no activity at the BRI endpoint, take the following steps: 1. Make sure SPID administration on the switch and endpoints are consistent. Repeat **status bri-port** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, go to Step 2. 2. Try replacing the endpoint. Repeat **status bri-port** to determine whether the Layer 2 state of the signaling link is **L3-established**. If it is not, follow normal escalation procedures.
ASAI	0-126	L3-Restarting	ext#		The switch has sent a Restart message to the adjunct but has not yet received a Restart Acknowledgment message from the adjunct.
ASAI	0-126	L3-Restarted	ext#		After receiving a Restart Acknowledgment message, the switch has sent a Heartbeat message to the adjunct and is waiting for a response.
ASAI	0-126	L3-Established	ext#		This is the normal state for ASAI adjunct.

bulletin-board

display bulletin-board

Use **display bulletin board** to see messages.

Syntax

```
display bulletin-board
```

For detailed information about the Communication Manager bulletin board, see *Administering Avaya Aura®Communication Manager (03–300509)*.

cabinet

add cabinet

Use **add cabinet** to administer cabinets on a five-carrier cabinet (MCC) with a Duplex server pair.

Syntax

```
add cabinet n
```

n Number assigned to the cabinet.

add cabinet field descriptions

Field	Description
Cabinet Description	
Cabinet	Number assigned to cabinet
Cabinet Layout	Description of the layout type of cabinet or stack: • cmc-carrier-stack (available when the **IP-PNC** field is y on the **system-parameters customer-options** screen) • five-carrier • G650-rack-mount-stack • G650-port • not-used • single-carrier-stack

Table continues…

Field	Description
Cabinet Type	Description of the type of cabinet: • cmc-port (available when **IP-PNC** is y on the **system-parameters customer-options** screen) • expansion-portnetwork • MCC (multicarrier cabinet) • PPN • SCC (single-carrier cabinet) • S75XE (System 75 XE single-carrier cabinet) • G650-rack-mount-stack, expansion-port network is displayed in the Cabinet Type.
Number of Portnetworks	1–5
Survivable Remote EPN	y/n
Location	If the entry for Location is 1 through 2000: (Depending on your server configuration, see*Avaya Aura®Communication Manager System Capacities Table (03-300511)*.) Assigns the location number to the cabinet. Use **display locations** to see the administered descriptions of all locations. If **display system-parameters customer-options** shows **Multiple Locations** set to *n*, Location defaults to 1. See the “Location” sections in *Avaya Aura®Communication Manager Feature Description (555-245-205)* for a list of features that use location. If the entry for Location is blank: The location is obtained from the cabinet containing the CLAN or the gateway that the endpoint registered with. By default, the value is blank.
IP Network Region	IP Network Region assigned to the cabinet, to map port networks (non-IP circuit packs) to Network Regions. Cabinets connected through a center stage switch (CSS) are required to be in network region 1.
Cabinet Holdover	**A-carrier-only**, or **all-carriers** Displayed when Five Port Networks Max Per MCC is y on the **system-parameters customer-options** screen.
Rack	Displays when Cabinet Layout is **G650-rack-mount-stack** or **rack-mount-stack**
Room, Floor, Building	The physical location of the equipment
Carrier Description	
Carrier	Letter designation of the carrier
Carrier type	• expansion-control

Table continues…

Field	Description
	• fan • not-used • port • rmc-port • switch-node When Cabinet Layout is **G650-rack-mount-stack**, Carrier Type for Carrier A is **G650-port** and is display-only.
Number	PN (port network) or SN (switch-node) number of the carrier
Duplicate	

change cabinet

Use **change cabinet** to administer cabinets on a five-carrier cabinet (MCC) with a Duplex server pair.

Syntax

```
change cabinet  n
```

n Number assigned to the cabinet.

See **add cabinet** for the descriptions of the fields.

display cabinet

Use **display cabinet** to see the how a specific cabinet is administered.

Syntax

```
display cabinet  n
```

n Number assigned to the cabinet.

See **add cabinet** for the descriptions of the fields.

list cabinet

Use **list cabinet** to see the type, layout, room, floor, building, location, and port network number for each cabinet in the system.

Syntax

```
list cabinet [ schedule ]
```

schedule Specify a time to run the command.

list cabinet field descriptions

Field	Description
Number	Number assigned to the cabinet.
Type	The type of cabinet.
Layout	Description of the layout type of the cabinet or stack: • cmc-carrier-stack • expansion-control • fan • not-used • port • switch-node Duplicated servers: • rmc G650: • G650-port • G650-rack-mount-stack
Room	Room where cabinet resides, if administered on the cabinet screen.
Floor	Floor where cabinet resides, if administered on the cabinet screen.
Building	Building where cabinet resides, if administered on the cabinet screen.
Loc	Location number in which cabinet resides. Use **`display locations`** to see the administered descriptions of all locations. If **`display system-parameters customer-options`** shows Multiple Locations set to *n*, Loc defaults to 1.
A B C D E	The letter designation of each carrier. For each carrier the port network number is given (**PN**). If the carrier is a switch node this number is preceded by **SN**.

status cabinet

Use **`status cabinet`** to see the operational status and attributes of the specified cabinet.

The output screen displays configuration information for each carrier, connectivity, and alarm information for each port network or switch node and the emergency transfer status of the cabinet.

Note:

When a system contains no PN maintenance boards, the **Emergency Select Transfer Switch** field is **NoEqp**.

Syntax

```
status cabinet  UU
```

UU Location number of cabinet.

status cabinet field descriptions

Field	Description
Carrier Location	The cabinet number and carrier letter of each carrier in the cabinet.
PN/SN Number	The Port Network number or Switch Node number (1 or 2) of the indicated carrier.
Carrier Type	The type of the indicated carrier: processor, port, expansion-control, switch-node, dup-sw-node, or not-used.
Cabinet Type	One of the following types: • MCC (multicarrier cabinet) • SCC (single-carrier cabinet) • S75XE (System 75 XE [pre-R1V4] single-carrier cabinet) • blank (undetermined cabinet type).
PN/SN	Each Port Network and Switch Node located in the cabinet is identified by its PN number or its SN number and PNC designation (A or B).
Connectivity Status	For PNs connectivity status refers to the availability of the EAL (Expansion Archangel Link) and INL (Indirect Neighbor Link) to the carrier for both active and standby PNCs (if duplicated). Possible values are: • **up** — EAL and INL are both available • **down** — EAL and INL are both unavailable • **near-end** — The EAL is available, and the INL is unavailable • **far-end** —The INL is available, and the EAL is unavailable • **aa** — Points to a problem with the archangel. The control is up, but the archangel is not functioning and is not available. • **blank** — In the standby column, this means PNC is not duplicated For SNs connectivity status indicates circuit pack insertion on the Switch Node as follows: • **up** — At least one switch node interface circuit pack in the Switch Node is inserted • **down** — There are no switch node interface circuit packs inserted on the Switch Node • **blank** — In the active column, this indicates that the Switch Node carrier is currently the standby in a critical-reliability system. In the

Table continues…

Field	Description
	standby column, this indicates that the Switch Node carrier is currently active (whether or not PNC is duplicated).
Emergency Transfer	The location of the circuit pack containing the emergency transfer select switch (PN maintenance).
Select Switch	The current setting of the emergency transfer switch: • **on** — Emergency transfer has been manually activated • **off** — Emergency transfer is being manually prevented • **auto+** — The cabinet is controlling emergency transfer and is activated • **auto-** — The cabinet is controlling emergency transfer and is not activated • **unavail** — The current setting of the emergency transfer switch is not available
PN/SN	Each Port Network and Switch Node located in the cabinet is identified by its PN number or its SN number and PNC designation (A or B).
Mj, Mn, Wn	The number of major, minor, and warning alarms currently logged against the Port Network or Switch Node.

calltype route-chosen

list calltype route-chosen

Use **`list calltype route-chosen`** to see how digits are handled for a particular call.

Syntax

```
list calltype route-chosen x [ location n | all ] [ partition n ] [ schedule ]
```

x	Dialed number
location n	(Optional) Location number 1–250 or all. The default is all.
partition n	(Optional) Partition Group Number (1–8)
schedule	(Optional) Specify a start time for the command.

list calltype route-chosen field descriptions

Field	Description
Location	Location from the command line. You can see what would happen if the telephone number you enter into your administration terminal were dialed from a telephone's call log in this location. • If there are matching entries in the entered location, those get used. • If there are no matching entries in the entered location, Communication Manager tries the entries in location all.
Match	• **numeric** — the entry in the Calltype Digit Analysis table that was selected for the dialed string • **blank** — no matching entries for this dialed string in the Calltype Digit Analysis table
length Min Max	• **numeric** — the entry in the Calltype Digit Analysis table that was selected for the dialed string • **blank** — no matching entries for this dialed string in the Calltype Digit Analysis table
Selected Location	Phones dialing from this location use the entries on this form. If there are matching entries in the telephone's location, those entries get used. If there are no matching entries in the telephone's location, Communication Manager tries the entries in location all.
After Delete and Insert	The digit string as it is after call type digit manipulation for that pattern, up to four manipulations.
Type	• ext • aar • ars • udp The call type used by the call type algorithm to test the modified string. Call types correspond to the equivalent entries on the Calltype Digit Analysis yable (**`display calltype analysis`**).
Result	Results of the analysis on the dialed string. If there was a successful match and completion of the call, the modifications to the dialed string. Results stop at the first successful match and valid route. Use this information to view the call type's specific routing analysis form (AAR Routing table, ARS Routing table, dialplan analysis tables and the uniform-dialplan tables) for more information about the routing of the call.

campon-busyout

campon-busyout

Use **campon-busyout** to busy-out system resources that need maintenance or repair, and to remove idle VoIP resources from the system's pool of available VoIP resources. You can use **campon-busyout** to continue present activity and prevent future activity, so that the facilities eventually become idle and board replacement occurs.

Use **campon-busyout media-processor** to select the media processor to be busied out while the media processor is still in service. Once all of the media processor's resources are in a busy-out state, the associated board can be removed from the system without disrupting active calls. Use **status media-processor board** to check the busy-out status of a media processor.

Syntax

```
campon-busyout trunk [ trunk-group | member ] processor [ location ]
```

trunk *trunk-group*	Location of the resource.
trunk *member*	Location of the resource.
processor *location*	Location of the resource.

A redundant **campon-busyout**, issued for a media processor already in the pending busyout or busyout service state, results in ABORT with an error code for any media processor resource that is already busied.

Use **release board** to abort **campon-busyout**:

- Busied resources are returned to service. The command result is PASS.
- Resources marked for busyout, pending busyout, are cleared. The command result is ABORT with an error code that signifies the release of a media processor that was in the pending busy service state.

busyout board and **busyout port** override any pending busyout states created with campon-busyout for media processors.

capacity

display capacity

Use **display capacity** to see how your system is administered and to see a snapshot status of system resources.

Syntax

```
display capacity [ schedule ]
```

schedule Use schedule to specify a start time for the command.

Description

Use **display capacity** to see the maximum capacities of system resources assigned by the system and the current level of usage. Most of the maximum capacities depend on your contract with Avaya. Capacities are defined in the license files and displayed on the system-parameters customer-options screen.

display capacity field descriptions — Page 1

Field	Description
Current System Memory Configuration	The platform on which the translations were saved. Can also be unknown if no flash card is present or translations made on old load. This is important because platforms are not always compatible. Standard or Extra Large = translations are saved on CM 4.0 or later. Anything other than Standard or Extra Large = translations were saved on a pre-CM4.0 system.
AAR/ARS	
AAR/ARS Patterns	The number of route patterns. See *Administering Avaya Aura®Communication Manager (03–300509)*.
Inserted Digit Strings	The number of 12-digit strings inserted and available for AAR/ARS preferences. See *Administering Avaya Aura®Communication Manager (03–300509)*.
AAR/ARS Analysis Entries	The number of entries in ARS, AAR and Dial Plan Analysis forms (combined)
AAR/ARS Conversion Entries	The number of entries in ARS and AAR Digit Conversion forms (combined)
Toll Analysis Entries	The number of entries in Toll Analysis form
Digit Nodes (contributes to Percent Full)	Building blocks used for storing entries in ARS, AAR, Dial Plan, Toll and Calltype Analysis and Digit Conversion forms
Short Digit Nodes (contributes to Percent Full)	Building blocks used for storing entries in ARS, AAR, Dial Plan, Toll and Calltype Analysis and Digit Conversion forms
ABBREVIATED DIALING (AD)	
AD Entries Per System	The number of abbreviated dialing entries for both group and personal lists.
AD Personal Lists Per System	The number of abbreviated dialing personal lists. See *Administering Avaya Aura®Communication Manager (03–300509)*.
Adjunct Switch Application Interface (ASAI)	
Active Controlling Associations	The number of station domain controls that ASAI adjuncts can request.

Table continues…

Field	Description
Notification Requests	The number of requests ASAI can make to monitor call activity at a split or VDN.
Simultaneous Active Adjunct Controlled Calls	The number of calls that can be controlled by ASAI adjuncts.

display capacity field descriptions — Page 2

Field	Description
ATTENDANT SERVICE	
Attendant Positions	The number of administered attendants.
Queue Length	A real-time snapshot of the number of calls waiting for attendant service.
Queue/Call Status Buttons	The number of attendant queue status buttons administered on stations. There are two types of queue status buttons: • atd-qcalls (ATD - Queue Calls) • atd-qtime (ATD - Queue Time)
Authorization Codes	The number of authorization codes used for security purposes. See *Administering Avaya Aura®Communication Manager (03–300509)*.
BASIC CALL MANAGEMENT SYSTEM (BCMS)	
BCMS Measured Agents	The number of agents the Basic Call Management System (BCMS) is measuring.
BCMS Measured ACD Members	The number of ACD members BCMS is measuring.
BCMS Measured Splits/Skills	The number of hunt groups BCMS is measuring.
BCMS Measured VDNs	The number of vector directory numbers BCMS is measuring.

display capacity field descriptions — Page 3

Field	Description
CALL COVERAGE	
Coverage Answer Groups	The number of coverage answer groups. See *Administering Avaya Aura®Communication Manager (03–300509)*.
Coverage Answer Group Members	The number of members in all coverage answer groups.
Coverage Paths	The number of administered coverage paths. See *Administering Avaya Aura®Communication Manager (03–300509)*.
Call Pickup Groups	The number of administered call pickup groups. See *Administering Avaya Aura®Communication Manager (03–300509)*.
Call Records	The maximum number of active calls at a given time.
CALL VECTORING/CALL PROMPTING	
Total Vector Directory Numbers	The number of system VDNs. See *Avaya Aura® Call Center Release 4.01 Call Vectoring and Expert Agent Selection (EAS) Guide*.

Table continues…

Field	Description
Meet-me Conference VDNs per system	The number of vector directory numbers for the meet-me conference feature.
Maximum Number of Expanded Meet-me Conf. Ports	License-file based value for the number of Expanded Meet-me Conference ports. The maximum value for this field is 300.
Total Vectors Per System	The number of vectors per system. See *Avaya Aura® Call Center Release 4.01 Call Vectoring and Expert Agent Selection (EAS) Guide*.
Meet-me Conference vectors per System	The number of vectors for the meet-me conference feature.
BSR Application - Location Pairs Per System	The number of mappings administered in a multisite network. The maximum number of application-location pairs per system is 2560. For example, for a network of 10 locations, you can assign up to 256 applications. With 20 locations, you can assign up to 128 applications. See *Avaya Aura® Call Center Release 4.01 Call Vectoring and Expert Agent Selection (EAS) Guide*.
Background BSR Poll VDNs	The number of BBP VDNs associated with the BSR polling
Vector Comment Steps (non-blank)	The total number of available, used and system vector steps that can have non-blank comments
Policy Routing Tables	The number of PRTs that can be defined
Policy Routing Points	The number of PRTs x Number of VDNs defined as destination

display capacity field descriptions — Page 4

Field	Description
DATA PARAMETERS	
Administered Connections	The number of connections between two access or data endpoints. See *Administering Avaya Aura®Communication Manager (03–300509)*.
Alphanumeric Dialing Entries	See *Administering Avaya Aura®Communication Manager (03–300509)*.
DIAL PLAN	
Extensions	This includes stations, data endpoints, hunt groups, announcements, TEGs, VDNs, common shared extensions, and code calling IDs.
Miscellaneous Extensions	Anything that is not a station, trunk, data module, or attendant. This includes, but is not limited to, PCOL groups, common shared extensions, access endpoints, administered TSCs, code calling IDs, VDNs, LDNs, hunt groups, announcements, and TEGs.
Calltype Analysis Entries	The number of entries in Calltype Analysis form
UDP Extension Records	The number of 4-digit or 5-digit extension numbers that a user can use to call from one PBX to another.
UDP Digit Nodes	Building blocks used for storing entries in Uniform Dial Plan form
UDP Short Digit Nodes	Building blocks used for storing entries in Uniform Dial Plan form

Table continues…

Field	Description
Digital Data Endpoints	The number of digital serial communication devices that permit the asynchronous transfer of data. This also includes the number of analog adjuncts.
Expansion Port Networks	The number of port networks connected to the TDM bus and packet bus of a processor port network.
Facility Busy Indicators	The number of visual indicators of the busy/idle status of any particular trunk group, hunt group member, or station user. See *Administering Avaya Aura®Communication Manager (03–300509)*.

display capacity field descriptions — Page 5

Field	Description
HUNT GROUPS, SPLITS, OR SKILLS	
Groups/Splits/Skills	The number of ACD hunt groups.
Administered Logical Agents	The number of logical agents administered. Applicable to systems with Expert Agent Selection.
Administered Logical Agent-Skill Pairs	The number of logical agent-skill pairs that are administered.
Logged-In ACD Agents	A real-time field displaying the number of agents actually logged in. For example, if an agent is logged into 4 skills (and there are no other agents), then the Logged-In ACD Agents field is 1 and the Group Members Per System field is 4.
Logged-In Advocate Agents	The number of Advocate agents that are currently logged in.
Logged-In IP Softphone Agents	The number of IP Softphone agents that are currently logged in.
Logged-In SIP EAS Agents	The number of available and used number of ACD agents logged in using the SIP endpoint.
Group Members Per System	The number of agent/group pairs.
CMS Measured ACD Members	The number of agent pairs being measured by CMS.
Dynamic Queue Slots Per System	The number of hunt group queue positions being used. The system pool of queue slots is dynamically assigned as needed. All calls can be queued.
Queue/Call Status Buttons	The number of hunt group queue status buttons administered on stations. There are four types of queue status buttons; attendants use the last two queue status buttons: • q-calls (Queue Calls) • q-time (Queue Time) • atd-qcalls (ATD - Queue Calls) • atd-qtime (ATD - Queue Time)
Intercom Groups Per System	The number of intercom groups set up within your organization.

Table continues…

Field	Description
Modem Pool Groups Per System	The number of modem pool groups. See *Administering Avaya Aura®Communication Manager (03–300509)*.
Personal CO Line (PCOL) Trunk Groups	The number of PCOL trunk groups. See *Administering Avaya Aura®Communication Manager (03–300509)*.

display capacity field descriptions — Page 6

Field	Description
RECORDED ANNOUNCEMENTS/MUSIC/AUDIO SOURCES	
Analog Queue Slots	The number of available and used queue slots that can be or have been assigned to analog line port or aux trunk connected announcement hardware for queuing up calls when the port is busy.
Administered Announcement Files	The total number of available and used extensions for announcement / audio sources that can or have been assigned.
TN2601 VAL Board	The current usage, license limit, and available capacity associated with the “Maximum TN2601 VAL Boards” license feature.
Media Gateway VAL Sources	The current usage, license limit, and available capacity associated with the “Maximum Media Gateway VAL Sources” license feature.
TN2602 Boards with 80 VoIP Channels	The current usage, license limit, and available capacity associated with the "Maximum TN2602 Boards with 80 VoIP Channels" license feature. Used = total number of TN2602 circuit packs in the system administered with 80 VoIP channels Limit = value in the Maximum TN2602 Boards with 80 VoIP Channels field on the system -parameters customer-options form.
TN2602 Boards with 320 VoIP Channels	The current usage, license limit, and available capacity associated with the "Maximum TN2602 Boards with 320 VoIP Channels" license feature. Used = total number of TN2602 circuit packs in the system administered with 320 VoIP channels Limit = value in the Maximum TN2602 Boards with 320 VoIP Channels field on the system -parameters customer-options form.
TEMPORARY SIGNALLING CONNECTIONS (TSC)	
Administered TSCs	The total number of available and used ISDN administered or fixed Temporary Signaling Connections that can or have been assigned.
NCA-TSC Calls	The number of available and used Non Call Associated Temporary Signaling Connections that can or have been assigned.
REMOTE MESSAGE WAITING LAMPS (aut-msg-wt and Message Lamp Ext for other stations	
Automatic Message Waiting Count	The total number of Automatic Message Waiting buttons and Message Lamp extensions that are administered for stations. In this total, the system does not include the extensions that are identical to the station extensions.

display capacity field descriptions — Page 7

Field	Description
TRUNKS	
DS1 Circuit Packs	The number of assigned DS1 circuit packs.
DS1 With Echo Cancellation	The number of DS1 circuit packs that can have echo cancellation.
ICHT For ISDN/SIP Trunks	The number of Incoming Call Handling Table (ICHT) entries administered for trunk groups.
ISDN CBC Service Selection Trunks	The number of call-by-call trunk groups.
Trunk Groups	The number of trunk groups administered.
Trunk Ports	The number of trunk ports administered.
H.323 Trunks (included in Trunk ports')	The number of administered H.323 Office trunks
Remote Office Trunks (included in 'Trunk ports')	The number of administered Remote Office trunks.
SBS Trunks (included in 'Trunk ports')	The number of administered SBS (Separation of Bearer and Signaling) trunks.
SIP Trunks (included in Trunk ports')	The number of administered SIP trunks
Ad-hoc Video Conferencing Ports	The number of ad-hoc ports configured for the system

display capacity field descriptions — Page 8

Field	Description
VOICE TERMINALS	
Station Button Memory (units)	The percentage of memory being consumed by every administered button.
Team Button / Monitored stations	The number of team button assignments. Team buttons are used to monitor members of a team of stations, functional between one Communication Manager server and the Tenovis 155 hardware platform.
Customized Button Labels	The percentage of the Customized Labels available on the currently used system.
Station Records	The number of resources being used by regular stations, announcements, and music on hold.
Stations (includes BRI stations)	The number of voice terminals.
Station Records Used by TTI (Not Shared)	TTI ports that are administered by the system when TTI is activated on the Feature-Related System-Parameters screen (**`change system-parameters`** features). The ports provide dial-tone to the unadministered physical station attached to the physical port location.
Station Records Used by TTI (Shared)	Ports that are shared with AWOH stations. The ports are administered by the system when is TTI activated on the Feature-Related System-Parameters screen (**`change system-`**

Table continues…

Field	Description
	parameters features). The ports provide dial-tone to the unadministered physical station attached to the physical port location.
Stations (includes BRI stations)	The number of voice terminals.
Stations With Port	The number of connected voice terminals (stations with specific administered ports).
Stations Without Port	The number of voice terminals not having an administered port, such as AWOH.
Other Stations	The number of ports used as conversion resources, agent login ID, MASI, and analog announcements.
TTI Ports	The number of ports assigned by TTI features.
Auto Moves Stations	The number of stations available to move using ACTR.
Administered IP SoftPhones	The number of the currently administered IP soft phones.
Video Capable Stations	The current number of simultaneously administered video capable H.323 stations.
Video Capable IP Softphones	The number of the currently administered video-capable IP soft phones.
ISDN-BRI Endpoint and Trunk Ports	The number of ISDN-BRI ports.

display capacity field descriptions — Page 9

Field	Description
TOTAL LICENSED CAPACITY	
Station and Trunk Ports	The number of subscribed ports in the system.
Station Capacity	
SBS Stations	The number of extensions administered as SBS (Separation of Bearer and Signaling).
Radio Controllers	The number of subscribed Radio Controller circuit packs
Wireless Terminals	The number of subscribed wireless terminals
XMOBILE Stations	The number of X-station mobility (XMOBILE) stations
EC500	The number of Avaya Extension to Cellular (EC500) ports
ISDN DECT	The number of ISDN-based DECT X-Mobile stations.
IP DECT	The number of IP-based DECT X-Mobile stations.
PHS	The number of PHS ports
Off-PBX Telephone - EC500	Usage of the EC500 application (AvayaExtension to Cellular)
Off-PBX Telephone - OPS	Usage of the OPS application (Off-PBX Station, supporting non-native endpoints)
Off-PBX Telephone - PBFMC	Usage of the Public Fixed Mobile Convergence (PBFMC) application.
Off-PBX Telephone - PVFMC	Usage of the Private Fixed Mobile Convergence (PVFMC) application.

Table continues…

Field	Description
Off-PBX Telephone - SCCAN	Usage of the Seamless Converged Communications Across Network (SCCAN) application.
Survivable Processor Capacity	Usage of the total number of Survivable Core Servers and Survivable Remote Servers administered on the system.

display capacity field descriptions — Page 10

Field	Description
System Limit (units)	
Administered Applications (%)	Usage of application memory and mapping memory by Administered Applications
Enterprise Mobility User (%)	Usage of application memory and mapping memory by EMU
Acquired Shared Mappings (%)	Usage of application memory and mapping memory by Acquired Shared Mappings
one-X server Mappings (%)	

display capacity field descriptions — Page 11

Field	Description
CONCURRENT USAGE COUNTS	
IP Stations	The number of IP stations
IP Stations in TTI State	The number of registered IP stations in the TTI state
IP Attendant Consoles	The number of IP attendant consoles
Remote Office Stations	The number of remote office stations
Unauthorized H.323 Stations	The number of H.323 station types that do not need to authenticate with Communication Manager
AES Server Licensed IP Stations	The number of IP stations registered to the switch through the Application Enablement Services (AES) servers and using AES licenses
IP PORT USAGE COUNTS	
Total IP station ports	The number of ports for IP stations
Administered IP Stations and Attendants	The number of ports administered with IP stations and attendants currently in use
Softphone Enabled on Station Form	The number of stations that have the IP Softphone field enabled on the station forms
Unnamed Registrations (TTI IP phones)	The number of IP ports used by H.323 phones that do not have an extension number

display capacity field descriptions — Page 12

Field	Description
ID	Product identifier from the license file • AgentSC =

Table continues…

Field	Description
	• IP_API_A = • IP_Agent = IP agents • IP_NonAgt = • IP_Phone = IP phones • IP_ROMax = R300 remote office phones • IP_Soft = IP Softphones • IP_Supv = • IP_eCons = IP Softconsole • oneX_Comm =
Rel	Release number of IP endpoint. A blank implies any release.
Used	The number of products registered
Avail.	The number of products available for registration
System Limit	Registration limit

display capacity field descriptions — Page 13

Field	Description
CURRENT SYSTEM INFORMATION	
Software Load	The current software load on which the system is running.
Memory Configuration	The system platform.
Offer Category	The system's offer category.
LAST TRANSLATION LOADED INFORMATION	
Software Load	The software load translations saved before upgrade or reboot. Can also be `unknown/no trans` if no flash card is present. Also, if load translations were upgraded from one prior to G3V4 load 71 or early G3V5 loads, `unknown/no trans` displays.
Memory Configuration	The platform on which the translations were saved. Can also be `unknown` if no flash card is present or translations made on old load. This is important because platforms are not always compatible. Standard or Extra Large = translations are saved on CM 4.0 or later. Anything other than Standard or Extra Large = translations were saved on a pre-CM4.0 system.
Offer Category	The offer category that was set when the last **`save translation`** was done before upgrade or reboot. Can also be unknown if no flash card is present or translations made on old load.
Platform	A number (identifier) indicating the platform the customer is using.
H.323 Stations via TLS	**Note:** The **H.323 Stations via TLS** field complies with the Unified Capabilities Requirements (UCR) 2008 Change 3 requirements and is approved by

Table continues…

Field	Description
	Joint Interoperability Test Command (JITC). This field is available only for the USA Department of Defense (DoD) and approved Federal government customers. As a DOD customer capacity limit, Communication Manager capacity for H. 323 station support for desk phones or softphones is: • Large CM Platform- 2000 encrypted channels • Medium CM Platform- 1000 encrypted channels • Small CM Platform (S8300x)- 160 encrypted channels

carrier

recycle carrier

Use **recycle carrier** to momentarily shut down and restore power to a specified G650 carrier or duplex server pair. When a power unit is replaced in a carrier, use **recycle carrier** to restart the power on that carrier.

⚠ Caution:

- Duplex server pair: When a port carrier is recycled, every port and adjunct supported by circuit packs on that carrier undergoes a service outage. Use **recycle carrier** UUC [override] to power recycle a control carrier.
- Never recycle power to a carrier containing AUDIX TN566/TN2169 circuit packs without first shutting down the AUDIX system. Doing so can damage AUDIX software. Follow instructions on the TN566/TN2169 faceplate (these also under ADXDP-PT in *Maintenance Alarms for Communication Manager, Branch Gateways and Servers (03–300430)*).
- **recycle carrier** drops all calls within a carrier when only a carrier is specified or slot 0 was specified for a carrier with a single power supply.
- Use **recycle carrier** override to power cycle a control carrier that contains a TN2312BP,

Syntax

```
recycle carrier  UUC [ SS ] [ override ]
```

UU The location of the cabinet.

C Location of the carrier (or G650 within a G650 stack).

SS (Optional) The slot location (0 or 15 in a G650).

override Required when the controlling TN2312BP circuit pack is present in the same carrier as the specified power supply.

Description

Use recycle carrier to:

- Reset all the boards in the carrier in an attempt to clear a problem when a board stops responding to control channel messages
- Verify that each power supply, in a carrier with two power supplies, can supply the full power load for the carrier. Check the voltages from redundant power supplies Specify the slot number, and force the power supply in the other slot to be the only power supply on the backplane. The power supplies monitor the voltage on the backplane, not the voltage from the power supplies.

The following carriers cannot be recycled:

- Switch Node Carrier
- PN Control Carrier
- Any carrier holding an active Tone-Clock or an active EI circuit pack.

Note:

recycle carrier might take 90 seconds to complete. Do not use the LED activity on the front of the power supply as an indicator of the command status.

When you specify a slot, only the power supply in that slot is shut down. If there is another power supply, it provides power to the carrier while the other power supply is shut down. When you do not specify a slot, all operating power supplies in the carrier are momentarily shut down and restored. Use **test board** to confirm that the power supply in slot 15 has ringing capability.

Example

```
recycle carrier 2c
recycle carrier 1a15
recycle carrier 2b override
```

cdr-link

busyout cdr-link

Use **busyout cdr-link** to put the call detail recording link in a maintenance busy state.

Syntax

```
busyout cdr-link primary | secondary
```

primary Primary CDR link. This is the default.

secondary	Secondary CDR link.

Description

When busied out, the link is dropped and must be re-established later when returned to service.

Example

```
busyout cdr-link  secondary
busyout cdr-link
```

release cdr-link

Use **release cdr-link** to remove maintenance objects associated with specified call detail recording (cdr) links from a maintenance busy state.

Syntax

```
release cdr-link primary | secondary
```

primary	Primary CDR link. This is the default.
primary	Secondary CDR link.

Description

These links provide asynchronous data connections from switches to peripherals. They are composed of:

- A manager that initiates and maintains the link
- A controller/protocol that services the link

The Maintenance Name field displays:

- PRI-CDR for the primary CDR link
- SEC-CDR for the secondary CDR link

Example

```
release cdr-link
release cdr-link  primary
```

status cdr-link

Use **status cdr-link** to see the status of the call detail recording (CDR) links.

Syntax

```
status cdr-link
```

Description

If a link is down, the report includes the number of times the switch has tried to re-establish the link. The CDR link is established by socket connection between Communication Manager and a CDR

output device such as a CDR adjunct. The link is used by the server to send call detail records to the output device. A system may have up to two CDR links: a primary and a secondary.

status cdr-link field descriptions

Field	Description
Link State	The operational status of the link: • *up* The link is established and is capable of supporting the application. This is the normal operational state. • *down* The link is physically down. • *endpoint not administered* An output device has not been assigned on the CDR system parameters screen.
Number of Retries	The number of times the switch has tried to set up the link.
Date & Time	The last time the CDR link went up or down.
Forward Seq. No	A counter which increments with every Session Protocol Data Unit (SPDU) sent from the switch to the CDR adjunct. Both the primary and secondary CDR outputs have independent Forward Sequence numbers.
Backward Seq. No	A counter that indicates the number of the next Session Protocol Data Unit (SPDU) that is expected from the CDR adjunct. Both the primary and the secondary CDR outputs have independent Backward Sequence numbers.
CDR Buffer % Full	When the switch produces a CDR record that cannot be immediately transmitted to the CDR adjunct, that record is placed in the CDR buffer. This percentage indicates how full the CDR buffer is at any point in time. If the switch, the CDR adjunct, and the IP link that interconnects them are all working properly, this number should be zero or very close.
Reason Code	Why the CDR link (primary or secondary) last changed from up to down or vice versa. Values when CDR is administered are: • CDR connection is closed • CDR connection is closed • CDR Output mode is blank • Data write failure • EIA port Bit rate changes • Survivable Remote Server is inactive • Maintenance Busy • Path is destroyed by COM • Primary extension is changed • Queue for primary CDR is full • Secondary extension is changed

test cdr-link

Use **test cdr-link** to validate that a call detail recording link has been administered and established.

Syntax

```
test cdr-link primary | secondary [ short | long ] [ repeat# | clear ] [ schedule ]
```

primary	Primary CDR link. This is the default.
secondary	Secondary CDR link.
short	Run the short test sequence. This is the default.
long	Run the long test sequence.
repeat #	(Optional) The number of times to repeat the command. The default is 1.
schedule	(Optional) Specify a start time for the command.
clear	(Optional) Repeat the test sequence until any active alarms are cleared or until any test in the sequence fails.

Description

test cdr-link first validates that the Call Detail Recording (CDR) link has been administered and exists in the switch. Then individual diagnostic tests run on the link and return results of the test along with any possible error codes.

Example

```
test cdr-link
test cdr-link   repeat 4
```

circuit-packs

change circuit-packs

Use **change circuit-packs** to administratively add, change or remove circuit packs that are to be inserted into port, expansion control, and switch node carriers.

Syntax

```
change circuit-packs cabinet#
```

cabinet#	The number of the cabinet containing the circuit packs to be modified. The default is 1.

Description

Use **change circuit-packs** to:

- configure the system when the circuit packs have not yet been physically inserted.
- remove a 655A power supply from translations
- add a missing 655A power supply to translations

Note:

When you add a DS1-C circuit pack to a G650 media gateway, set IP Control on the IP Server Interface screen for the gateway to *n*.

A 655A power supply is self-administering. Do not use **change circuit-packs** to add power supply translations.

The TN code for the TN2312 IPSI and TN2182 tone generator circuit packs cannot be entered on this form. The system displays the TN code, but you cannot change it.

change circuit-packs field descriptions

Field	Description
Cabinet	The administered number of the cabinet
Cabinet Layout	Type of cabinet G650-rack-mount-stack when Cabinet Layout is G650-rack-mount-stack
Carrier	Each page of this screen reports the information for one carrier. This field indicates the letter designation of the carrier displayed on the current page.
Carrier Type	The function of the carrier: • port • G650-(port) when Cabinet Layout type is G650-rack-mount-stack processor • switch-node • dup-switch-node • not-used • cmc-port
Slot	The carrier slot numbers. Populates 655A in slots 00 and 15 if a power supply is plugged in when Cabinet Layout type is G650-rack-mount-stack.
Code	The TN or UN part number of the circuit pack. This number identifies the circuit pack type to system software.
Sfx	The letter suffix of the circuit pack, if applicable.
Name	The name of the circuit pack. This field aids in entering the circuit pack codes. This field is not populated automatically.

display circuit-packs

Use **display circuit-packs** to list circuit packs on a specific cabinet. The output shows what boards are in which slots in each cabinet and carrier.

Syntax

```
display circuit-packs cabinet [ schedule ]
```

cabinet	Cabinet number (1–64)
schedule	(Optional) Specify a start time for the command.

clan-all

status clan-all

Use **status clan-all** to display the status of a C-LAN board.

Syntax

```
status clan-all
```

Description

status clan-all will determine if a C-LAN board:

- is in-service
- can be used by IMS (Integrated Management System) as a source board
- is healthy for firmware-download (no alarms on the board or ports)

status clan-all field descriptions

Field	Description
Slot	The slot where the C-LAN circuit pack is located.
Service State	• in-service • out-of-service
Auto FWDL Capable	• **n** — CLAN is not firmware-capable, CLAN is in use on another download form, or no PPP ports available • **y** — CLAN is healthy and available for firmware-download

clan-ip

status clan-ip

Use **status clan-ip** to see the activity on a C-LAN circuit pack.

Syntax

```
status clan-ip location
```

location The board location of the C-LAN circuit pack.

status clan-ip field descriptions

Field	Description
Reset Time	Time the last reset occurred.
Incoming Received: Octets	The number of octets received since the last reset.
Incoming Received: Datagrams	The total number of input datagrams received from interfaces, including those received in error, since the last reset.
Incoming Received: Discards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space) since the last reset. This total does not include any datagrams discarded while awaiting re-assembly.
Incoming Received: Hdr Errors	The number of input datagrams discarded since the last reset due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
Outgoing Transmitted: Octets	The number of octets transmitted since the last reset.
Outgoing Transmitted: Datagrams	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission since the last reset.
Outgoing Transmitted: Discards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space) since the last reset.
Outgoing Transmitted: No Routes	The number of IP datagrams discarded since the last reset because no route could be found to transmit them to their destination. This total includes any datagrams which a host cannot route because all of its default gateways are down.
Datagrams w/o Routes: ICMP Dest Unreachables	The number of ICMP Destination Unreachable messages received since the last reset.
Datagrams w/o Routes: ICMP Redirects	The number of ICMP Redirect messages received since the last reset.

clan-port

status clan-port

Use **status clan-port** to see link and status information regarding a C-LAN port.

Syntax

```
status clan-port port-location
```

port-location C-LAN port location. The default is 1.

Description

There are five pages of output which display the following:

- Link/port Status
- Error Counters
- Processor Channel Status
- TCP/IP Applications Currently Active
- Gateways

See **status link** for field descriptions.

cleared-alarm-notif

status cleared-alarm-notif

Expert Systems use **status cleared-alarm-notif** to detect chronic alarming conditions.

Syntax

```
status cleared-alarm-notif 1 | 2
```

1 Display the status for the first OSS telephone number. This is default.

2 Display the status for the second OSS telephone number.

Description

Expert Systems use **status cleared-alarm-notif** to detect chronic alarming conditions. If **cleared-alarm-notif** displays **Feature is suspended**, Expert Systems can identify open trouble tickets as chronic problems for special consideration.

communication-interface links

change communication-interface links

Use **change communication-interface links** to administer the links to the servers from peripheral adjuncts.

See **status links** for more details on links.

Syntax

```
change communication-interface links
```

display communication-interface links

Use **display communication-interface links** to list translations for the links to the servers from peripheral adjuncts.

See **status link** for more details on links.

Syntax

```
display communication-interface links [ schedule  ]
```

schedule Specify a start time for the command.

communication-interface processor-channels

change communication-interface processor-channels

Use **change communication-interface processor-channels** to assign each local processor channel to an interface link channel, and to define the information associated with each processor channel on an Ethernet link.

Syntax

```
change communication-interface processor-channels  [ schedule ]
```

schedule Specify a start time for the command.

change communication-interface processor-channels field descriptions

Field	Description
Enable	**y/n** — processor channel is enabled/disabled.
Appl	Identifies the switch application type/adjunct connection used on this channel over a dedicated network. The application gateway is used for conversion between ISDN and TCP/IP. Other forms must be properly administered as well. Valid entries are: • **audix** — Voice Messaging • **dcs** — Distributed Communication System • **fp-mwi** — ISDN Feature Plus Message Waiting Indication. This channel passes message waiting light information for subscribers on the messaging system, from a messaging adjunct on a main switch for a phone on a satellite switch. The terminating location (far end) of this channel must be a Communication Manager system compatible with ISDN Feature Plus proprietary protocol. • **gateway** — Supports an X.25-connected AUDIX connected to an ISDN DCS network. • **gtwy-tcp** — Supports a TCP connected AUDIX connected to an ISDN DCS network. • **mis** — Management Information System, otherwise known as CMS (Communication Management System) • **qsig-mwi** — QSIG Message Waiting Indication. Used with a QSIG-based interface to a messaging system, this channel passes message waiting light information for subscribers on the messaging system. • blank. All **msa** entries refer to an obsolete product. An error message appears if an **msa** value is entered: **msaamwl**, **msaclk**, **msahlwc**, **msallwc**, **msamcs**.
Gtwy To	Identifies which processor channel the given processor channel is serving as a gateway to. Valid entries are a number between 1-(maximum number of processor channels), or blank.
Mode	Identifies whether the IP session is passive (client) or active (server). This field must be blank if the interface link is **processor**. This field cannot be blank if the type of interface link is **ethernet** or **ppp**. Valid entries are **c** (client), **s** (server), or **blank**.
Interface Link	Identifies the physical link carrying this processor (virtual) channel. Links are numbered 1 through 254 or **p** for processor.
Interface Chan	For TCP/IP, interface channel numbers are in the range 5000-64500. The value 5001 is set for CMS and 5003 is set for DCS.
Destination Node	Identifies the switch or adjunct at the far end of this link. Enter an adjunct name, switch name, far-end IP address, node ID, or leave

Table continues…

Field	Description
	blank for services local to this switch. For ppp connections, match the Destination Node Name on the ppp Data Module screen.
Destination Port	Identifies the port number of the destination. The number 0 means any port can be used. Valid entries are **0**, **5000--64500**.
Session Local	The Local and Remote Session numbers can be any value between 1 and 256 (si model) or 384 (r model), but they must be consistent between endpoints. For each connection, the Local Session number on this switch must equal the Remote Session number on the remote switch and vice versa. It is allowed, and sometimes convenient, to use the same number for the Local and Remote Session numbers for two or more connections.
Session Remote	
Mach ID	Destination switch ID identified on the dial plan of the destination switch.

display communication-interface processor-channels

Use **display communication-interface processor-channels** to list the TCP/IP listen port to carry each processor (virtual) channel (on an Ethernet link).

Syntax

```
display communication-interface processor-channels
```

conference

status conference

Use **status conference** to help identify problems with a multimedia conference, and to help solve more complex problems.

Syntax

```
status conference [ all | conference-ID] [ schedule ] [ endpoint-all | endpoint-ID]
```

all Display all stored conference data.

conference-ID Display data for the specified conference (current or last).

schedule Schedule a time to run the command.

endpoint-all Display conference data for all endpoints in the specified conference. This is the default.

endpoint-ID Display conference data for the specified endpoint.

Description

The first screen is displayed when status conference is entered and at least 1 valid conference is found. Use status conference to solve the following multimedia problems:

- A user unable to join or remain joined to a conference.
- A conference having poor video quality due to it being downgraded because of the automatic algorithms — audio AUTO mode and the Px64 video picture specifications.
- A user unable to receive full service, such as being an audio-only endpoint (no video).
- An audio add-on user unable to join or remain joined to a conference.
- A conferee invisible to other users due to interworking problems.
- A user unable to participate in the Multipoint Communications Service conference.
- A continuous conference, without switching endpoints in or out of quadrants.

Depending on the **`status conference`** command entered, it is possible to have many records display. Active conferences display first (in order of conference-ID), followed by completed conferences (most recently completed first). There is no data or information about conferences yet to begin.

The data for each conference displays in 2 parts: the first screen describes the status of the conference and indicates the modes and levels of the conference. It also shows certain endpoint information such as which endpoints are in use and which endpoint caused the conference operating mode to change. This screen is similar to the administration screens. The remainder of the screens display endpoint level data (up to 8 endpoints per screen), displaying the ports and drop reasons.

status conference output field descriptions — page 1

Field	Description
Status	The current status of the conference: • active • in-use • complete
Conference Name	Always set as **MMCH DYNAMIC**
Conference Mode	Always set as **voice-activated**
Password	not applicable
Password Scope	not applicable
Cascade Mode	Conference cascade mode — blank
Audio Mode	The current operating audio mode — G.711-A, G.711-mu, G.728, G.722
Class	The type of conference — dedicated
Data Mode	Data mode capability for this conference — none, any-mlp, ww-pcs

Table continues…

Field	Description
MLP Rate	MLP Data Rate for this conference — blank
No. of Channels	The number of channels (transfer rate) required for each Px64 endpoint —- 2.
Chair	Identifies the current chair token holder. This field is always blank.
Conf Bandwidth	The current operating channel conference bandwidth. This can be different from the administered bandwidth because of Rate Adaptation.
Rate Adaptation	Does this conference support Rate Adaptation? — **n/y**.
Format (in/out)	• For single-screen conference, the video format of the conference, **CIF**, **QCIF**, **QCIF/CIF**, **H.CTS**, **H.CTX+**, and **SG4**. • For conferences other than H.261, the input and output formats are always symmetric and the mode is the same for input and output. These display as **H.CTX**, **H.CTX+**, **SG4**. • For H.261 mode non-continuous presence conferences, the format is always symmetric and displays as **CIF** and **QCIF**. The same is true for the non-presentation, continuous presence conference in single-screen. • For presentation mode H.261 single screen continuous presence capable conferences, the input and output formats may be symmetric QCIF/CIF (displayed as **CIF**) or asymmetric QCIF/CIF, depending on if the format is administered as upgradeable. • For quad-screen conferences, the format is QCIF/CIF to reflect the input of QCIF from every participant and output of CIF to every participant. • For presentation mode quad-screen conference, the format is also **QCIF/CIF** to reflect the input/output of every participant except the presenter. In quad-screen mode, the input from the presenter is always **CIF**.
FPS	The CIF frame rate (frames per second) — ‘**-**‘, **30**, **15**, **10**, **7.5**. FPS indicates the rate that an endpoint is capable of receiving frames. Note that there is no indication of the maximum transmit frame rate nor the current frame rate that the MCU can detect. The frame rate changes as a function of the amount of motion in the input image.
QFPS	The ACIF frame rate (frames per second) — ‘**-** ‘, **30**, **15**, **10**, **7.5**. QFPS indicates the rate that an endpoint is capable of generating/receiving frames. For quad-screen VAS conferences, QFPS reflects the highest common QCIF frame rate of every endpoint and the rate of the video mixer board, which may be lower than the rest of the participants. Note that QCIF calculation takes into account the highest common CIF frame rate declared by every conference participant, since QCIF rate cannot be greater than that of the highest common CIF rate. For quad-screen presentation conferences, QFPS reflects the highest common QCIF frame rate of every participant and the rate of the video

Table continues…

Field	Description
	mixer board. Note that the QFPS cannot be greater than the CIF frame rate announced by the presenter. QFPS field is blank for proprietary modes.
Lo/Hi Interworking	Conference supports Low Speed/High Speed Interworking. Always **n**.
Type	The type of conferee, either Audio/Video (**P64**), Audio Add-on (**AUD**), Cascade Link (**CAS**), BONDing Call (**BOND**), BONDing Cascade Link (**BCAS**), UCC Controller (**UCC**), or Dedicated Access (**DA**). BONDing calls use up to 12 channels to form a single multimedia pipe.
Ext	Endpoint extension chosen at administration. This field is blank.
Meet-me Number	Meet-Me Number administered for the Meet-Me Extension. This field is blank.
Dial Type	Indicates whether dial-in or dial-out is used to join the endpoint to the conference: • **in** — dial-in • **out**— dial-out
In Use	Is the endpoint currently participating in the conference or in process of connecting to the conference? • **y** — The endpoint is in use and is fully connected on all media in an active conference. • **c** — The endpoint is in use and is fully connected, however the endpoint has changed the conference audio or video capability or has changed the rate of the conference because of rate adaptation. This condition requires analysis of this endpoint's capabilities and mode fields to identify which capability was reduced. • **e** — The endpoint is in use but the endpoint had capability problems. The endpoint does not have one of the required capabilities (Vid, Bhl, MLP) to be a full participant. For MLP capabilities, see the T120 field. This condition requires analysis of this endpoint's capabilities and mode field to identify the missing capability. • **f** — The endpoint is in use but is disconnected from all media. This indicates that the endpoint has declared every required capability (channel/video/audio/data) but is not fully connected to all conference media at this time. This endpoint may be in the process of connecting, has failed to connect, or is not a valid video source. This condition requires analysis of this endpoint's capabilities and mode fields to identify the problem. • **n** — The endpoint was connected in a conference but has/was disconnected or attempted to connect to a conference but was unsuccessful. • **blank** — until the first call is made from/to the endpoint.

Table continues…

Field	Description
Chl	Data on the quantify and quality of channels (transfer rate)? • **y** — The endpoint has the required number of channels. • **e** — The endpoint has not declared support for the correct number of channels and cannot participate fully in the conference. • **n** — The endpoint has declared the correct number of channels, but every channel has not yet joined the conference, due to either a network or endpoint problem. • **blank** — Audio add-on endpoints always set to blank.
Aud	Does the endpoint have the required audio capability? • **y** — The endpoint has the required audio capability. Audio add-on endpoint always have the Aud field set to y once the endpoint has joined the conference. • **c** — This endpoint is PCM only and it changed the video quality of the conference by changing the operating audio from G.728 to G. 711. If the administered audio mode is auto and the administered bandwidth is 112 kbps (56 k/channel) or 128 kbps (64 k/channel), the system starts out with the highest common audio of G.728. When the administered bandwidth is greater than 128 kbps, the system starts out with the highest common bandwidth of 7 kHz. • **e** — A PCM-only endpoint that did not have the capability of supporting the administered audio mode of G.728 (such as a data conference), or G. 278/G.711 endpoint that did not have the capability of supporting the administered audio mode of 7 kHz. Such endpoints operate with PCM audio and interwork with the current operating audio mode. • **blank** — until the first call is made from/to the endpoint.
Vid	Does the endpoint have the required video capability and is receiving video? • **y** — The endpoint has the required video capability and should be receiving video if the Chl, Aud, and Dat fields are **y**. • **c** — It downgraded the conference's video quality - either from CIF to ACIF or by decreasing the frame rate. The conference video mode is set by default to CIF and if a QCIF-only endpoint joins the conference, then the entire conference is made to operate in QCIF, with the video clarity downgraded. Also, the conference frame rate is initially set to the highest frame rate that can then be reduced by any endpoint. If the conference video mode is not administered with upgrade capability, then if the video parameters for a conference have been **downgraded**, they are not **upgraded** until every endpoint disconnects from the conference. • **e** — The endpoint has not declared any video capability in its cap-set.

Table continues…

Field	Description
	• **n** — Audio only, not receiving video, possibly due to an audio or data problem. • **blank** — Audio add-on endpoints always blank.
Mlp	The state of the Control Link to the ESM (T.120 stack terminator), the endpoint MLP data capability, and the state of the data connection in the T.120 stack. This field value is always blank, indicating that the Data Mode for the conference is **none**, and therefore, the data does not apply, or the endpoint has never joined the conference.
Gx	Does the endpoint have the Still Frame Graphics capability? • **y** — This endpoint has this capability. • **e** — This endpoint did not declare this capability. The conference retains the still frame graphics capability when a non-compliant endpoint joins the conference. • **blank** — This endpoint has never joined the conference.
Rate Adpt	Rate adaptation/interworking indicator. Values of **5** and **6** apply only to low-speed/high-speed interworking. Every other value applies only to rate adaptation. • **5** — A 56-kbps (low-speed) endpoint has joined a high-speed (128-kbps or above) conference. This endpoint is connected with audio-only capability, but is neither a valid video source nor destination. • **6** — A 64-kbps (low-speed) endpoint has joined a high-speed (128-kbps or above) conference. This endpoint is connected with audio-only capability, but is neither a valid video source nor destination. • **y** — This endpoint has joined a conference at the administered rate of 64 kbps, but (because rate adaptation to 56 kbps was triggered by another endpoint) this endpoint has successfully rate-adapted to 56 kbps. • **c** — The administered bandwidth of a conference is 64 kbps and this endpoint has joined the conference at 56 kbps. The first 56-kbps endpoint that joins a 64-kbps rate-adaptable conference triggers rate adaptation (see Join Time below). • **n** — A 64-kbps conference was triggered to rate adapt to 56 kbps by some other endpoint. This endpoint joined the conference at the bandwidth of 64 kbps, but encountered problems in rate adapting down to 56 kbps. This endpoint may have the audio and may be receiving video, but is not a valid video source. • **blank** — Rate adaptation was never triggered by any endpoints. So, if an endpoint is in use and connected, then it joined the conference at the administered bandwidth.
Bond Mode	Bonding Mode — **blank**. This field is blank for calls that are not related to bonding.

Table continues…

Field	Description
Ts	Indication of the talking state of the endpoint. • **t** — At the time the command was invoked, voice energy (talking) was detected from the endpoint. • **m** — At the time the command was invoked, the endpoint indicated to the MCU that it was muted. It is possible that an endpoint may mute, but not send any indication to the MCU. In this situation the MCU does not display a mute indication. • **M** — At the time the command was invoked, the endpoint's audio was muted via UDD/CRCS Agent interface. **M** displays when both the endpoint and the UCC/CRCS Agent have muted the endpoint audio. • **S** — At the time the command was invoked, the endpoint's audio was muted because of solo-audio state set by UCC/CRCS Agent. While in solo-audio state, new endpoints joining the conference are automatically muted. • **blank** — At the time the command was invoked, voice energy (talking) was not being detected from the endpoint.
Vs	• **a** — This value applies only to quad-screen conferences. ***a** indicates that an endpoint is part of the current mixed image and is fixed in one of the quadrants via administration. ***a** indicates that the endpoint is fixed in a quadrant but is not currently connected (Fill image displays). • **b** — For full-screen conference it indicates that at the time the command was invoked, this endpoint's video was being broadcast to other sites. This conference was in VAS, broadcast, or presentation mode. For quad-screen VAS conference it is prefixed with an asterisk (*) and indicates that this endpoint's video is part of the mixed image because of VAS. For quad-screen presentation conferences, **b** (without an asterisk) identifies the presenter as the broadcaster. • **B** — At the time the command was invoked the endpoint's video was being broadcast to other sites because of the UCC roll call feature. UCC roll call feature can only be performed in full-screen mode. • **c** — At the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in chair mode and the broadcaster was designated by the chair. Chair features can only be performed in full-screen mode. • **i** — At the time the command was invoked the endpoint was not a valid video source. For continuous presence conference, if this endpoint is fixed in a particular quadrant, a pound (**#**) is affixed before **i**. • **r** — For full-screen conferences, at the time the command was invoked the endpoint's video was the return video to the

Table continues…

Field	Description
	broadcaster. For continuous presence conference in presentation mode, ***r** represents a VAS quadrant that is part of the mixed image. • **R** — At the time the command was invoked, the endpoint's video was the return video to the broadcaster because of the UCC browse feature. UCC Browse feature can only be performed in full-screen mode. • **s** — At the time the command was invoked this endpoint's video was suppressed at the request of the endpoint. For continuous presence conference with fixed quadrant participants, if this endpoint is fixed in a particular quadrant a pound (**#**) is affixed before **s**. • **S** — At the time the command was invoked this endpoint's video was suppressed via UCC/CRCS Agent interface. For continuous presence conference with fixed quadrant participants, if this endpoint is fixed in a particular quadrant, a pound (**#**) is affixed before **S**. **S** is displayed when the endpoint and the UCC/CRCS Agent have suppressed the endpoint video. • **u** — For full-screen conferences, at the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in VAS mode and the broadcaster was designated by the UCC/CRSCS Agent interface. For quad-screen conferences, it indicates that UCC/CRCS Agent designated this endpoint as fixed in a quadrant. An asterisk (*****) is affixed before **u** if the endpoint is currently part of the quad image, and a pound (**#**) is affixed if the endpoint is not currently joined. • **U** — Applies only to quad-screen conference and indicates that UCC/ CRCS Agent designated a quadrant as VAS. An asterisk (*****) is affixed before **U** to indicate that this endpoint is part of the current quad image. • **v** — At the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in VAS mode but the endpoint has asked to be a broadcaster via **See-Me** request and was granted a MCV (Multipoint Command Visualize) token. The See-Me feature is only performed in full-screen mode. • **blank** — At the time of the request the endpoint's video was not broadcast, return, video, or part of the mixed-image, but it is a valid video source.

status conference output field descriptions — page 2

Field	Description
Sum Grp	The VD audio Level 1 (L1) and Level 2 (L2) summer group parts for each assigned group (1–4). Summer parts are assigned only for conferences with over 6 participants. When a conference operates at an audio mode of 7 kHz (administered audio mode is 7 kHz, or auto

Table continues…

Field	Description
	with the bandwidth greater than 128 kbps), the system allocates “primary” and “secondary” L1 and L2 summer parts. These primary and secondary parts are allocated as adjacent port slots on the same board. Status conference only displays the primary summer ports. The secondary summer ports are always one slot higher than the displayed primary summer port.
Join Time	Time (in 24-hour notation) when the channel joined the conference.
Drop Time	The endpoint is idle if the first channel has a drop time.
Drop Reason	The reason for the channel’s disconnect: • **2-pri** — This drop reason occurs when an administration error causes a mismatch in primary-secondary designation for a cascade link. This mismatch shows that both MCUs are administered as primaries (see Cascading for a description of primary-secondary compatibility). • **2-sec** — This drop reason occurs when an administration error causes a mismatch in primary-secondary designation for a cascade link. This mismatch shows that both MCUs are administered as secondaries (see Cascading for a description of primary-secondary compatibility). • **Agent** — The reservation agent has caused the call to disconnect (for example, the agent has changed a connected dial-out destination number). • **Bandwidth** — mismatch between a call and the conference it attempted to join. For example, a 56-kbps call attempted to join a 64-kbps conference that does not permit rate adaptation. • **BondHshake** — Bonding handshake drop reason can be caused due to the following reasons: information channel parameter not supported or invalid, parameter negotiation terminated out of sequence, timer expired because of the secondary channels did not establish, or BONDing framing was not detected for one of the other channels. • **Busy** — This dial-out drop reason occurs when the MCU detects that the conferee’s terminal equipment is busy. This drop reason is detected by an ISDN cause value (for example, h0). See Dial-out for a description of CPTR usage. • **Chair** — disconnected the endpoint, using either Chair Command Disconnect (CCD) or Chair Command Kill (CCK) signals. • **Conf End** — The conference was ended due to reaching stop time for a reserved conference or due to an active conference being converted to file.

Table continues…

Field	Description
	• **Endpoint** — Clearing received from DS1. The disconnect came from the endpoint. The endpoint notified the MCU that it intended to disconnect. • **Far-end** — Clearing received from DS1. The disconnect came from either the network or the endpoint. • **Handshake** — Either framing was never found (the endpoint could not complete initialization: problems finding Frame Alignment Signal (FAS), Multi Frame Alignment (MFA) and getting a corrected coded cap-set) or framing was lost for some time (over 40 seconds) and the endpoint was disconnected. • **IDtimeout** — The MCU has not received response to the UIN/password Query from the H.320 user after three attempts. Each attempt has a system administered timeout period. • **Internal** — MCU has a problem allocating trunk resources necessary to route the dial-out call for the specified dial-numbers. This problem can be associated with routing pattern or trunk associated translation (for example, TAC specified in the dial-out number or routing pattern points to a trunk group without members), or it can indicate a lack of trunk resources (for example, every trunk member is maintenance busy or every in-service member is busy on a call). • **Network** — Clearing received from DS1. The disconnect came from the network. The endpoint that had the disconnect notification capability disconnected without notifying the MCU. • **No-ring** — This dial-out drop reason occurs when the call has been up for 30 seconds and no ringing is detected. • **Not-MCU** — The dial-out destination number(s) of the **CAS** extension has terminated to a number that is not a dial-in cascade MCU extension. • **Password** — Either the user entered the wrong password or the audio add-on user did not enter it within the specified time period. Note that the audio add-on user gets one attempt to enter a correct password and inter-digit timing for each digit (that is, about 10 seconds between digits). • **Pre-AnsDrop** — The call disconnected before answer by an endpoint. The cause of the disconnect may be the network, an endpoint, or a terminal adapter. This drop reason is different from **No-answer**, which indicates that a 60-second timeout occurred while alerting. In this case, the call drops before the 60-second timer has expired. Some busy endpoints connected through terminal adapters display this behavior. • **Resource** — MCU could not provide resources (VC or MMI) when the call arrived or lost the resources during the call. This could be due to them being Out of Service, busied out by craft, or being used

Table continues…

Field	Description
	by system maintenance. This drop reason could also occur if the DS1/ MMI cable is disconnected. If there was a resource problem when the call arrived, it would get reorder (fast busy) and not get disconnected by the MCU. • **Reorder** — This dial-out drop reason occurs when the MCU detects that there are no available trunks in the network to place the call. This drop reason is detected by MCU CPTR resources. See Dial-out for a description of CPTR usage. • **System** — An MCU restart (level 2) disconnected every call. • **UIN-Inv** — The user entered an invalid User Identification Number. • **Unknown** — The system could not determine the cause of the disconnect. • **Wrong-num** — This dial-out drop reason occurs when the MCU detects the wrong destination number was dialed. This drop reason is detected by MCU CPTR resources SDN cause value. See Dial-out for details. • **UCC** — controller intentionally disconnected the endpoint.
AC Num	Administered Connection Number - from 1 to 128. AC number can be used to further diagnose a problem by combining status conference information with **`status administered connection`** and data stored in the error and alarm logs.
Ports Trunk	The data endpoint that the channel is using.
Ports Video	The MMI port for the channel.
Ports Aud	If the endpoint type is not **UCC**, the VC audio encoder port (which is always paired to a decoder port) for the channel (only the first channel). Because only one audio encoder port is allocated per endpoint, it is together with the ESM data port in the endpoint's channel 1 port slot position of the Port Aud/ESM column. For **UCC** endpoint type, the channel 1 port slot position displays the allocated Call Classifier resource.
Ports ESM	The Expansion Service Module MMI data port. This field is always blank.
Sum Grp	Endpoint's assigned summer group number. The summer group port assignments are on screen 1.
Software	For Avaya use only.

status conference x endpoint y field descriptions — page 1

Field	Description
Endpoint	Endpoint-ID is a slot number associated with the endpoint entered on the conference forms.

Table continues…

Field	Description
Product	Product identification number obtained from the endpoint.
Manufacturer/Country	Manufacturer identification number and manufacturer's country code obtained from the endpoint.
Terminal Name	blank
Sum Grp	Summer group number to which this endpoint belongs and the VC Audio Level (L1) and Level 2 (L2) summer ports for this group. These fields have an entry only for conferences with over 6 participants.
Dial Out #1 Dial Out #2	Blank Blank
In Use	Is the endpoint currently participating in the conference or in process of connecting to the conference? • **y** — The endpoint is in use and is fully connected on all media in an active conference. • **c** — The endpoint is in use and is fully connected, however the endpoint has changed the conference audio or video capability or has changed the rate of the conference because of rate adaptation. This condition requires analysis of this endpoint's capabilities and mode fields to identify which capability was reduced. • **e** — The endpoint is in use but the endpoint had capability problems. The endpoint does not have one of the required capabilities (Vid, Bhl, MLP) to be a full participant. For MLP capabilities, see the T120 field. This condition requires analysis of this endpoint's capabilities and mode field to identify the missing capability. • **f** — The endpoint is in use but is disconnected from all media. This indicates that the endpoint has declared every required capability (channel/video/audio/data) but is not fully connected to all conference media at this time. This endpoint may be in the process of connecting, has failed to connect, or is not a valid video source. This condition requires analysis of this endpoint's capabilities and mode fields to identify the problem. • **n** — The endpoint was connected in a conference but has/was disconnected or attempted to connect to a conference but was unsuccessful. • **blank** — until the first call is made from/to the endpoint.
Enh BAS	Enhanced Basic Service Flag • **y** — The endpoint supports the enhanced BAS commands/caps • **n** — The endpoint only supports the basic BAS commands/caps
Chl	Data on the quantify and quality of channels (transfer rate)? • **y** — The endpoint has the required number of channels.

Table continues…

Field	Description
	• **e** — The endpoint has not declared support for the correct number of channels and cannot participate fully in the conference. • **n** — The endpoint has declared the correct number of channels, but every channel has not yet joined the conference, due to either a network or endpoint problem. • **blank** — Audio add-on endpoints always have a blank Chl field.
Aud	Does the endpoint have the required audio capability? • **y** — The endpoint has the required audio capability. Audio add-on endpoint always have the Aud field set to y once the endpoint has joined the conference. • **c** — This endpoint is PCM only, and it changed the video quality of the conference by changing the operating audio from G.728 to G. 711. If the administered audio mode is auto and the administered bandwidth is 112 kbps (56 k/channel) or 128 kbps (64 k/channel), the system starts out with the highest common audio of G.728. When the administered bandwidth is greater than 128 kbps, the system starts out with the highest common bandwidth of 7 kHz. • **e** — A PCM-only endpoint that did not have the capability of supporting the administered audio mode of G.728 (such as a data conference). G.278/G.711 endpoint that did not have the capability of supporting the administered audio mode of 7 kHz. Such endpoints operate with PCM audio and interwork with the current operating audio mode. • **blank** — The field is blank until the first call is made from/to the endpoint.
Vid	Does the endpoint have the required video capability and is receiving video? • **y** — The endpoint has the required video capability and should be receiving video if the Chl, Aud, and Dat fields are y. • **c** — It downgraded the conference's video quality - either from CIF to ACIF or by decreasing the frame rate. The conference video mode is set by default to CIF and if a QCIF-only endpoint joins the conference, then the entire conference is made to operate in QCIF, with the video clarity downgraded. Also, the conference frame rate is initially set to the highest frame rate that can then be reduced by any endpoint. If the conference video mode is not administered with upgrade capability, then if the video parameters for a conference have been **downgraded**, they are not **upgraded** until every endpoint disconnects from the conference. • **e** — The endpoint has not declared any video capability in its cap-set.

Table continues…

Field	Description
	• **n** — Audio only, not receiving video, possibly due to an audio or data problem. • **blank** — Audio add-on endpoint always have the Vid field set to `blank`.
Mlp	The state of the Control Link to the ESM (T.120 stack terminator), the endpoint MLP data capability, and the state of the data connection in the T.120 stack. This field value is always blank, indicating that the Data Mode for the conference is **none**, and therefore, the data does not apply, or the endpoint has never joined the conference.
Gx	Does the endpoint have the Still Frame Graphics capability? • **y** — This endpoint has this capability. • **e** — This endpoint did not declare this capability. The conference retains the still frame graphics capability when a non-compliant endpoint joins the conference. • **blank** — This endpoint has never joined the conference.
Rate Adpt	Rate adaptation/Interworking indicator. Values of 5 and 6 apply only to low-speed/high-speed interworking. Every other value applies only to rate adaptation. • **5** — A 56-kbps (low-speed) endpoint has joined a high-speed (128-kbps or above) conference. This endpoint is connected with audio-only capability, but is neither a valid video source nor destination. • **6** — A 64-kbps (low-speed) endpoint has joined a high-speed (128-kbps or above) conference. This endpoint is connected with audio-only capability, but is neither a valid video source nor destination. • **y** — This endpoint has joined the conference at the administered rate of 64 kbps, but (because rate adaptation to 56 kbps was triggered by another endpoint) this endpoint has successfully rate adapted to 56 kbps. • **c** — The administered bandwidth of the conference is 64 kbps and this endpoint has joined the conference at 56 kbps. The first 56-kbps endpoint that joins 64-kbps rate-adaptable conference triggers rate adaptation (see Join Time below). • **n** — A 64-kbps conference was triggered to rate adapt to 56 kbps by some other endpoint. This endpoint joined the conference at the bandwidth of 64 kbps, but encountered problems in rate adapting down to 56 kbps. This endpoint may have the audio and may be receiving video, but is not a valid video source. • **blank** — Rate adaptation was never triggered by any endpoints. So, if this endpoint is in use and connected, then it joined the conference at the administered bandwidth.
Bond Mode	Bonding Mode — blank.

Table continues…

Field	Description
	This field is blank for calls that are not related to bonding.
Ts	Indication of the talking state of the endpoint. • **t** — At the time the command was invoked, voice energy (talking) was detected from the endpoint. • **m** — At the time the command was invoked, the endpoint indicated to the MCU that it was muted. It is possible that an endpoint may mute, but not send any indication to the MCU. In this situation the MCU does not display a mute indication. • **M** — At the time the command was invoked, the endpoint's audio was muted via UDD/CRCS Agent interface. **M** displays when both the endpoint and the UCC/CRCS Agent have muted the endpoint audio. • **S** — At the time the command was invoked, the endpoint's audio was muted because of solo-audio state set by UCC/CRCS Agent. While in solo-audio state, new endpoints joining the conference are automatically muted. • **blank** — At the time the command was invoked, voice energy (talking) was not being detected from the endpoint.
Vs	Indication of the MCU video state for this endpoint. For quad-screen conferences, an asterisk (*****) is affixed before the value of Vs to indicate that an endpoint is currently part of the mixed image. A pound (**#**) may be affixed before the value of Vs to indicate that an endpoint was fixed to be in the mixed image (via administration or UCC/CRCS Agent), but instead, a Fill video is shown in its place. This occurs when the video of an endpoint that is fixed in a quadrant cannot be used as a video source because the endpoint is currently not joined to the conference, has suppressed its video, or has invalid video to be the video source. Notice that at most four endpoints have an ***** or **#** affixed before the Vs field value. For quad-screen conference in VAS mode, the mixed image is broadcast to every endpoint. For quad-screen conference in presentation mode, the mixed image is return video to the presenter. • **a** — This value applies only to quad-screen conferences. ***a** indicates that an endpoint is part of the current mixed image and is fixed in one of the quadrants via administration. ***a** indicates that the endpoint is fixed in a quadrant but is not currently connected (Fill image displays). • **b** — For full-screen conference it indicates that at the time the command was invoked, this endpoint's video was being broadcast to other sites. This conference was in VAS, broadcast, or presentation mode. For quad-screen VAS conference it is prefixed with an asterisk (*****) and indicates that this endpoint's video is part of the mixed image because of VAS. For quad-screen presentation

Table continues…

Field	Description
	conferences, **b** (without an asterisk) identifies the presenter as the broadcaster. • **B** — At the time the command was invoked the endpoint's video was being broadcast to other sites because of the UCC roll call feature. UCC roll call feature can only be performed in full-screen mode. • **c** — At the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in chair mode and the broadcaster was designated by the chair. Chair features can only be performed in full-screen mode. • **B** — At the time the command was invoked the endpoint's video was being broadcast to other sites because of the UCC roll call feature. UCC roll call feature can only be performed in full-screen mode. • **i** — At the time the command was invoked the endpoint was not a valid video source. For continuous presence conference, if this endpoint is fixed in a particular quadrant, a pound (**#**) is affixed before **i**. • **r** — For full-screen conferences, at the time the command was invoked the endpoint's video was the return video to the broadcaster. For continuous presence conference in presentation mode, ***r** represents a VAS quadrant that is part of the mixed image. • **R** — At the time the command was invoked, the endpoint's video was the return video to the broadcaster because of the UCC browse feature. UCC Browse feature can only be performed in full-screen mode. • **s** — At the time the command was invoked this endpoint's video was suppressed at the request of the endpoint. For continuous presence conference with fixed quadrant participants, if this endpoint is fixed in a particular quadrant a pound (**#**) is affixed before **s**. • **S** — At the time the command was invoked this endpoint's video was suppressed via UCC/CRCS Agent interface. For continuous presence conference with fixed quadrant participants, if this endpoint is fixed in a particular quadrant, a pound (**#**) is affixed before **S**. **S** is displayed when the endpoint and the UCC/CRCS Agent have suppressed the endpoint video. • **u** — For full-screen conferences, at the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in VAS mode and the broadcaster was designated by the UCC/CRSCS Agent interface. For quad-screen conferences, it indicates that UCC/CRCS Agent designated this endpoint as fixed in a quadrant. An asterisk (*****) is affixed before **u** if the endpoint is currently part of the quad image, and a pound (**#**) is affixed if the endpoint is not currently joined. • **U** — Applies only to quad-screen conference and indicates that UCC/ CRCS Agent designated a quadrant as VAS. An asterisk (*****) is

Table continues…

Field	Description
	affixed before **U** to indicate that this endpoint is part of the current quad image. • **v** — At the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in VAS mode but the endpoint has asked to be a broadcaster via **See-Me** request and was granted a MCV (Multipoint Command Visualize) token. The See-Me feature is only performed in full-screen mode. • **blank** — At the time of the request the endpoint's video was not broadcast, return, video, or part of the mixed-image, but it is a valid video source.

status conference x endpoint y field descriptions — page 2

Field	Description
Join Time	Time (in 24-hour notation) when the channel joined the conference.
Drop Time	The endpoint is idle if the first channel has a drop time.
Drop Reason	The reason for the channel's disconnect: • **2-pri** — This drop reason occurs when an administration error causes a mismatch in primary-secondary designation for a cascade link. This mismatch shows that both MCUs are administered as primaries (see Cascading for a description of primary-secondary compatibility). • **2-sec** — This drop reason occurs when an administration error causes a mismatch in primary-secondary designation for a cascade link. This mismatch shows that both MCUs are administered as secondaries (see Cascading for a description of primary-secondary compatibility). • **Agent** — The reservation agent has caused the call to disconnect (for example, the agent has changed a connected dial-out destination number). • **Bandwidth** — mismatch between a call and the conference it attempted to join. For example, a 56-kbps call attempted to join a 64-kbps conference that does not permit rate adaptation. • **BondHshake** — Bonding handshake drop reason can be caused due to the following reasons: information channel parameter not supported or invalid, parameter negotiation terminated out of sequence, timer expired because of the secondary channels did not establish, or BONDing framing was not detected for one of the other channels. • **Busy** — This dial-out drop reason occurs when the MCU detects that the conferee's terminal equipment is busy. This drop reason is detected by an ISDN cause value (for example, h0). See Dial-out for a description of CPTR usage.

Table continues…

Field	Description
	• **Chair** — disconnected the endpoint, using either Chair Command Disconnect (CCD) or Chair Command Kill (CCK) signals. • **Conf End** — The conference was ended due to reaching stop time for a reserved conference or due to an active conference being converted to file. • **Endpoint** — Clearing received from DS1. The disconnect came from the endpoint. The endpoint notified the MCU that it intended to disconnect. • **Far-end** — Clearing received from DS1. The disconnect came from either the network or the endpoint. • **Handshake** — Either framing was never found (the endpoint could not complete initialization: problems finding Frame Alignment Signal (FAS), Multi Frame Alignment (MFA) and getting a corrected coded cap-set) or framing was lost for some time (over 40 seconds) and the endpoint was disconnected. • **IDtimeout** — The MCU has not received response to the UIN/password Query from the H.320 user after three attempts. Each attempt has a system administered timeout period. • **Internal** — MCU has a problem allocating trunk resources necessary to route the dial-out call for the specified dial-numbers. This problem can be associated with routing pattern or trunk associated translation (for example, TAC specified in the dial-out number or routing pattern points to a trunk group without members), or it can indicate a lack of trunk resources (for example, every trunk member is maintenance busy or every in-service member is busy on a call). • **Network** — Clearing received from DS1. The disconnect came from the network. The endpoint that had the disconnect notification capability disconnected without notifying the MCU. • **No-ring** — This dial-out drop reason occurs when the call has been up for 30 seconds and no ringing is detected. • **Not-MCU** — The dial-out destination number(s) of the **CAS** extension has terminated to a number that is not a dial-in cascade MCU extension. • **Password** — Either the user entered the wrong password or the audio add-on user did not enter it within the specified time period. Note that the audio add-on user gets one attempt to enter a correct password and inter-digit timing for each digit (that is, about 10 seconds between digits). • **Pre-AnsDrop** — The call disconnected before answer by an endpoint. The cause of the disconnect may be the network, an endpoint, or a terminal adapter. This drop reason is different from **No-answer**, which indicates that a 60-second timeout occurred while alerting. In this case, the call drops before the 60-second timer has

Table continues…

Field	Description
	expired. Some busy endpoints connected through terminal adapters display this behavior. • **Resource** — MCU could not provide resources (VC or MMI) when the call arrived or lost the resources during the call. This could be due to them being Out of Service, busied out by craft, or being used by system maintenance. This drop reason could also occur if the DS1/ MMI cable is disconnected. If there was a resource problem when the call arrived, it would get reorder (fast busy) and not get disconnected by the MCU. • **Reorder** — This dial-out drop reason occurs when the MCU detects that there are no available trunks in the network to place the call. This drop reason is detected by MCU CPTR resources. See Dial-out for a description of CPTR usage. • **System** — An MCU restart (level 2) disconnected every call. • **UIN-Inv** — The user entered an invalid User Identification Number. • **Unknown** — The system could not determine the cause of the disconnect. • **Wrong-num** — This dial-out drop reason occurs when the MCU detects the wrong destination number was dialed. This drop reason is detected by MCU CPTR resources SDN cause value. See Dial-out for details. • **UCC** — controller intentionally disconnected the endpoint.
Drop Code	A detail code complementing the Drop Reason (see above). Additional bonding related information may be obtained from supplementary Bonding Drop Codes described above.
AC Num	Administered Connection Number - from 1 to 128. AC number can be used to further diagnose a problem by combining status conference information with **`status administered connection`** and data stored in the error and alarm logs.
Ports Trunk	The data endpoint that the channel is using.
Ports Video	The MMI port for the channel.
Ports Aud	If the endpoint type is not **UCC**, the VC audio encoder port (which is always paired to a decoder port) for the channel (only the first channel). Because only one audio encoder port is allocated per endpoint, it is together with the ESM data port in the endpoint's channel 1 port slot position of the Port Aud/ESM column. For **UCC** endpoint type, the channel 1 port slot position displays the allocated Call Classifier resource.
Ports ESM	The Expansion Service Module MMI data port. This field is always blank.
Ports Bonding	The MMI port used for Bonding for the channel.

Table continues…

Field	Description
Fr Err	Frame error counter. A circular hex counter (0-FF) to indicate the occurrence of framing errors.

status conference x endpoint y field descriptions — page 3, Conference Info

Field	Description
Conference Info Applies mostly to full-screen conferences.	
Broadcaster	Indicates the endpoint number that is the current broadcaster. Applies to full-screen and quad-screen presentation mode conferences. • **Broadcast** — a broadcast mode broadcaster. • **Chair** — the broadcaster was designated by the chair. • **See-Me** — the broadcaster is a result of MCV request from an endpoint. • **Presenter** — a presentation mode broadcaster. • **Rollcall** — the broadcaster was designated by the UCC via the Rollcall feature. • **UCC** — the broadcaster was designated by the UCC. • **VAS** — Voice Activated Switching broadcaster.
Next Broadcaster	Indicates the endpoint number that is selected to be the next broadcaster.
Return Vid	Indicates the endpoint number that is the current return video. The return video can be qualified with the following keywords: • **blank** — the return video is the previous broadcaster forced to be return video because of VAS, action by Chair, action by UCC, or endpoint MCV request. The broadcaster qualifier identifies which action forced this endpoint to become return video. • **Autoscan** — auto scan return video. This is true only when conference mode is broadcast with auto scan. • **Browse** — the return video was designated by the UCC via the Browse feature. • **VAS** — a Voice Activated Switching return video.
Next Return Vid	Indicates the endpoint number that is selected to be the next return video. MCU

status conference x endpoint y field descriptions — page 3, Mode Commands/ Communication Modes

This is a collection of both incoming and outgoing bandwidth allocations for the multiplex. The Incoming data is the rate at which the MCU thinks the endpoint is communicating based on the Bit-rate Allocation Signal (BAS) codes received from the endpoint/codec and the capabilities the MCU has declared. The Outgoing data is the rate from the MCU toward the endpoint.

Field	Description
Conf	The desired conference operating mode. This may be different from the endpoint in (EPT-IN) or endpoint out (EPT-OUT) modes.
Cmd	labels for the various types of mode commands
Stat	Compatibility of conference mode and the incoming mode. • **y** — indicates mode compatibility • **n** — indicates that the modes are not compatible
EPT-IN	Communication modes coming in from an endpoint.
EPT-OUT	Communication modes sent out to an endpoint based on the number of channels connected and the capabilities of the endpoint.
XRate	One of the supported transfer rates. XRATE may be 64 when the endpoint is just dialing in, or in the event of problems. It implies that only one B-channel is being used.
Audio	Audio rate (kbps bandwidth) of the conference and the endpoint must be the same but not necessarily their mode. When the audio rate of the conference and the endpoint are different the endpoint's audio will interwork but the endpoint's video will be invalid. MCU may or may not send video to such an endpoint. Other possible AUDIO mode values include **neutral** (neutralized I-channel) and **Au-off**, **Frm** (no audio signal) which never match conference mode and are not supported by MCU.
56/64	The 56/64 field is **derestrict** when operating at per-channel rates of either 64, 128, 192, 256, 320, 384, 512, 768, 1472, 1536, or 1920 kbps. It is **restrict** when operating at rates of either 56, 112, 168, 224, 280, 336, 448, or 672 kbps. Note that if the conference is configured for N x 56-kbps operation, the endpoint may signal either via capabilities or modes that is operating at the proper rate. In such a case, even when we receive derestrict command which does not match the conference communication mode of **restrict**, if the capability indicates **restrict** (**MISC** capability has **restrict** displayed on Page 4) the **STAT 56/64** is **y** to indicate 56/64 compatibility between the conference and the endpoint.
Video	The Video mode: **H.261** (recommended), **H.CTX** (proprietary), **H.CTX+** (proprietary), or **SG4** (proprietary) indicate that video is on in the direction indicated; **video-off** when the video is off.
Mlp	Multi Layer Protocol data mode. When **Data Mode** is administered as **any-mlp** or **ww-pcs**, the MLP mode should be **var-MLP**. Other values will affect video status. The MLP mode should be **MLP-off** when Data Mode is administered as **none**. Again, other values in this mode will affect video status.
H_Mlp	The High Speed MLP mode. The HMLP mode should be **H-MLP-off**. Other values in this mode will affect video status.

Table continues…

Field	Description
LSD	Low Speed Data mode. The LSD mode should be **LSD-off**. Other values in this mode will affect video status.
HSD	High Speed Data mode. The HSD mode should be **HSD-off**. Other values in this mode will affect video status.
CRYPT	Encryption mode. The CRYPT mode should be **encrypt-off**. Other values in this mode will affect video status.
S/M	Single-/multi-channel interoperability mode. **6B-H0-comp** indicates that the sender is interoperating multiple channels and a single channel (for example, 6B and H0). **Not-comp-6B-H0** indicates that the sender is not interoperating between 6B and H0. Normally this value is **Not-comp-6B-H0**. Other values in this mode will affect video status.

status conference endpoint field descriptions — page 3, Endpoint Misc Info

EPT MISC contains miscellaneous states and counters for an endpoint. The flags can be **y** or **n**. The counters start with initial value of 0x00, they increment to 0xff, and then wrap around to 0x01. **AIM** and **VIS** are BAS commands which can be sent as input (I) to MCU from an endpoint or as output (O) from MCU to an endpoint.

Field	Description
AIM	Audio Indicate Muted. **y** on input (I) indicates that this endpoint has muted its audio. MCU will not VAS to an endpoint displaying mute indicate. **n** on input indicates that this endpoint has not muted (only if endpoint audio mode is turned on). **y** on output (O) indicates that every other endpoint in the conference has muted its audio (have sent AIM to MCU). MAC in turn tells this endpoint (by sending it AIM) that there is no audio output from MCU. **n** on output indicates that there is an audio path open across the bridge.
VIS	Video Indicate Suppressed. **y** on input (I) indicates that this endpoint has suppressed its video (indicated video is muted). **y** on output (O) indicates that the MCU is not sending video to this endpoint because there is no video broadcaster (broadcaster has not joined or broadcaster's video is not valid).
MIS	Multipoint Indicate Secondary-status.

Table continues…

Field	Description
	This command is only sent as output (O) to an endpoint. n indicates that the endpoint is viewed as capable of being a valid source (although not necessarily at this moment). **n** is correct for video. **y** indicates that MIS was sent to an endpoint and that this endpoint is viewed as a secondary endpoint. The endpoint is included in the audio portion of the conference but not the video portion. Video will not be sent.
MCV	Multipoint Command Visualize. This command is only sent as input (I) from an endpoint. **y** indicates that an endpoint has requested to become a broadcaster. This is used during Still Frame Graphics and to force **presentation** mode.
TALK	Multipoint Command Visualize. This command is only sent as input (I) from an endpoint. **y** indicates that an endpoint has requested to become a broadcaster. This is used during Still Frame Graphics and to force “presentation” mode.
VRCV	**y** indicates if the endpoint is receiving video (MMCH is sending video to the endpoint). The VRCV counter indicates the number of times video was sent/not sent to this endpoint.
BCTK	Applies to single screen and quad-screen presentation mode conferences. **y** indicates that the endpoint is the video broadcast source. The BCTK counter indicates the number of times this endpoint was the video broadcast source.
RTTK	Applies to single screen conferences. **y** indicates that the endpoint is the return video source. The RTTK counter indicates the number of times this endpoint was the return video source.
BCLS	Applies to single screen and quad-screen presentation mode conferences. **y** indicates that the endpoint is watching the video of the broadcast source.
RTLS	Applies to single screen conferences. **y** indicates that the endpoint is watching the video of the return source.
HYPR	**y** indicates hyperactivity from an endpoint (MCU isolated endpoint from the MCU conference due to **thrashing** behavior) and affects endpoint’s status as a video source (for 5 seconds of hyperactivity timer). The HYPR counter indicates the number of times this endpoint was hyperactive.
DMUTE	**y** indicates that the decoder was muted by the VC board or the software in the MCU. VC board mutes the decoder when it loses MMI or endpoint framing is lost, when it receives an invalid audio code word, and when endpoint is hyperactive. The only time that the MCU software mutes the decoder of an endpoint is to mute every endpoint, other than the broadcaster, when a mode of a conference is **broadcastw/scan** (broadcast with auto scan). The DMUTE counter indicates the number of times this endpoint’s decoder was muted by the VC board.

Table continues…

Field	Description
VFMT	The video format applicable only to quad-screen conferences. Always **n**, indicating QCIF format.
H.261	**y** indicates video framing loss. The H.261 counter indicates the number of times the framing was lost.

status conference endpoint field descriptions — page 3, Frame Alignment Word Info

Frame Alignment Word (FAW) includes channel information for the communication paths labeled CHL 1 and 2. For 2B calls, both CHL 1 and 2 are used. For 1-channel calls (at rates of 112, 128, 168, 196, 224, 256, 280, 320, 336, 384, 768, 1472, 1536, and 1920 kbps), only CHL 1 is used. **A-OUT**, **A-IN**, **M-FRM**, **MFA**, and **MFN** are flags with values of **y** or **n**.

Field	Description
A-OUT	MCU has endpoint framing.
A-IN	Endpoint has MCU framing.
M-FRM	Multichannel frame alignment is present (alignment of both channels in 2B).
MFA	Multiframe alignment word is present (required in 2B call).
MFN	Multiframe numbering is present (required in 2B call).
FAS	Frame Alignment Signal (FAS) channel number (1 or 2). This number should match the column header.
MCUFAL	MCU Frame Alignment Loss (MCUFAL). A counter of the number of times the MCU indicates to the endpoint that it has lost endpoint FAW or multichannel synchronization (M-FRM). The MCU a-bit toggles when the MCU gains or loses endpoint multichannel synchronization. This counter starts with an initial value of 0x00, increments to 0xff, then wraps around to 0x01. The MCUFAL count is also shown in the Fr Err field.
FEFAL	Far End Frame Alignment Loss (FEFAL). A counter of the number of changes the MCU detects in the endpoint's a-bit (A-OUT). The endpoint a-bit toggles when an endpoint gains or loses MCU framing. This counter starts with an initial value of 0x00, increments to 0xff, then wraps around to 0x01.

status conference endpoint field descriptions — page 4

Fields on this page only when an endpoint declares the specific capability. For example, if an endpoint does not declare the VID H.CTX capability, the H.CTX field does not display.

Field	Description
VID	Provides information about the type of video and frame rate the endpoint supports.

Table continues…

Field	Description
	vfmt — does not display if the endpoint has no video capability. Every value is blank if there is an active call or if this is an audio-only endpoint. Otherwise, values for this field include: • **FCIF** — full CIF. • **QCIF** — quarter CIF. Support of CIF implies support of QCIF. In general, for larger screens, CIF displays sharper resolution video, which ZCIF is blocked, but may run at higher frame rates and less clear. The differences are less observable on very small displays. • **cfps** and **qfps** — maximum frame rate (frames/second) at which the endpoint can receive video for CIF and QCIF operating modes. CIF frame-rate values are 30 fps, 15 fps, 10 fps, and 7.4 fps. If the endpoint does not support CIF (that is, the **vfmt** field is QCIF), the **cfps** value should be blank. • **da_sfg** — indicates support for H.261 Still Frame Graphics transfers. • **H.CTX**, **H.CTX+** and **SG4** — proprietary video format capabilities. • **SG4_sfg** — indicates support for SG4 Still Frame Graphics.
MISC	The restrict field is one way for an endpoint to indicate that it is operating at 56 kbps per channel. Another way is the 56/64 command mode with restrict. An endpoint on a 56-kbps conference must send one or both of the 2 indications that they are operating at 56 kbps before they become a video source in a 56-kbps conference. If they signal either way that they are operating at 56 kbps in a 64- or 384-kbps conference, they are an audio-only source, but the MCU continues to send Selected Communication Mode (SCM) toward them when possible. A MISC capability of derestrict and a 56/64 command of derestrict together indicate that an endpoint is operating at 64 kbps. If either is restrict, the conference operates at 56 kbps. Other field values include: • **dcomp** — indicates support for WorldWorx PCS data compliance. • **mbe** — indicates support for Multi Byte Extension. MBE capability is used for the exchange of passwords, terminal names, and other special capabilities, such as, support of WorldWorx PCS specific features. • **cic** — Chair Indicate Capability. Indicates chair control capability.
XR	Transfer rate capabilities are statement about the speeds at which the endpoint can operate over the current connection and operate a Px64 Multiplex. For a 384-kbps (H0) call, the endpoint sends its capabilities to indicate 384-kbps support, which displays as **384**. On a 336-kbps call, the endpoint must signal 384-kbps support. If an endpoint does not indicate support for 384 kbps on a 384-/ 336-kbps conference, the

Table continues…

Field	Description
	MCU provides Audio Only Communications Mode (ACOM). For a 2B conference, the MCU sets the rate to 2x64, expecting the endpoints to do likewise (**64x2** is displayed; if this is not displayed, there is no 64x2 capability). Endpoints may occasionally take 2x64 (or the current channel rate: 384, 768, 1472, 1536) out of their capability. This is Mode 0 forcing and is part of normal procedures. The MCU will provide AOCM if the endpoint does not signal support matching the configuration of the conference.
AUD	The audio fields are statements of the audio protocols that the endpoint supports. **711m** and **711a** are PCM (G.711) and support Mu and A-law, respectively, and at least one is required of endpoints. The **g728** field indicates whether G.728 is supported (LB_CELP). This value depends upon the type of the endpoint and how that endpoint is currently configured. The **g722_48** field indicates endpoint support for G.722 (7 kHz) at both 48 and 56 kbps. Therefore, **g722_48** indicates that the endpoint supports G.722 audio at both rates. The **g722_64** field indicates endpoint support for G.722 at 64 kbps in an unframed (not supported by the MCU) mode.
LSD	The LSD fields indicate the capabilities for Low Speed Data conferencing.
HSD	The HSD fields indicate the capabilities for High speed Data conferencing.
MLP	The MLP fields indicate the capabilities for Multi Layer Protocol Data capabilities.
HMLP	The HMLP fields indicate the conference's capability for High Speed MLP data conferencing.

status conference endpoint field descriptions — page 5, Endpoint Call Status Information

This screen summarizes such call-related status as per-channel join counts, join/drop time, drop reason, drop code, and auxiliary bonding drop code. It also contains a drop code and software fields from the previous call. The data on the page is always retained. The Endpoint Call Status Information section groups together call-related fields. The Join Count field is described below, and other fields are described in the following field description tables.

Field	Description
Join Count	Shows the number of times this endpoint joined this conference during this conference session. This counter starts with 0, can increment to 64, and wraps around back to 1.

status conference endpoint field descriptions — page 6, Administered Connections

This screen summarizes information about the administered connections associated with this endpoint. This data can be viewed while the conference is active.

Field	Description
Dial-Out Number	The actual numbers that are dialed out by the administered connections for each channel in the call. Note that the dial Out #1 and #2 on page 1 of the forms display the DCP endpoint number. This is particularly useful with bonding dial-out calls.
Connection State	Indicates the current call state of the AC. The following are connection states associated with dial-out ACs: • **enabled** — transient in nature and indicates that an AC is about to enter the attempting to connect state. • **disabled** — this may mean one of three things: - The AC has reached an administered retry threshold, and all retries are stopped. Verify this by checking the error log and checking whether an error type of 9 is logged against the AC. - The AC was in a connected state and the far end disconnected. - The initial channel call has not yet connected. No dial out call attempt is made for the additional channel(s) until the initial channel has reached a connected state. • **not scheduled** — transient in nature and indicates that an AC is about to enter the **attempting to connect** state. • **waiting to retry** — the AC is inactive (sleeping) and waiting for the retry timer to expire. Once the timer expires, the AC sends a dial out call and enters the **attempting to connect** state. ACs in this state indicate that the dial out call has failed at least once. • **attempting to connect** — the AC is active on a call, but the call has not yet connected. • **connected** — the call associated with the AC has been answered and join cut-through to the conference.
Retry Count	Number of retries have been attempted for this AC during this join attempt. This field does not clear when the AC connects. This field clears when a new join attempt is made via a Redial feature. Note that this is different from the Join Count which counts the number of times the channel joined the conference during this conference session.
Failure Cause	ISDN or CPTR cause value (values lower than 0x7f) recorded when the last dial out call was dropped. Values above 0x7f are generated internally. The following table lists all possible failure cause values displayed by this field and its associated description. This value is logged in the error log and is displayed with **`display errors`**. Err Type is displayed as a decimal.

Status AC — Failure Cause Values

Failure Causes	Description
0x00 (0t0)	Not applicable

Table continues…

Failure Causes	Description
0x01 (0t1)	Incorrect destination address
0x02 (0t2)	Reason unknown
0x06 (0t6)	Reason unknown
0x10 (0t16)	Normal call clearing
0x11 (0t17)	Endpoint not available
0x12 (0t18)	ISDN timer expired
0x15 (0t21)	Reason unknown
0x12 (0t22)	Destination address changed
0x1C (0t28)	Bad destination or access denied
0x1D (0t29)	Access denied
0x1F (0t31)	Reason unknown
0x22 (0t34)	Trunks unavailable
0x26 (0t38)	Temporary or facility failure
0x29 (0t41)	Temporary or facility failure
0x2A (0t42)	Resources unavailable
0x2C (0t44)	Resources unavailable
0x32 (0t50)	Access denied
0x34 (0t52)	Access denied
0x36 (0t54)	Access denied
0x3A (0t58)	Resources unavailable
0x41 (0t65)	Required capability not implemented
0x42 (0t66)	Required capability not implemented
0x45 (0t69)	Required capability not implemented
0x51 (0t81)	ISDN protocol error
0x52 (0t82)	Required capability not implemented
0x58 (0t88)	Incorrect destination number
0x60 (0t96)	ISDN protocol error
0x61 (0t97)	ISDN protocol error
0x62 (0t98)	ISDN protocol error
0x64 (0t100)	ISDN protocol error
0x66 (0t102)	ISDN timer expired
0x7f (0t127)	Reason unknown
0xC2 (0t194)	Ring no answer
0xC8 (0t200)	Hi and dry – no feedback detected
0xC9 (0t201)	Cascade link administered wrong
0xCA (0t202)	CPTR not available to detect failure

configuration

list configuration

Use **list configuration** to generate a hardware configuration report. The report includes the type, code, suffix, and vintage of the requested circuit packs as installed in the switch, and every assigned port on the circuit packs.

To display SN circuit packs, use the all, carrier, or board qualifiers.

Syntax

```
list configuration [ all | board location | carrier c | circuit-pack board-code | control
| ds1 | hardware-group | port network n | stations | trunks ][ schedule ]
```

all	Displays all the boards.
board *location*	Displays every assigned port on a circuit pack specified by cabinet, carrier, and slot.
carrier *c*	Displays every circuit pack and assigned port on a specified carrier.
circuit-pack *board-code*	Displays all the requested circuit packs in the system that are inserted. AWOH and unplugged circuit packs are not listed.
control	Displays every circuit pack located in the control complex.
ds1	Displays every DS1 circuit pack (TN722, TN767, and TN464) administered and/or every physically inserted port carrier of the system.
hardware-group	Displays every circuit pack administered and/or physically inserted in every port, switch node, and control carrier of the system.
port network *n*	Displays every circuit pack located in a specified port network. However, Circuit packs in switch node carriers do not display. **list cabinet** gives the port network number(s) associated with a particular cabinet. To display SN circuit packs, use the **all**, **carrier**, or board qualifiers.
stations	Displays every circuit pack that can be assigned stations, including DS1 circuit packs for remote stations. Every assigned port is displayed. See **list configuration stations**.
trunks	Displays every circuit pack that can be used for administering trunks. Every assigned port is displayed.
schedule	Specify a time to run the command.

list configuration field descriptions

Field	Description
Board Number	Location of the circuit pack
Board Type	Type of board
Code	The TN or UN code and suffix of the circuit packs
Vintage	The vintage number, or the hardware (HW) and firmware (FW) vintages of the circuit pack. Also: • **no board** — the circuit pack is administered but not physically installed • **conflict** — the circuit pack administered to the slot differs from the circuit pack that is physically installed • **no link** — the T1 link is down to a DS1 circuit pack
Assigned Ports	Each port on the circuit pack is represented by a position corresponding to its circuit number in ascending order from left to right. Two rows for circuit packs with more than 8 ports. The assigned ports for list configuration ds1 do not display. Identifies the current status of the port that corresponds to the position: • **01–32** — the circuit number of an assigned port • **mj** — the port is assigned as an external device major (**mj**) alarm port • **mn** — the port is assigned as an external device minor (**mn**) alarm port • **p** — psa (personal station access) • **t** — the port is not assigned and is supported by Terminal Translation Initialization. Activate the port with the TTI association sequence. • **u** — the port exists but is unassigned. Each port on a TN556 ISDN-BRI circuit pack can have two BRI endpoints. BRI ports once when assigned only one endpoint and twice when fully configured with two endpoints.

list configuration ds1 field descriptions

Field	Description
Location	Location of the DS1 circuit pack
Code	The TN or UN code and suffix of the DS1 circuit packs
Vintage	The vintage number, or the hardware (HW) and firmware (FW) vintages, of the circuit pack. Other values that may be shown: • **no board** — The circuit pack is administered but not physically installed

Table continues…

Field	Description
	• **conflict** — The circuit pack administered to the slot differs from the circuit pack that is physically installed • **no link** — The T1 link is down to a DS1 circuit pack
Signaling	Displayed for **`list configuration ds1`**. Values are the same as the signaling mode administered for the ds1 circuit pack, or **none** if the circuit pack is not administered.
Name	Displayed for **`list configuration ds1`**. Values are the same as the signaling mode administered for the ds1 circuit pack, or **none** if the circuit pack is not administered.
CSU MOD	Displayed for **`list configuration ds1`** option. Contains the identification number of the Integrated CSU module present on the DS1 circuit pack (TN767E or later/TN464F or later), or **none**. **unknown** — the circuit pack is a TN464E or TN767D **n/a** — the circuit pack is a TN464D or TN767C or earlier suffix DS1 board

list configuration media-gateway

Use **`list configuration media-gateway`** to see all the assigned ports on the media modules for the specified gateway.

Syntax

```
list configuration media-gateway x
```

x Gateway number.

list configuration media-gateway field descriptions

Field	Description
Module Number	Physical location of the ports. Vn is the module number (V1–V4) or the virtual slots V8 or V9.
Module Type	Type of Avaya Media Module in the slot. If an administered Media Module is in conflict with the inserted Media Module, a pound sign (#) is displayed to the left of the Module Type field on the Media Gateway screen.
Code	Media Module code. Displays the value as S8300E for an S8300E ICC media module.
Vintage	Hardware and firmware vintage of the module. No code or vintage is listed for the virtual media modules in slots V8 and V9.

Table continues…

Field	Description
Assigned Ports	Status of ports associated with Media Module/slot. Blank means no assigned port.

list configuration power-supply

Use **list configuration power-supply** to see information about the power supplies in a specified G650 stack with a TN2312BP later IPSI circuit pack.

Syntax

```
list configuration power-supply cabinet |carrier
```

cabinet Cabinet location.

carrier Carrier location.

list configuration power-supply field descriptions

Field	Description
Location	The power supply cabinet/carrier/slot
Power Supply Serial Number	The serial number of the power supply
Power supply Make/Model Number	The apparatus code and hardware revision number of the power supply. If the system cannot communicate with the power supply, or if the power supply is removed from the carrier, this field contains the message: `power supply not present`.
SAP®	Part number SAP is a registered trademark of SAP America, Inc.
Power Supply Firmware Version	The version number of the power supply firmware (10 characters)

list configuration software-versions

Use **list configuration software-versions** to display:

- software version numbers and compatibility indexes of the software load modules stored in system memory (RAM)
- the dates and times when translation and announcement data were last saved
- information about any software update files that have been applied to the system

Syntax

```
list configuration software-versions [ memory-resident ][ schedule ]
```

memory-resident Specifies display of RAM-resident files.

schedule Specify a time to run the command.

If the memory card contains a core dump file, fields for tape or memory card data display — **coredump**. When a core dump is present, all other files on the device are marked invalid.

If the memory card cannot be read at the time the command is entered, the relevant fields display — **no tape or memory card**. (This does not indicate that the system does not recognize the presence of the device.)

list configuration software-versions field descriptions

Field	Description
Software Version	Information related to the current software-load module stored in memory
Memory Resident	Version number of the RAM-resident load module
Disk Resident	The last date and time that translation data was saved to disk. This date is read from disk, and is blank if the disk is not installed.
Translation Data	Information related to the translation files as stored in memory and the disk.
Memory Resident	Date and time marked on the disk when translation data was last read into memory. This is stored in memory and is not modified by changes to translation data. Date invalid is displayed when the timestamp does not contain the expected information.
Disk Resident	The last date and time that translation data was saved to disk. This date is read from disk, and is blank if the disk is not installed.
Disk Second Copy	The last date and time that translation data was saved to disk. This date is read from the second copy of the file on the disk.

list configuration stations

Use **`list configuration stations`** to see every circuit pack that can be assigned stations, including DS1 circuit packs for remote stations. Every assigned port is displayed.

Syntax

```
list configuration stations
```

list configuration stations field descriptions

Field	Description
Board Number	Physical location of the port.
Board Type	Type of circuit pack in the slot.
Code	Circuit pack TN code and suffix.
Vintage	Hardware and firmware vintage of the circuit pack.
Assigned Ports	Status of ports associated with the circuit pack/slot. Blank means no assigned port.

craft2

enable craft2

Use **enable craft2** to create a second craft login assigned to Profile 3. Only one login in addition to craft can be enabled to use Profile 3 at a time.

To change the name of the second craft login, disable the current login (disable craft2) and enable a new one.

Only logins assigned to profiles 0 (init), 1 (inads), and 2 (dadmin) can run this command.

Syntax

```
enable craft2 [xyz]
```

xyz The name of the second craft login.

disable craft2

Use **disable craft2** to remove the second craft login assigned to Profile 3.

Only logins assigned to profiles 0 (init), 1 (inads), and 2 (dadmin) can run this command.

cti-link

busyout cti-link

Use **busyout cti-link** to busyout a specified endpoint for a link that is administered on the AESVCS Administration page of the IP Services screen. An ASAI adjunct link provides connectivity to an ASAI adjunct (for example, CentreVu CT), which is connected to an Ethernet LAN.

See **status link** for more details on links.

Syntax

```
busyout cti-link  link
```

link Link number (1–8)

Feature interactions for busyout cti-link

- All ASAI service is disabled.

- A Warning alarm is generated even if more severe CTI link (for example, adj-ip) alarms are present.
- Periodic and scheduled tests continue to run. No alarms more severe than a Warning are generated until the CTI link is released from busyout.
- The release of CTI link from busyout retires all alarms.
- If a problem still exists, background maintenance generates new alarms within a few minutes.

change cti-link

Use the **change cti-link** command to modify the fields associated with the CTI link screen. You can use this command only if you enable the **ASAI Link Core Capabilities** field or the **Computer Telephony Adjunct Links** field on the System Parameters Customer Options screen.

Syntax

```
change cti-link n
```

n the Computer Telephony Integration (CTI) link number

change cti-link field descriptions — page 1

Field	Description
COR	Use this field to specify the Class of Restriction (COR) number.
CTI Link	Use this field to specify the CTI link number.
Extension	Use this field to specify the extension number assigned to the CTI link.
Name	Use this field to specify the alphanumeric characters for identifying the CTI link.
Port	Use this field to specify a port for an Adjunct-Switch Application Interface (ASAI) or Adjunct Links (ADJLK) CTI link. The following are the character specifications for ports: • 01 to 64: the first character and the second character represent the cabinet number • A to E: the third character represents the carrier • 01 to 20: the fourth character and the fifth character represent the slot number • 01 to 32: the sixth character and the seventh character represent the circuit number X: if the **Port** field is set to X, there is no hardware associated with the port.
Type	Use this field to specify the type of the CTI link. The available types of CTI links are: • **ADJLK**: The system no longer supports the ADJLK type.

Table continues…

Field	Description
	• **ADJ-IP**: Computer Telephony Adjunct Links. ASAI adjunct links administered without hardware. • **ASAI**: The system no longer supports the ASAI type. • **ASAI-IP**: The associated adjunct controls all the agent logins and logged-in agents can use their data terminal keyboards to perform telephone functions, for example, change work state. **ASAI** links are administered without hardware.
CRV Length	Use this field to specify the length of the Call Reference Value (CRV) for each interface. This field is available only for ASAI or ADJLK CTI links types. The system no longer supports the ASAI and ADJLK types. You cannot modify this field unless you busy out the CTI link.
Fixed TEI	Use this field to enable a fixed Terminal Endpoint Identifier (TEI) for an endpoint. Use TEI to use multiple physical phones on a single BRI interface. This field is available only for ASAI or ADJLK CTI links types. The system no longer supports the ASAI and ADJLK types. You cannot modify this field unless you busy out the CTI link.
MIM Support	Use this field to enable Management Information Message (MIM) for an ASAI or ADJLK link. The system no longer supports the ASAI and ADJLK types.
XID	Use this field to enable Layer 2 XID testing capability for the system. This field is available only for ASAI or ADJLK CTI links types. The system no longer supports the ASAI and ADJLK types.

change cti-link field descriptions — page 2

Field	Description
Block CMS Move Agent Events	Use this field to enable the blocking of some event messages that are related to an agent move. The system does not send event messages related to the changes to the agent state, such as logout followed by login and return to previous state. You cannot modify this field unless you busy out the CTI link.
Event Minimization	Use this field to enable event minimization for the CTI link. Event minimization limits the number of event reports that the system sends to an adjunct. Use this field when the system sends event reports on multiple associations, but the adjunct recieves only a single report. The selection of the association on which the event is sent is based on association precedence as follows: • active notification (if enabled) • call control (if enabled) • domain control (if enabled) You cannot modify this field unless you busy out the CTI link.

Table continues…

Field	Description
Send disconnect Event for Bridged Appearance	Use this field to specify if the system must send an event report when a bridged appearance disconnects. You cannot modify this field unless you busy out the CTI link.
Special Character for Restricted Number	Use this field to append the asterisk (*) to the digit string of the restricted number.
Two-Digit Aux Work Reason Codes	Use this field to enable sending of two-digit Aux Work Reason Codes over the ASAI link. All messages that include Aux Work Reason Codes allow codes from 1 to 99. You cannot modify this field unless you busy out the CTI link.

list cti-link

Use **list cti-link** to list the administered CTI links.

See **status link** for more details on links.

Syntax

```
list cti-link  number  [ count ]
```

number cti-link number.

count Maximum number of links to list.

list cti-link field descriptions

Field	Description
Link	Link number
Ext	Extension associated with the CTI link (the extension is required but not used)
Type	Link type: ASAI-IP, ADJ-IP, ASAI, ADJLK
Port	Port number
Name	Node name for the link
COR	Class of restriction number

list usage cti-link

Use **list usage cti-link** to list vectors and IP services that use the specified CTI link, and indicate whether the link is currently used to monitor a hunt group as a controlling link, and/or through an event notification or domain control association.

CTI links are identified by the CTI link number in Communication Manager administration screens, not by extensions. For CTI links, use **list usage cti-link** instead of **list usage extension**.

Syntax

```
list usage cti-link  link
```

link	Link number (1–64).

release cti-link

Use **release cti-link** to release a busied-out endpoint for a link that is administered on the AESVCS Administration page of the IP Services screen. An ASAI adjunct link provides connectivity to an ASAI adjunct (for example, CentreVu CT), which is connected to an Ethernet LAN.

See **status link** for more details on links. For more information, see Busyout and Release Commands.

Syntax

```
release cti-link  link#
```

link#	Link number.

test cti-link

Use **test cti-link** to test the specified CTI link.

For more information on the CTI link, see **status firmware download**. See **status link** for more details on links.

Syntax

```
test cti-link n [ short | long ][ repeat # | clear ]
```

n	Link number.
short	Execute a series of nondestructive diagnostic tests.
long	Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
repeat #	(Optional) The number of times to repeat the command. The default is 1.
clear	Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

customer-alarm

test customer-alarm

Use **test customer-alarm** to test the customer provided alarm device by closing the alarm relay contact on the PN and EPN maintenance circuit pack in a specified cabinet, including the TN2312BP, for 1 minute and then restoring the alarm relay contact to its current state. Verify the test by checking the customer alarm attached to the specified circuit pack.

Syntax

```
test customer-alarm  UU C [ short | long  ][ repeat # | clear ][ schedule ]
```

location *UU C*	Extension of the data module or data channel to be tested, per dial-plan.
short	Execute a series of nondestructive diagnostic tests.
long	Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
repeat #	Number of times to repeat the test.
clear	Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.
schedule	Specify a start time for the command.

Example

```
test customer-alarm
test customer-alarm  02  r  2
test customer-alarm  01b  r  25
test customer-alarm  2a
test customer-alarm  2a  sh
test customer-alarm  3  c
```

data-module

busyout data-module

Use **busyout data-module** to put a data module in a maintenance busy state, even an uninstalled data module.

Use **release data-module** to return the specified data module or data channel into service.

Syntax

```
busyout data-module  extension
```

extension Extension number per dial plan.

Use **list data-module** to see a list of every data module administered on the system, including the extension, port, type, and other data for each data module. The maintenance object name for each data module in the Type field is:

Type of data module	Maintenance Object
adm-t	BRI-SET
announcement	DAT-LINE
dtdm	DIG-LINE
pdm	PDMODULE
system-port	DAT-LINE

Example

```
busyout data-module  31300
```

release data-module

Use **release data-module** module to activate the specified data module or data channel. Hardware tests are executed to verify that the equipment is functioning.

For more information, see Busyout and Release Commands.

Syntax

```
release data-module  extension
```

extension Extension number associated with data module or data channel.

status data-module

Use **status data-module** to see the internal software states of a specified data-module port. This information helps diagnose and locate facilities to which the data module is connected.

Syntax

```
status data-module  extension
```

extension Data module extension.

status data-module field descriptions

Field	Description
Data Ext/Sta Ext for Stn DM	Data module extension number. For DTDMs, the connected station extension is shown.
Port/ChannelNumber	Location of the port connected to the data module. For data channels, the channel number is shown.
Service State	The operational state of the data-module: • **in-service/idle** — data module is connected but idle. • **in-service/active** — data module is connected and in use. • **out-of-service** — data module has been removed from service • **disconnected** — data module no longer appears to be present

If the specified port is administered as a system port, the following fields will be for more information.

Field	Description
CF Destination Ext	The call-forwarding destination, if any, of the station.
Maintenance Busy	Whether the object is busied out for testing.
Connected Ports	Locations of ports to which the data module is currently connected.
Service State	The operational state of the associated port.

test data-module

Use **test data-module** to perform hardware diagnostic tests on a data module or a data channel. Test results are determined by the interface to the digital switch-data line port, digital line port, or network control data channel.

Syntax

```
test data-module  extension  [ short  |  long ][ repeat  #  |  clear ] [ schedule ]
```

extension Extension of the data module to be tested (per dial-plan).

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

schedule Specify a start time for the command.

Example

```
test data-module 30000  l
test data-module 30000
test data-module 32000  sh  r  2
test data-module 33000  1  r 25
test data-module 30000  c
```

directory

list directory

Use **list directory** to list every file in the specified board's memory file system.

Forward slash (/) is the default path for listing files in the root directory. To list the files in a directory other than the **/root** directory, specify the complete path.

Syntax

```
list directory board  location  |  path
```

board	Board location file or directory name.
path	Path to the directory.

Example

```
list directory board  1c12
```

disabled-MOs

list disabled-MOs

Use **list disabled-mos** to list the maintenance objects that have been disabled with **disable mo**, **disable all**, or **disable mo-all**, as well as whether or not the command has been run.

Use display **disabled-tests** for numbers of tests that have been disabled.

Syntax

```
list disabled-mos [ schedule ]
```

schedule	Specify a time to run the command.

disabled-tests

display disabled-tests

Use **display disabled-tests** to display the list of maintenance tests that have been disabled.

The disabled tests are not available for background or demand testing.

ds1-facility

busyout ds1-facility

Use **busyout ds1-facility** to put a DS1 facility of a DS1C complex into a maintenance busy state. Each DS1C complex uses from 1 to 4 DS1 facilities.

- The packet facility carries the control channel for every facility in the complex, all packet traffic, and some circuit connections.
- The other facilities carry circuit connections only.

Syntax

```
busyout ds1-facility  location [ override ]
```

location Location of the ds1-facility.

override All packet and circuit traffic on the packet facility is switched to another facility, and all traffic that was on the destination facility before the switch is dropped.

Whenever the circuit pack resets, the packet facility is set on the **a** facility. If system software detects a problem with this facility, it switches the packet and control traffic to another facility. The **busyout** command is not allowed on the packet facility without **override**. When **override** is used, all packet and circuit traffic on the packet facility is switched to one of the other three facilities, and all traffic that was on the destination facility before the switch is dropped.

There is no way to tell which facility is carrying the packet and control traffic without attempting to busy it out. If there is only one facility left in service on the circuit pack, it cannot be busied out. In this case, the circuit pack must be busied out.

Caution:

Busying out a non-packet facility disrupts all traffic carried on that facility. Using override to busy the packet facility disrupts all traffic on the facility to which the packet and control traffic is moved. This facility cannot be determined in advance.

On critical-reliability systems (duplicated PNC) a facility on the active PNC cannot be busied out. Use **busyout pnc** to busyout a standby PNC, and then busyout a facility on the standby PNC.

Example

```
busyout ds1-facility  6b
```

test ds1-facility

Use **test ds1-facility** to perform a series of tests on the specified facility. Each test runs diagnostics on the facility and returns results of the test along with any possible error codes. The long test is destructive and is not allowed unless the facility has been busied out.

Syntax

```
test ds1-facility location [ short  |  long  |  external loopback ][ repeat # ] [
schedule ]
```

location	Location of the DS1 Converter circuit pack plus a letter (a–d) corresponding to the four facilities connected to the circuit pack.
short	Execute a series of nondestructive diagnostic tests.
long	Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
external loopback	This initiates a destructive test that sends a test pattern to an external device and returns it for comparison to the original. Configure the external device to loop back the signal. See 'DS1-FAC (DS1 Facility)' and 'DS1-BD (DS1 Interface Circuit Pack)' in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers*
repeat #	Number of times to repeat the test.
schedule	Specify a start time for the command.

Example

```
test ds1-facility 1a05
test ds1-facility 04a01d
test ds1-facility 03a01a sh c
```

ds1-loop

test ds1-loop

For TN464F or TN767E or later suffix DS1 Interface circuit packs, use **test ds1-loop** for loopback and one-way span testing of the DS1 span.

Use **test ds1-loop** to validate that the board exists at the specified location, that the board is a TN464F or TN767E or later suffix DS1 Interface board. Based on the command parameter, a long-duration loopback/span test or series of short-duration loopback tests will be executed.

Long-duration loopback tests execute for an extended period of time until the system technician terminates it. Short-duration loopback tests return the result of the test to the screen when finished executing. Use **list measurements ds1 summary** to monitor the status of a long-duration loopback/span test.

If the [inject-single-bit-error] parameter is used, but no CPE loopback jack, far-end CSU, or one-way span test is active on the DS1 circuit pack, the following error message appears:

Parameter valid only if a loopback/span test is active on the DS1.

Syntax

```
test ds1-loop location [ cpe-loopback-jack-test-begin [ number-of-bitsbit-pattern ] |
far-csu-loopback-test-begin | one-way-span-test-begin | end-loopback/span-test |
inject-single-bit-error | ds1/csu-loopback-tests ]
```

location	Represents the physical position of the board to be tested. It is represented by the cabinet number, the carrier, and the slot position. A one-digit cabinet (1–3) is entered with or without a leading zero (0).
cpe-loopback-jack-test-begin ***number-of-bits bit-pattern***	For TN464F or TN767E or later suffix DS1 boards, this causes a long-duration loopback test to be setup through the CPE (customer-premises equipment) loopback jack. The command allows you to specify a loop-up code for the CPE loopback jack if it differs from the default of 0x47F. Specify the number-of-bits in the loop-up code as well as the actual bit-pattern (in hexadecimal). The test aborts if the **busyout** command has not been set
far-csu-loopback-test-begin	For TN464F or TN767E or later suffix DS1 boards, this causes a long-duration loopback test to be setup through the far-end CSU (channel service unit).
one-way-span-test-begin	For TN464F or TN767E or later suffix DS1 boards, this begins execution of a long-duration one-way span test.
end-loopback/span-test	For TN464F or TN767E or later suffix DS1 boards, this parameter terminates long-duration one-way span and loopback testing.

inject-single-bit-error	For TN464F or TN767E or later suffix DS1 boards, this parameter causes a single bit error to be sent within an active framed 3-in-24 test pattern used in long-duration loopback and span testing.
ds1/csu-loopback-tests	For TN464F or TN767E or later suffix DS1 boards, this parameter executes the following loopback tests: DS1 Board LoopBack, CSU Module Equipment LoopBack, and CSU Module Repeater LoopBack. These tests are performed sequentially for a short duration each, and individual PASS/FAIL/ABORT test results are reported following each test.

Feature Interactions for test ds1-loop

Loopback or span tests are allowed only on DS1 boards that are busied out.

Only one of the CPE loopback jack, far-end CSU, one-way span, or DS1/CSU loopback tests may be active at any given time on a DS1 span.

Example

```
test ds1-loop  1c08
test ds1-loop 10c08 cpe
test ds1-loop 1b12 far
test ds1-loop 2c14 end
```

eda-external-device-alrm

list eda-external-device-alrm

For detailed information regarding **`list eda-external-device-alrm`**, refer to 'EXT-DEV' in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers*

test eda-external-device-alrm

Use **`test eda-external-device-alrm`** to perform hardware diagnostic tests on the alarm port for either an individual device, or every external device.

If `all` is entered, **`test eda-external-device-alrm`** performs a hardware diagnostic test on every administered external device's alarm port. If an administered external device's alarm port is entered, this command performs a hardware diagnostic test on that port.

The test **passes** if the external device is not reporting an external device alarm and **fails** if the external device is reporting an external device alarm. If the technician specifies a port, it must be administered as an external device's alarm port either on a maintenance board or on an analog line board.

Note:

If you enter **test eda-external-device-alrm** on an IPSI-connected port, an error message appears. The IPSI circuit pack contains maintenance board functionality.

Syntax

```
test eda-external-device-alrm all | physical-location [ repeat # | clear ][schedule]
```

all	Test every administered external device's alarm port on analog line boards and maintenance boards.
physical location	For an administered external device alarm analog line port, the physical location represents the physical position of the port to be tested. Since the "maintenance board" alarm connections connect to control carrier boards that are in unnumbered slots, the standard port format cannot be used to designate these alarm connections. The special ports **UUmajor** and **UUminor** are used designate the major or minor maintenance board alarm connection for cabinet **UU**. The special locations **UUmajor** and **UUminor** designate the name of the major or minor Maintenance circuit pack alarm connection for cabinet **UU** (depends upon the auxiliary connector of the Port Network). Thus, both a **major** and **minor** port can be administered with major, minor, or warning alarms.
repeat #	Number of times to repeat the test.
clear	Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.
schedule	Specify a start time for the command.

emergency

set emergency

Use **set emergency** to manually set the state of emergency transfer on a TN2312BP in a gateway or Compact Modular Cabinet (CMC). **set emergency** generates a major alarm if emergency transfer is set to **on** and generates a warning alarm if emergency transfer is set to **off**.

Syntax

```
set emergency  on | off | auto [ cabinet ]
```

on	Activates emergency transfer
off #	Deactivates emergency transfer

auto	The server controls emergency transfer
cabinet	Specify the cabinet location (1-64)

environment

status environment

Use **status environment** to see status information for the 655A power supplies in a specified G650 or G650 stack.

Syntax

```
status environment [ cabinet ][ carrier ]
```

cabinet	Cabinet location.
carrier	Carrier location.

Note:

The microcontroller on the power supply might provide data for diagnostic tests and **status environment**, even if the power supply itself fails. The microcontroller can get input power from three sources, the supply output voltage, backplane power, or its own power supply, and might work even though the power supply fails. If the power supply is in a control carrier without a redundant power supply and the carrier fails, then communication with the power supply is not available.

Note:

If the system cannot communicate with the power supply, or if the power supply is removed from the carrier, all fields except **Pow Loc** and **Alm Cnt** contain a single dash (-).

status environment field descriptions

Field	Description
Pow Loc	Location of the 655A power supply (cabinet/carrier/slot)
Alm Cnt	Number of active major and miner alarms for the maintenance objects, MO_E_I2C_BUS, MO_E_POW_SUP, MO_E_CAB_TEMP, MO_E_RING_GEN
Temp (F/Client)	The inlet air flow temperature (Fahrenheit is on the left and Celsius is on the right)
Temp (F/C) Ex	The outlet air flow temperature (Fahrenheit is on the left and Celsius is on the right)

Table continues…

Field	Description
Hot Spot	The status of the temperature at the power supply's hot spot: • ok • wn (warning) • sh (shutdown)
Voltage	The three voltages monitored are: • +5VDC Primary logic control • -5VDC Logic support • -48VDC Telephone support (Talk Battery)
Fan Ctrl	The speed at which the fans are running. Fan voltage is: • **udr** – under 12VDC • **mid** – +12VDC • **hgh** – +14VDC • **ovr** – above +14
Fan Alm	A fan alarm occurs when one or more fans fail.
Ring Voltage Stat	Status of the ringer on the associated power supply. See **Ring Status and Ring Control states** for the valid states for **Ring Stat** and **Ring Ctrl**: • ok • over (overloaded) • shrt (shorted) • fault • cmd (commanded off)
Ring Voltage Ctrl	Indicates if the associated power supply is providing ringing voltage for the G650. Only one power supply can provide ringing voltage to the carrier. See Ring Status and Ring Control states for the valid states for Ring Ctrl and Ring Stat: • actv (active) • stby (standby) • dsbl (disabled, see **Ring Set** field values) • off (due to short or internal failure)
Ring Voltage Set	Indicates the ringing voltage frequency. The ringing voltage frequency is set via a physical switch on the 655A power supply: • 20 Hz (North American Ringer Signal) • 25 Hz (European/International Ringer Signal) • off (ringer switch on the power supply is set to off)

Table continues…

Field	Description
Det	• **y** — backplane ringing is detected • **n** — backplane ringing is not detected
Input Power	Type of current (active input voltage) that is being used on the power supply and an alternate source that can be used. Lower case letters indicate that an input source is present but not being used. Upper case letters indicate the input source that is being used. • AC (Alternating Current) • DC (Direct Current)

Table 4: Ring Status and Ring Control states

Stat/Ctrl	Ring Generator State
ok/actv	The ring generator on this power supply is the active ringer.
ok/stby	The ring generator on this power supply is the standby ringer
ok/dsbl	The ring generator on this power supply is OK, but is disabled with the ringer select switch on the power supply. This is done when an external ringer is used, for example the TN2202 French Ringing circuit pack.
over/actv	The ringer voltage on this power supply is overloaded, but the ring generator on this power supply is still active.
shrt/off	The ring generator on this power supply is off due to a short on its output.
fault/off	The ring generator on this power supply is off due to a failure detected by an internal power supply audit.
cmd/off	The ring generator on this power supply is off due to a software command.

test environment

Use **`test environment`** to perform hardware diagnostic tests of the environment monitoring and control, and emergency transfer functions of a specified cabinet. This command tests PN cabinets. Circuit packs involved are the PN's maintenance and tone-Clock (for the ring generator test).

Caution:

The long test recycles power on every port circuit pack carrier and is destructive. It does not recycle power on active or standby servers. When a port carrier is recycled, all service and links to ports on the carrier are dropped. If a carrier containing an active EI or Tone-Clock is recycled, all service to that cabinet is disrupted.

Syntax

```
test environment cabinet [ short | long ][ repeat # | clear ][ schedule]
```

cabinet Cabinet number.

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

schedule Specify a time to execute the command.

Maintenance objects reported with test environment

There are 10 maintenance objects reported with the **`test environment`**.

Maintenance Object	Notes
AC-POWER	Appears for SCC (Single carrier cabinet) and MCC (Multi carrier cabinet) cabinets.
CABINET	Appears for SCC and MCC cabinets.
CARR-POW	Appears for SCC and MCC cabinets.
CUST-ALARM	CUST-ALARM is part of the environment functionality but is not tested with test maintenance. See **`test customer-alarm`** for details.
DC-POWER	Appears for SCC and MCC cabinets.
EMG-XFER	Appears for SCC and MCC cabinets.
EXT-DEV	Appears when the External Device Alarm Admin field is `n` on the change system-parameters customer-options screen.
POWER	Appears for SCC and MCC cabinets.
RING-GEN	Appears for SCC and MCC cabinets.
RMV-GEN	Appears when the rack mount cabinet is used on duplicated servers.

errors

clear errors

Use **`clear errors`** to move every error and resolved alarm to the cleared errors list, to make room for new incoming error messages that might otherwise be dropped. Clear errors does not clear

active alarms from the alarm log. Cleared error entries are the first entries overwritten when additional room is needed to log new entries.

Use **display errors clear** to list the cleared errors.

⚠ Caution:

Use **clear errors** with care. Cleared data is lost when the logs fill up.

Syntax

```
clear errors
```

display errors

Use **display errors** to select the errors that appear on the hardware error report.

Errors can result from in-line firmware errors, periodic tests, failures detected while executing a test command, software inconsistency, or a data audit discrepancy. The error log is restricted in size. A new entry overwrites the oldest unalarmed entry. The overwritten entry must be at least six minutes old, or the new entry is dropped.

Syntax

```
display errors [ high-resolution ] [ schedule ]
```

high-resolution	Include high resolution time stamps for the first occurrence and last occurrence of the error. This shows seconds and a sequence count within a second. The sequence count starts over for each second. See Error Log Report High Resolution.
schedule	Specify a time to run the command.

Help messages

- When the first page of a multiple page list of alarms/errors or after the **Prev Page** key is pressed:

  Press CANCEL to abort or NEXT PAGE for next page
- After the **Next Page** key is pressed and there are more pages of alarms/errors to be displayed:

  Press CANCEL to abort, NEXT PAGE for next page, PREV PAGE for previous page.
- After the **Next Page** key is pressed and there are no more alarms/errors to be displayed:

  Press CANCEL to abort, NEXT PAGE to complete, PREV PAGE for previous page.

System Reboots and Error and Alarm logs

Avaya Aura® Communication Manager software attempts to save the error and alarm logs to the disk when any of the following events take place:

- The save translation command is executed.
- Translations are saved as part of scheduled maintenance (as administered on the Maintenance-Related System Parameters screen).

- A demand or software-escalated system reboot takes place.

Whenever the Communication Manager software reloads, the error log is restored from the disk. Since the logs are saved to the disk, the versions restored at reload time may not be current. This occurs when either:

- The attempt to save at reload did not succeed.
- The server that is active coming out of reload is not the same one to which the logs were last saved.

In such a case, the logs will not show the errors and alarms that have been logged since the last time a save was made to the server that became active with the reboot. When looking at errors that precede the last reload, look for indications preceding the reload to determine whether the logs restored at reboot are complete. System resets less severe than a reload rarely affect the error and alarm logs.

Note:

If there are system errors in the error log, use **`display initcauses`** for more information. Information that could not be logged during a system reset may be found here.

display errors input field descriptions

The display errors input screen specifies which errors display on the report. When every selection has been made, press **ENTER**. If no selections are made or if the schedule option is specified, the system displays every error from the last day that are associated with active alarms.

Field	Description
Error Type	The report can be restricted to specific error codes. Default is every error.
Error List	The report can be restricted to errors from one of three lists described below: active-alarms, errors, or cleared-errors. Default is active-alarms.
Interval	Specifies error records for the last month, hour, day, week, or all errors (**m**, **h**, **d**, **w**, **a**). The default is all.
From	Specifies error records starting from the time specified by **mm/dd/hh/mm** (month/day/hour/minute). If no From date is entered, errors from the earliest record in the log are displayed.
To	Specifies every error record up to the time specified by **mm/dd/hh/mm**. If no To date is entered, every error up to the current date appears.
Equipment Type	To limit the report to a specific group of components, enter the location of a type of equipment in one of the following fields. If no entry is made, errors for the entire system are displayed. • **Gateway:** Enter the gateway number. • **Cabinet:** Enter the cabinet number. • **Port Network:** Enter the port network number. • **Board:** Enter the cabinet-carrier-slot address of the circuit pack (for example, 11c04). If the cabinet number is omitted, it defaults to 1.

Table continues…

Field	Description
	• **Port:** Enter the cabinet-carrier-slot-circuit address of the port (for example, 11c0408). If the cabinet number is omitted, the system will default to 1. • **Category:** Enter a category to restrict the report to maintenance objects in a specific category. The **HELP** key displays a list of categories. • **Extension:** Enter the extension number of a port. • **Trunk (group/member):** Enter a trunk-group number, or a trunk-group and member number separated by a slash (for example, 78 or 78/1).

display errors output field descriptions

Field	Description
Port	The physical location of the alarmed object. • For circuit pack based MOs, the location is `cabinet-carrier-[slot]-[circuit]`. • For PN-based objects, such as TDM-BUS, the location displays as `3PN xx`, where *xx* is the PN number. • For Fiber Link-based objects, the location displays as `x a,b-PNC` where *x* is the Fiber Link number and `a-` or `b-pnc` indicates one of the PNC pair. Always `a-pnc` for a high-reliability system with an unduplicated PNC.
Maintenance Name	The name of the MO as it appears in the alarm and error logs.
	The alternate name depends upon the type of the object. For example: • **Station MO** — alternate name is *nnnnn* (extension) • **Trunk MO** — alternate name is *nn/n* (trunk-group number/member number) • **Personal CO line MO** — alternate name is *P/xx* (P/personal CO line group number)
Error Type	Numerical error code that identifies the type of problem. The meanings of these codes are explained under the name of the MO in the *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers (03–300430)*.
Aux Data	Additional numerical information about the error type. Only the most recent auxiliary data for each error type appears.
	First line: Month, day, hour, and minute (and second, if the **high-resolution** command-line option is used) that the error was first recorded.

Table continues…

Field	Description
	Second line: The month, day, hour, and minute (and second, if the high-resolution command-line option is used) of the most recent error. If the system is unable to retrieve the time of day when the error occurred, a **dummy** date will be stamped in the log so as to distinguish it from reliable data. It appears as **00/00/01:07**.
Seq Cnt	Sequence Count. These numbers give the order in which the errors were logged. Each sequence covers a period of one second. Sequence numbers are assigned to the first and last occurrences of a given error within the one second period given in the time stamp. There may be gaps in the sequence numbers within a given second because the last occurrence of an error may replace an existing entry and because sequence numbers are also assigned to software events not shown in the hardware error log. This information appears when the high-resolution option is specified on the command line.
Err Cnt	The total number of times that the error type has occurred. The maximum entry is 999.
Err Rt	Average hourly rate at which the error has occurred from the first occurrence to the present. The maximum entry is 999.
Rt/Hr	An approximation of the rate at which this error occurred in the last hour. The maximum entry displayed is 999.
Al St	Alarm Status. A character indicating the status of this MO in the error and alarm logs. • **a** — active alarm entry • **r** — resolved alarm entry • **c** — resolved alarm entry due to long clear option of test • **s** — resolved alarm entry due to a software-requested (non-demand) system restart • **t** — resolved alarm entry due to a technician-requested system restart • **n** — not alarmed
Ac	**y/n** — Whether the maintenance object is still under active consideration by the maintenance subsystem.

ess

disable ess

Use **disable ess** to disable a Survivable Core Server or main server from connecting to IPSIs in a port network. The **disable ess cluster n** command allows a Survivable Core Server cluster to be disabled (taken out of service).

Communication Manager preserves the enabled/disabled status of Survivable Core Servers and Main servers across server shutdown and restart.

A cluster may be disabled if and only if it is not controlling any IPSIs. A disabled Survivable Core Server will not connect to IPSIs.

A disabled Survivable Core Server remains registered and receives file sync translation updates.

Execute **disable ess** from either a main or Survivable Core Server. A Survivable Core Server may disable only its own cluster ID. When disable ess is run from the main server, any and all clusters may be disabled including the main server itself.

⚠ Caution:

Use caution when using **disable ess all**. Since the main typically controls IPSIs and a cluster may not be disabled when it controls IPSIs, it is generally safe to use **disable ess cluster all** to disable only the Survivable Core Server clusters.

Be aware that if the main is not controlling IPSIs and **disable ess cluster all** is used, the main will also be disabled.

When a Survivable Core Server is disabled, it reboots. After the reboot, the server is in the Survivable Core Server disabled state and will not connect to any IPSIs. If the cluster involves duplicated servers, this process may take slightly longer while the active server informs the standby of its new Survivable Core Server disabled state. When the system duplicates Survivable Core Server, the standby server also gets updated and rebooted.

When a valid **disable ess** command is run from a Survivable Core Server:

- The server reboots.
- No SAT screen is displayed.
- Once the server has rebooted, use **status ess cluster** to confirm that the disable operation succeeded.

When a valid **disable ess** command is run from a main server:

- TEST RESULTS screen appears
- If the **disable ess** command specifies the cluster ID of the main itself, the server reboots and no SAT screen is displayed.
- Use **status ess cluster** to confirm that the disable operation succeeded.

Syntax

```
disable ess[ all | cluster n]
```

all Disables all Survivable Core Servers

cluster *n* Number (1–999) of the cluster ID for the target Survivable Core Server or main server.

Error codes

The following table describes the error codes that may be returned from the **disable/enable ess** commands:

Error Code	Description
1991	Requested Survivable Core Server cluster is not administered
1992	Requested Survivable Core Server cluster is not registered
1993	Requested Survivable Core Server is controlling an IPSI PN
1994	A Survivable Core Server cluster may not enable/disable other clusters.
2500	Internal operation failed

Example

```
disable ess  cluster 7
disable ess all
```

enable ess

Use **enable ess** to enable a Survivable Core Server. Once a Survivable Core Server cluster is enabled, it attempts to connect to IPSIs.

Use **enable ess** from either a main or a Survivable Core Server. A Survivable Core Server may enable only its own cluster ID. When **enable ess** is run from the main server, any and all cluster IDs may be enabled including the main itself. Care should be taken when using **enable ess all**.

When a Survivable Core Server is enabled, it removes its translations and reboots. The TEST RESULTS screen is not displayed.

When a main server is enabled, it reboots but does not remove its translations. A TEST RESULTS screen is displayed. The exception is when the **enable ess** cluster command specifies the cluster ID of the main itself. In that case, the server reboots and no screen is displayed.

After the reboot, the server is in the Survivable Core Server enabled state and will attempt to connect to IPSIs. If the cluster involves duplicated servers, this process may take slightly longer while the active server informs the standby of its new Survivable Core Server enabled state.

Syntax

```
enable ess[ all | cluster n ]
```

all Enable all Survivable Core Servers

cluster *n* Number (1–999) of the cluster ID for the target Survivable Core Server or main server.

See 'Error Codes' for a description of possible error codes returned from the **enable ess** command.

status ess clusters

Use **status ess clusters** to see the state of the main server and all administered Survivable Core Servers. Under normal conditions, with full network connectivity, all Survivable Core Servers should register with the main.

Syntax

```
status ess cluster
```

When **status ess clusters** is run on a main server (Cluster ID 1), the Main server:

- knows the identities of all of its associated Survivable Core Server from the translations input to the main server.
- knows the state of all of the Survivable Core Servers that have successfully registered with it.
- shows its own state.

status ess clusters field descriptions

Note:

The field definitions are the same whether the **status ess** command is executed on a main server or Survivable Core Server.

Field	Description
Cluster ID (title line)	Cluster Identifier (1–999) of the server where **status ess** was run. In a duplex server environment, both the active and the standby server have the same cluster ID. Cluster ID is initially obtained from the license file (where it is called the Module ID or MID). Once save translation is executed, the cluster ID is saved in translations.
Cluster ID (detail line)	Cluster Identifier (1–999) of a server who's state is known to the server where **status ess** was run. The detail lines are shown in cluster ID order. When **status ess** is issued on a main server, there is one detail line for the main server itself and a detail line for every Survivable Core Server that is registered with the main server. When **status ess** is issued on a Survivable Core Server there is only one detail line since a Survivable Core Server only knows its own state.
Enabled	The Survivable Core Server enabled or disabled state of the server. • **y** — enabled. This server will connect to administered IPSIs. • **n** — disabled. This server will not connect to administered IPSIs.

Table continues…

Field	Description
	• **unknown** — the main server does not yet know the maintenance state of the Survivable Core Server. This may be because: - the Survivable Core Server is not registered with the main server - the Survivable Core Server has not yet acknowledged a maintenance state change request from the Main via an **enable ess** or **disable ess** command.
Active Server ID	The server identifier of the active server for each cluster, Survivable Core Server or main server (1–99). This is the Server ID that was entered for this server in the Set Server Identities page during configuration. • If the server is a simplex configuration, there is only one Server Identifier. • If the server is a duplex configurations, the A and B servers each have unique server identifiers. Because in a duplex configuration only the active server registers with the Main, only its server identifier is displayed. Only server IDs for registered Survivable Core Servers are displayed.
Registered	The registration state of the server. • **y** — registered • **n** — not registered The main server does not register with itself, but always displays its own registration as **y**.
Translations Updated	For a Survivable Core Server: The time and date of the latest translation update reported by the Survivable Core Server to the Main server over the registration link. For a main server (Cluster ID 1): The time and date of the latest successful save translation command of any kind. **Note:** For a main server, this time stamp may be later than those shown for Survivable Core Servers. A **save translation** on the Main updates its time stamp. A **save translation [ess | all]** updates the Survivable Core Server translations and time stamp.
Software Version	The software version of Communication Manager running on the server. For a Survivable Core Server, this is reported to the Main server over the registration link.

status ess port-networks

Use **status ess port-networks** to see the status of all administered Port Networks on Survivable Core Server and non-Survivable Core Server systems.

- For Survivable Core Server and Main servers, on IP Port Network Connectivity (PNC) and Asynchronous Transfer Mode (ATM) PNC systems, **status ess port-networks** shows the status of all of the administered Port Networks.
- For Center Stage Switch (CSS) PNC systems, only the IPSI equipped Port Networks are known to the Survivable Core Server, because only the Main server has access to the CSS. The information displayed is very dynamic and may, for brief periods, appear inconsistent.

Syntax

```
status ess port-networks
```

status ess port-networks field descriptions

Field	Description
Cluster ID (title line)	Cluster Identifier (1–999) of the server on which **status ess port-networks** was run. In a duplex server pair, both the active and the standby server should have the same cluster identifier. Each server initially learns its own cluster ID from its license file (where it is called the Module Identifier or MID). After **save translations** is executed, the cluster identifier is saved in translations. However, the cluster identifier is always overridden by the license file as long as the license file is present and readable.
PN	The number that identifies the Port Network (PN). This is the same number that identifies the Port Network in the **list cabinet** command.
Com Num	The community number of the Port Network (1–64) assigned to the Port Network on **display system-paramters**. After losing connectivity with their server, port networks try to be controlled by a local preferred server in the same community.
Intf Loc	Interface Location. Board location of the most recent interface in the Port Network with which the system tried to control the Port Network. The interface may be any circuit pack through which the Port Network may be controlled, such as a TN2312 IP Server Interface (IPSI), a TN2305B or TN2306B ATM Expansion Interface (ATM EI), or a TN570D Expansion Interface (CSS EI). blank — there is no interface.
Intf Type	The type of interface whose location is shown in the **Intf Loc** field. • IPSI — IP Server Interface

Table continues…

Field	Description
	• EI — either type of Expansion Interface (TN570 or TN2305/2306) • UNKN — the interface type cannot be determined • blank — there is no interface.
Port Ntwk Ste	The Port Network state from the point of view of the server on which **`status ess port-networks`** is run. • **up** — the Port Network is up • **down** — the Port Network is down • **unkn** — the state is unknown • **blank** — there is no Port Network state The Port Network is up from the perspective of the server that is controlling the Port Network. The Port Network is down from the perspective of all other servers.
IPSI Gtway Loc	IPSI Gateway Location. The location of the IPSI whose Packet Interface (PKTINT) is being used to deliver packet traffic to the packet bus in this Port Network. The IPSI may be in this Port Network (this location is the same as **Intf Loc**), or it may be in a different Port Network.
Pri / Sec Loc	The location of the Primary and Secondary IP Server Interface (if any) in this Port Network. • If the Port Network has a single IPSI, only one line is displayed. • If the Port Network has duplicated IPSIs equipped, each is displayed on successive lines. • blank — the Port Network has only an Expansion Interface from which it is controlled
Pri / Sec State	The state of the Primary and Secondary IPSIs whose locations are shown in the Pri / Sec Loc field. • **actv-aa** — the IPSI is both active and is controlling the Port Network (hosting the Arch Angel). • **active** — the IPSI is active but not controlling the Port Network. In this case the Port Network may not be controlled or is being controlled through an Expansion Interface (EI). • **standby** — the IPSI is in standby mode (duplex Port Network connectivity). • **unknown** — the IPSI state is unknown l blank = there is no IP Server Interface.
Cntl Clus ID	Control Cluster Identifier. The cluster identifier of the server that was last known to be controlling this Port Network through this IPSI. If there

Table continues…

Field	Description
	are duplicate IPSIs in this Port Network, they should show the same Cluster ID • Cluster ID (1–999) • * (asterisk) - The server where status ess port-networks is run cannot connect to the IP Server Interface in this Port Network. This may be because: • the IPSI is being reset • the IPSI rejected the connection request from the server, perhaps because it is already connected to its limit (8) of servers. - The controlling Cluster ID reported for the IPSI is not known to the server (in its translations) where status ess port-networks was run. • . (period) - The controlling Cluster ID reported by this interface is not known to the server on which this command is executed given its own translations. This can occur when a new Survivable Core Server is brought on-line and translated on the main server but the translations have not yet been file synchronized to every other Survivable Core Server. The server on which this command is being executed cannot map from the Server ID reported by the interface to a Cluster ID known to the server in its translations. • ! (exclamation) - The Cluster ID reported by this interface is not in the valid range of values. • blank - There is no IPSI in this Port Network. - There is no controlling server.
Connected Clus(ter) IDs	Connected Cluster Identifiers. The list of cluster identifiers that were last known to be connected to this IP Server Interface. These servers are candidates to control the Port Network through the IPSI if connectivity to the current controlling server is lost. If a server was rejected by an IPSI, the information displayed here may be stale. This information will be updated periodically as each server attempts to connect or reconnect to the IPSI. The Cluster ID of the controlling server should always be displayed in the list of Cluster IDs. • Cluster ID (1–999) • - (dash) - A dash indicates that the server whose Cluster ID would have been in this position has lost the socket connection to this duplicated IPSI but not the connectivity to the IPSI's pair interface

Table continues…

Field	Description
	in the same port network. The server in question should appear in the same relative position in the list of Connected Clusters for the IPSI's pair interface. • . (period) - The controlling Cluster ID reported by this interface is not known to the server on which the command was executed given its own translations. This can occur when a new Survivable Core Server is brought on-line and translated on the main, but the translations have not yet been file synchronized to every other Survivable Core Server. The server on which this command is being executed cannot map from the Server ID reported by the interface to a Cluster ID known to the server in its translations. • ! (exclamation) - There is no IP Server Interface in this port network - There is no connected Cluster ID. • * (asterisk) - The Cluster ID reported by the IPSI is not known to the server (in its translations) where **status ess port-networks** was executed. • blank - There is no IPSI in this Port Network. - There is no controlling server.

ethernet-options

get ethernet-options

Use **get ethernet-options** to generate a report about a specific Ethernet connection.

Syntax

```
get ethernet-options  location
```

location The physical location of the circuit pack.

Comments on this document? infodev@avaya.com

get ethernet-options field descriptions

Field	Description
Auto Negotiation	Enter **y** for the system to automatically negotiate the highest possible network speed. Enter **n** to manually assign the Speed and Duplex fields.
Speed	10 Mbps 100 Mbps N/A (not available)
Duplex	Half Full N/A (not available)
Link Integrity	Active Inactive

list ethernet-options

Use **list ethernet-options** to see locations and settings for ethernet-enabled ports.

Syntax

```
list ethernet-options
```

set ethernet-options

Use **set ethernet-options** manually or automatically set the Ethernet connection parameters.

Note:

The Ethernet port must be administered and busied out before you can issue **set ethernet-options**.

Syntax

```
set ethernet-options  location
```

location The physical location of the circuit pack.

set ethernet-options field descriptions

Field	Description
	y — the system automatically negotiates the highest possible network speed.

Table continues…

Field	Description
	n — you must manually assign the Speed and Duplex fields. If **n**, the Speed and Duplex fields do not appear.
Speed	10 Mbps/100 Mbps Appears when Auto Negotiation is **y**.
Duplex	Half/Full Appears when Auto Negotiation is **y**.

events

display events

Use **`display events`** to see a log that shows a vector event is the occurrence of something unexpected during a vector-routed call due to resource exhaustion or faulty vector programming. For example, route-step failures are typically due to the programming of an invalid extension. These types of failures are not due to faulty hardware or system software error and do not constitute incorrect feature operation.

An IP event occurs when an IP endpoint registration is denied.

You can see the detailed information about denial events on the System Logs page. Use display events to diagnose and correct IP registration denials, and vectoring problems due to resource exhaustion or faulty vector programming. See *Avaya Aura® Call Center Release 4.01 Call Vectoring and Expert Agent Selection (EAS)* to see how to interpret vectoring fields on this report.

Syntax

```
display events
```

display events field descriptions

Use the Event Report to request events of a certain type or from a certain time period. Enter the desired parameters and press **ENTER**.

Field	Description
Category	Enter the type of event to display. The valid values are `all`, `contact-cl`, `data-error`, `denial`, `meetme`, and `vector`.
Report Period	Select the time period for the vector events you want to see. If fields are blank, every recorded vector event is reported.
Interval	The time period for which events are reported: `m` (month), `d` (day), `h` (hour), `m` (minute), or `a` (all). The following information message displays on the display events screen:

Table continues…

Field	Description
	`IPv6 addresses are truncated, see System Logs web page for complete address.`
Start/Stop Time	Enter the date and time of day when you want to start and end the search.
Vector Number	Enter a specific vector number to include in the report. If blank, events for every vector are reported. If the category field is meetme, this field is ignored.
Event Type	Enter a specific event type to include in the report. If blank, all event types are reported.
Extension	Enter a specific event type to include in the report. If blank, all events for all extensions are reported.

display events output field descriptions

Field	Description
Event Type	The event identification number that points to a specific piece of software code. See *Avaya Aura®Communication Manager Denial Events (03-602793)*.
Event Description	25-character string describing the problem See *Avaya Aura®Communication Manager Denial Events (03-602793)*.
Event Data 1	The station UID that is attempting to register See *Avaya Aura®Communication Manager Denial Events (03-602793)*.
Event Data 2	The IP address of the station that is attempting to register See *Avaya Aura®Communication Manager Denial Events (03-602793)*.
First Occur	The time and date when this event first occurred
Last Occur	The time and date when this event last occurred
Evnt Cnt	The number of occurrences of the event between the First Occur and Last Occur times

extended-user-profile

change extended-user-profile

Use **`change extended-user-profile`** to administer detailed access permissions for the vector and station forms.

Syntax

```
change extended-user-profile  n
```

n The number of the extended profile to change.

change extended-user-profile field descriptions

Field	Description
User Profile Name	The name of the standard profile for which this is the extended profile. Display only.
Form	Category and type of form (SAT screen) that are administered for extended permissions. Display only.
Allow Only	Specify access to all, certain, or no instances of the form. • all = access to all instances of the form • blank = no access to the form List specific instances in a valid format as: • list separated by commas (1,2,3) • one or multiple pair separated by a dash (1000–2000). As many combinations can be administered as can fit in the field.

display extended-user-profile

Use **display extended-user-profile** to see the access permissions on an existing Extended User Profile.

Syntax

```
display extended-user-profile  n
```

n Number of the extended user-profile to display.

See **change extended-user-profile** for screen and field descriptions.

extension-type

list extension-type

Use **list extension-type** to see the type of stations associated with specific extensions.

Syntax

```
list extension-type [ n | partial-string * | all | type ]
```

n Extension number.

partial-string *	List all extensions that begin with the partial string, as in searching for all numbers that begin with a specific area code.
all	List all extensions.
type	Refer SAT command Help to see the list extension-type type entries.

failed-ip-network-region

display failed-ip-network-region

Use **display failed-ip-network-region** to see a list of the worst, first 100 network regions with broken connectivity rank ordered by the worst to least worst.

To troubleshoot broken connectivity, see **status ip-network-region** and **test failed-ip-network-region**.

Syntax

```
display failed-ip-network-region
```

test failed-ip-network-region

Use **test failed-ip-network-region** to initiate a real-time **ping** test for failed network-region connections.

The default is that all connections that failed the last background maintenance ping test are tested. If network region *x* is specified, then just failed connections from region *x* are tested. If a previously failed connection passes the ping test, then the associated minor alarm is cleared.

To troubleshoot broken connectivity, also see **display failed-ip-network-region** and **change ip-network-region**.

Syntax

```
test failed-ip-network-region [ all | x  ]
```

all	Test all failed IP network regions.
x	Test the specified failed IP network region.

test failed-ip-network-region field descriptions

Field	Description
Region	Network region that had a connection failure to **Dest. Region**.
Dest. Region	A network region to which **Region** is connected, where the connection between the two regions is previously failed the **ping** test.
Maintenance Name	The name of the MO as it appears in the alarm and error logs.
Test No.	Test Number used to run **ping** test.
Result	Result of ping test — PASS or FAIL. If test failed, follow troubleshooting procedures in 'NR-CONN (Network-Region Connect)', *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*.
Error Code	**ping** test error code

fiber-link

add fiber-link

Use **add fiber-link** to create a fiber link.

Syntax

```
add fiber-link fiber# [ a-pnc | b-pnc ]
```

fiber# The administered number assigned to the fiber link. In a system with duplicated PNC, this represents a fiber link pair.

a-pnc For an unduplicated PNC, a-pnc is the only valid qualifier. Use on a system with duplicated PNC, to distinguish between the two fibers of a duplicated pair. a-pnc is the default.

b-pnc Use on a system with duplicated PNC, to distinguish between the two fibers of a duplicated fiber pair.

Description

A fiber link is a connection carrying all circuit and packet traffic between two port networks, two switch nodes, or a port network and a switch node. A fiber link may contain a DS1 converter complex used to provide connectivity to a remote PN. On critical-reliability systems (duplicated PNC), each fiber link is duplicated and exists as a pair. When PNC duplication is enabled, only the DS1 Converter complex attributes fields can be changed.

Before Avaya Communication Manager Release 2.0, **add fiber-link** restricted the placement of an expansion interface (EI) circuit pack to slot A01 in the A carrier of a port network. In Communication Manager Release 2.0, the TN2312BP resides in slot A01 of a G650 media gateway.

Slot B01 of a port network can be used for a duplicate fiber connection when IPSI duplication is not active. When IPSI duplication is required, the duplicate IPSI must reside in slot B01 and any fiber connection there must be moved.

add fiber-link field descriptions

Field	Description
Fiber Link #	Identifying number of the fiber link.
Is one endpoint remoted via DS1 Converter Complex	y/n y indicates that a DS1C converter complex is used on this link to remotely locate a port network. If y, a second page is displayed for administering the DS1C complex attributes.
Board Location	The physical address (cabinet-carrier-slot or gateway:module) of the circuit packs comprising the two endpoints (ENDPOINT-1 and ENDPOINT-2) of the fiber link.
Board Type	ei or sni, the type of circuit pack administered at each endpoint.
Fiber Translation	multi-mode or single-mode Use for faster remote diagnosis.
Converter	y/n Use for faster remote diagnosis.
Type of Transceivers	A/B Use for faster remote diagnosis.

busyout fiber-link

Use **busyout fiber-link** to put a fiber link into a maintenance busy state.

Caution:

On a standard- or high-reliability system (unduplicated PNC), **busyout** is destructive. Every call and application link carried on the busied-out fiber link will be torn down, and new calls will not be established over the link.

Syntax

```
busyout fiber-link fiber# [ a-pnc | b-pnc ]
```

fiber# The administered number assigned to the fiber link. In a system with duplicated PNC, this represents a fiber link pair.

a-pnc For an unduplicated PNC, a-pnc is the only valid qualifier. Use on a system with duplicated PNC, to distinguish between the two fibers of a duplicated pair. a-pnc is the default.

b-pnc Use on a system with duplicated PNC, to distinguish between the two fibers of a duplicated fiber pair.

Description

A fiber link is a connection carrying all circuit and packet traffic between two port networks, two switch nodes, or a port network and a switch node. A fiber link may contain a DS1 converter complex used to provide connectivity to a remote PN.

On a critical-reliability system with duplicated PNC, **busyout fiber-link**:

- is permitted only on a fiber link on the standby PNC
- does not impact service
- requires that the standby PNC be busied first

Use **list fiber-link** to see a list of every fiber link administered on the system, including its number, endpoint, and other useful information.

---

change fiber-link

Use **change fiber-link** to change the translation data associated with an existing fiber link.

Syntax

```
change fiber-link fiber#
```

fiber# The administered number associated with a fiber link or, on a duplicated PNC, with a fiber link pair.

Description

On critical-reliability systems (duplicated PNC), each fiber link is duplicated and exists as a pair. When PNC duplication is enabled, only the DS1 Converter complex attributes fields can be changed.

Translation data changes after the ENTER key is pressed. Press CANCEL any time before pressing ENTER to return to the command line without changing any translation data.

To change the endpoint board locations, remove a fiber and add it again for either a:

- High-reliability system, an unduplicated PNC
- Critical-reliability system with a fully operational duplicated PNC

change fiber-link field descriptions — Page 1

Field	Description
Fiber Link #	Display-only. Identifying number of the fiber link.
Board Location	The physical address (cabinet-carrier-slot or gateway:module) of the circuit packs comprising the two endpoints (ENDPOINT-1 and ENDPOINT-2) of the fiber link.
Board Type	ei or sni, the type of circuit pack administered at each endpoint. Display-only.
DS1 Converter	y indicates that a DS1C converter complex is used on this link to remotely locate a port network. If y, a second page is displayed for administering the DS1C complex attributes.

Table continues…

Field	Description
Fiber Translation	multi-mode or single-mode Use for faster remote diagnosis.
Converter	y/n Use for faster remote diagnosis.
Type of Transceivers	A/B Use for faster remote diagnosis.
Converter Type	Avaya/other. Displayed when Converter on the Fiber Link Administration screen is y.

change fiber-link field descriptions — Page 2

The following fields when a DS1 converter complex is administered on the fiber link. DS1 CONV complex attributes are administered here. The circuit pack is administered by **`change circuit-packs`**. Use page 2 for the A-PNC. If the PNC is duplicated, the fields are repeated as display-only on page 3 for the B-PNC. Page 3 fields change when their counterpoints on page 2 are changed.

Field	Description
Board Location	Under DS1C-1, the physical location of the converter board connected to ENDPOINT-1. When the location is entered, validation is performed to ensure that the board has been administered and is of the correct type (DS1 CONV).
DS1 Converter Facilities	Attributes of the four DS1 facilities (A, B, C, D) that can be connected to the DS1 CONV.
Facility Installed	y/n Specifies whether the indicated facility has been provided and installed. Facility A is required for the DS1 CONV complex. See DS1 Line Equalization Settings table. The line equalization setting defaults to the median value of 3. This setting remains in effect until changed by administration. Incorrect equalizer settings may cause a higher error rate on the DS1 facility.
DS1 CONV-2 Line Compensation	Same as for ENDPOINT-2 of the DS1 CONV complex.
Zero Code Suppression	zcs/b8zs specifies the line coding format for each facility. There are 2 line coding options supported by the DS1 Interfaces to meet the density requirements in the data stream. Zero Code Suppression (ZCS) line coding is in place following an initialization until changed by administration. Either line coding option may be used on the DS1 Interface that carries the packet time slots.
Framing Mode	esf/d4 specifies the data framing format used on the facility. When esf, an automatic selection process is executed until the DS1 Interface is brought into frame, or until an Options CCMS message is received by the framing options master. Once options are set by administration, they remain fixed on the framing option master until the board is again initialized, reset, or sent new options. The framing option on the framing option slave converter board can change to track the framing option master's option.

DS1 Line Equalization Settings

Equalizer Setting	Distance to DSX-1 Interface (feet)	
	22 AWG ABAM and 24 AWG PDS	26 AWG PDS
1	1 to 133	0 to 90
2	133 to 266	90 to 180
3	266 to 399	180 to 270
4	399 to 533	270 to 360
5	533 to 655	360 to 450

display fiber-link

Use **display fiber-link** to see the translation data associated with an existing fiber link.

Syntax

```
display fiber-link fiber# [ schedule ]
```

fiber# The administered number associated with a fiber link, or fiber link pair in a duplicated PNCs.

schedule (Optional) Specify a start time for the command.

Description

The output for **display fiber-link** is the same as that for **change fiber-link**.

list fiber-link

Use **list fiber-link** to list every fiber link in the system, and to see a summary of data entered on the fiber link screen (**add**, **display**, **change**, or **remove fiber-link**).

Syntax

```
list fiber-link [ schedule ]
```

schedule (Optional) Specify a start time for the command.

Fiber mismatch

Even though a DS1-fed EPN is in service with no complaints, list fiber-link can report a MISMATCH for the Primary Facility. This MISMATCH indicates that the two ends of the DS1 fiber do not agree which DS1 facility is carrying the Primary Facility, or control channels of the fiber. This indicates that the two DS1 spans are crossed, that is, the A-facility in PPN is connected to the B-facility in the EPN. The EPN DS1C board searches both spans for the control channel, and when it finds it, the system link comes up on either A or B facility. This then becomes fiber group 1 and the other span is fiber group 2. The end result is that the system link is up, all timeslots are mapped correctly, and

there are no end-user problems. This is only a problem when there are DS1 problems. To fix this problem flip the A and B spans at one end, either PPN or EPN.

list fiber-link field descriptions

Field	Description
FIBER LINK #	The administered number used to identify the fiber link (1 to 27).
TYPE	The types of circuit packs that constitute endpoint 1 and endpoint 2 of the fiber link (ei or sni).
A-PNC LOC	The physical locations (cabinet-carrier-slot number) of the circuit packs that constitute the endpoints.
DS1 CONV LOC	Location of the DS1 Converter.
B-PNC LOC	In a system with duplicated PNC, the physical location (cabinet-carrier-slot number) of the circuit packs that constitute the endpoints of the link in the B-PNC.
DS1 CONV TYPE	Whether or not an endpoint of the link is remotely located by means of a DS1C Converter complex.

reset fiber-link

Use **reset fiber-link** to reset the Expansion Interface and/or Switch Node Interface circuit packs that are endpoints of a specified fiber link, dropping the link in the process.

⚠ Caution:

The reset fiber-link command is destructive on a high-reliability system (unduplicated PNC), and may cause an entire port network to be removed from service.

Syntax

```
reset fiber-link fiber# [ a-pnc | b-pnc ]
```

fiber# The administered number of the fiber link (1-44). On a critical-reliability system (duplicated PNC), this number designates a fiber link pair; the following qualifier specifies which fiber in the pair is to be reset

a-pnc For an unduplicated PNC, a-pnc is the only valid qualifier. Use on a system with duplicated PNC, to distinguish between the two fibers of a duplicated pair. a-pnc is the default.

b-pnc Use on a system with duplicated PNC, to distinguish between the two fibers of a duplicated fiber pair.

Description

A fiber link must be busied out before being reset. To busyout a fiber on critical-reliability systems, the fiber must be on the standby PNC and the standby PNC must first be busied out. See **busyout fiber-link**.

Use **list fiber-link** to see a list of fiber links and their locations.

test fiber-link

Use **test fiber-link** to validate that the optical fiber connection between switch node interfaces (SNI) and expansion interfaces (EI), or a combination thereof, are administered.

Syntax

```
test fiber-link link# [ a-pnc | b-pnc ]
 [ short | long ] [ repeat # ] [ clear ] [ schedule ]
```

link#	The administered number assigned to the fiber link. In a system with duplicated PNC, this represents a fiber link pair.
a-pnc	For an unduplicated PNC, a-pnc is the only valid qualifier. Use on a system with duplicated PNC, to distinguish between the two fibers of a duplicated pair. a-pnc is the default.
b-pnc	Use on a system with duplicated PNC, to distinguish between the two fibers of a duplicated fiber pair.
short	Run short test sequence.
long	Run long test sequence.
repeat #	(Optional) The number of times to repeat the command. The default is 1.
clear	(Optional) Repeats the test sequence until any active alarms against the maintenance object are cleared by the passing of tests, or until any test in the sequence fails.
schedule	(Optional) Use schedule to specify a start time for the command.

Description

If the fiber link is administered, a series of hardware diagnostic tests are performed on the specified fiber link. The test results along with any possible error codes are displayed on the MT. The long test sequence includes destructive tests. Every destructive test aborts unless the fiber link is first busied out. The short test sequence is non-destructive and can be performed regardless of whether the fiber link is busied out.

A fiber link is a connection between port networks (PNs), switch nodes (SNs), or between a PN and the Center Stage Switch (CSS). This connection is comprised of a bi-directional optical fiber connection (optionally extended via a DS1 Converter complex), with each end terminated on either an Expansion Interface (EI) or a Switch Node Interface (SNI). Fiber links provide the medium for circuit and packet connections between PNs.

The long sequence includes destructive tests and requires that the fiber link be busied out first. When a fiber is busied out, every call over that fiber is dropped.

clear firmware-counters clears the firmware counters of specified SNI, SNC, -EI or DS1C circuit packs, or of an the entire PNC (A or B).

Example

```
test fiber-link 1 b-pnc
test fiber-link 03 b-pnc sh r 3
```

file

remove file

Use **remove file** to request the board location to remove the file given by path. If the file does not exist on the source board's filesystem, an error message – `file not found` – appears on the SAT.

To remove a file in a subdirectory, specify the entire path starting at `/`.

Syntax

```
remove file [ board location | gateway  location ] [ filename ]
```

board *location*	Location of the board.
gateway *location*	Location of the gateway.
filename	Name of the file to remove using the entire path starting with `/`.

filexfer

disable filexfer

Use **disable filexfer** to disable Secure Shell (SSH), and Secure FTP (SFTP) remote access protocols through login/password authentication on C-LAN and VAL circuit packs.

disable filexfer also disables FTP sessions.

Syntax

```
disable filexfer   location
```

location	Location of the circuit pack.

enable filexfer

Use **enable filexfer** to enable Secure Shell (SSH) and Secure FTP (SFTP) remote access protocols through login/password authentication on C-LAN and VAL circuit packs. FTP capabilities remain enabled.

Syntax

```
enable filexfer  location
```

location Location of the circuit pack.

enable filexfer enables the C-LAN and VAL circuit packs as SSH/SFTP servers (not clients) that prefer the following symmetric algorithms in decreasing order:

- AES
- Arcfour
- Blowfish
- CAST128
- 3DES

Note:

To ensure that technicians can access the relevant circuit packs using SSH or SFTP, technician laptops must have SSH and SFTP clients that use the same algorithms installed.

enable filexfer field descriptions

Field	Description
Login	3–6 alphabetic characters
Password	7–11 characters containing at least one letter and one number.
Renter Password	Re-enter the password.
Secure	**y** — enable SFTP **n** — enable FTP
Board Address	Location of the circuit pack.

firmware-counters

clear firmware-counters

Use **clear firmware-counters** to clear the firmware error counters on the specified circuit packs. This command is valid only for SNI, SNC, and DS1C and ATM-EI board locations. When `a-pnc` or `b-pnc` is specified, every such circuit pack in a single PNC can be cleared at once. On a

critical-reliability system (duplicated PNC), only circuit packs on a standby PNC that is busied out can be cleared.

Use **clear firmware-counter** to quickly clear lingering alarms after a hardware problem has been fixed. **test clear** commands do not clear alarms on SNI, SNC, and DS1C circuit packs.

Warning:

clear firmware-counters can mask actual hardware problems, because firmware is cleared and appears as if no problems were ever encountered.

Syntax

```
clear firmware-counters   location | a-pnc | b-pnc
```

location	Location of the circuit pack.
a-pnc / b-pnc	The specified location must be occupied by an SNI, SNC, or DS1C circuit pack. Every circuit pack in the standby PNC can be cleared at once by specifying a-pnc or b-pnc. To do so, the standby PNC must first be busied out.

firmware download

change firmware download

Use **change firmware download** to schedule a C-LAN-distributed download or a self-download firmware download, immediately or at a later date and time.

For information regarding firmware station downloads, see the FW-STDL (Firmware Station Download) section in the *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*.

To update firmware on Avaya equipment:

1. Open a browser window on your computer and go to http://www.avaya.com.
2. Select Support.
3. Select Software and Firmware Downloads.

If a firmware download schedule is already pending or active, **change firmware download** is blocked.

Note:

You must execute **test ipserver-interface** after scheduling a download but before the download begins.

Note:

If you receive an error message asking you to use **test ipserver-interface**, there is a problem with a previous firmware download. Run the test before proceeding.

Syntax

```
change firmware download schedule-number
```

schedule-number Value between 1 and 4.

Description

Insert a description of the command, including what it does and when to use it.

change firmware download field descriptions

Field	Description
Source Board Location	The board location where the firmware image resides. For “remote downloads”, this location is a C-LAN board. For “self-downloads”, this location is the same as the target board location. The value for this field can be **self** (download of multiple boards) or **auto** (Communication Manager chooses the correct C-LAN board to do the download).
File Server	The IP address of the File Server.
File Retrieval Protocol	Display-only field.
Login	Login for the file server.
Password	Password for the file server.
Firmware Image File Name	The firmware image file name, including the file extension, to download.
Target Board Code	The TN-code of the target board to be downloaded, such as TN799.
Suffix	The suffix of the target board to be downloaded. For example, AP, DP, GP.
Firmware Vintage	Display-only, the firmware vintage of the entered image file. This field is always blank for a **change firmware download**. This field contains a value with **display firmware download** while a download is in progress, and with **status firmware download** after a download is complete.
Schedule Download	**y/n** — Specify whether to run the download immediately or at some future time. If **y**, Start Date/Time and Stop Date/Time appear. If **n**, the download begins when the screen is submitted.
Remove Image File After Successful Download	**y/n** — Specify whether to automatically remove the firmware image file on the source board after the download is successful for the specified target boards.

Table continues…

Field	Description
	If **y**, and every board was successfully downloaded, the image file is removed, and the file system on the source board is disabled.
Start Date/Time	The date and time to begin the firmware download (mm/dd/yyyy, 2 digits for month, 2 digits for day, and 4 digits for year, and hh:mm, 2 digits for hour, and 2 digits for minutes). This field appears when Schedule Download field is **y**.
Stop Date/Time	Appears when the Schedule Download field is y. It indicates the date and time to end the firmware download to end. If the scheduled stop time is reached before the new firmware image file has been downloaded to every circuit pack, the system finishes downloading to the circuit pack in progress and then aborts the remainder of the download schedule. If this field is blank, the download continues until completion. The field is formatted: mm/dd/yyyy (2 digits for the month, 2 digits for the day, and 4 digits for the year). and hh:mm (2 digits for the hour, and 2 digits for the minutes).
Target Location	These fields contain the target board locations of the boards that will receive the download file image. For a self-download, the target location is the same as the source location.

disable firmware download

Use **disable firmware download** to stop the firmware download for a specified schedule (1–4). If a target board is currently downloading, the download is first completed for the current board, but the remaining boards are not downloaded. Run **status firmware download** to determine how far along the current download is.

Syntax

```
disable firmware download schedule-number
```

schedule-number Value between 1 and 4.

display firmware download

Use **display firmware download** to see the status of the specified download schedule. Use **change firmware download** to schedule a download. If a scheduled download has not yet occurred or is currently in progress, use **display firmware download** to view the settings for the scheduled downloads. If all downloads have finished, the fields are blank.

See **status firmware download** , **disable firmware download** , and **test ipserver-interface** , and the 'MO FW-STDL (Firmware Station Download)' in *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)* for more information.

Syntax

```
display firmware download schedule-number
```

schedule-number	Value between 1 and 4.

See **change firmware-download** field descriptions for the field descriptions for **display firmware download**.

status firmware download

Use **status firmware download** to see the download status for each board that is scheduled, or was scheduled, to receive new downloaded firmware as requested by change firmware download. Use last to see the download schedule of the last completed download for a particular schedule. If there is no active download schedule and there was no previous schedule for the last qualifier to invoke, status firmware download shows a blank download schedule.

The following status flags are shown for each target board:

P	The download to the board is pending.
C	The download to the board was completed successfully.
F	The download to the board failed. Look into the error logs for firmware download for more information about the failure.
S	The board was skipped (the board requires manual intervention to busy-out).
A	The download to the board was aborted.

Syntax

```
status firmware download [ schedule-number | last schedule-number ]
```

schedule-number	Value between 1 and 4.
last schedule-number	Last completed or aborted download schedule

status firmware download field descriptions

Field	Description
Firmware Vintage	Vintage of the firmware
Start Date/Time Stop Date/Time	If the last parameter was used, this actual dates and times at which the download was started and stopped appear. Otherwise, scheduled dates and times appear.
St	The download to that board is pending (P), completed (C), failed (F), or aborted (A). If a download fails, **enter test ipserver-interface** to see the error code. See 'Troubleshooting procedures for each error code in Firmware Download Test (#1413)' in *Maintenance Alarms for Avaya*

Table continues…

Field	Description
	Aura® Communication Manager, Branch Gateways and Servers (03–300430).

For more field descriptions, see **change firmware download**.

test firmware download

Use **test firmware download** when there is a download scheduled or there are errors or alarms against the **FW-DWNLD** maintenance object from a previous download. If there is a download scheduled, then this command verifies the Firmware Download screen entries. If there are **FW-DWNLD** errors or alarms, then this test resolves the errors and clears the alarms.

See 'Firmware Download Test (#1413)' in the *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers (03–300430)* for more information about the test that is run and the troubleshooting procedures to use if the test does not pass.

You must execute test firmware download after scheduling a download with **change firmware download**, but before the download begins. The test is blocked if a download is in progress. If a download is in progress or has already completed, use **status firmware download** to view progress and status.

For the complete download procedure:

1. Open a browser window on your computer and go to http://www.avaya.com/.
2. Select Support.
3. Select Software and Firmware Downloads.

Syntax

```
test firmware download schedule-number
```

schedule-number Value between 1 and 4.

firmware station-download

change firmware station-download

Use **change firmware station-download** to select the range of stations for download and schedule the start/stop time. When there is an active scheduled download, **change firmware station-download** is blocked.

Syntax

```
change firmware station-download
```

disable firmware station-download

Use **disable firmware station-download** to disable a currently running download schedule and allow any active station downloads to complete.

Syntax

```
disable firmware station-download
```

display firmware station-download

Use **display firmware station-download** to see information for the currently scheduled download.

Syntax

```
display firmware station-download
```

status firmware station-download

Use **status firmware station-download** to see the status of the currently scheduled download.

Syntax

```
status firmware station-download
```

status firmware station-download field descriptions

Field	Description
Terminal Type for download	Displays the information related to the firmware, font, language, boot, and DSP telephones.

Table 5: Schedule States of status firmware station-download command

State	Schedule done?	Description
Idle	No	No downloads Pending or Active and there are no unresolved errors/ alarms for the last download
Pending	No	Download has been scheduled but not yet started. Check the start time to see when it is scheduled to start.
Active	No	Download is currently active. Actively downloading terminals should be listed with a status of ACTV. If the schedule has just started and no

Table continues…

State	Schedule done?	Description
		downloads are listed, the system may be waiting for a FAC requested or terminal requested download to complete before it begins.
Resume-pending	No	Download was stopped at the Stop Date/Time but not all of the terminals have been attempted. Downloading will resume at the scheduled Start Date/Time listed on the screen.
Aborted	Yes	Download was aborted for the entire range of terminals. This could happen if the firmware image was bad, damaged or lost.
Failed	Yes	At least two terminals rejected the firmware as invalid. As a result, the download was aborted to prevent problems with any further terminals. Check the Reason Codes of the failed terminals in the list to find the reason why the download failed. See 'Reason Codes for status firmware station-download command'.
Completed	Yes	The scheduled download has completed either due to all terminals in the range of extensions having completed or due to the stop timer.
Disabled	Yes	An Active schedule was disabled with the **`disable firmware station-download`** command. After an active schedule is disabled, the Schedule state remains **Active** until all currently active terminal downloads have completed.
No Image	Yes	The download was stopped because there was no firmware image present in memory.
Restart	Yes	The download was stopped due to a system restart. You must schedule a new download for any Aborted terminals.
Sys Fail	Yes	The download was stopped due to a system error.
Sys Occ	No	The download has been suspended due to the system's occupancy level. The schedule resumes when the occupancy level drops to a safe level.
Dnld Timeout	Yes	While the scheduled download was running, two or more consecutive terminals failed to respond to the download process.

Table 6: Reason Codes for status firmware station-download command

Reason Code	Status	Description
1	ABORT	The firmware image that was noted in the change firmware station-download form has disappeared. The download schedule had to be stopped.
2	ABORT	The terminal could not be downloaded due to a discrepancy relating to the maximum number of downloads allowed.
3	ABORT	The terminal was not downloaded before the scheduled stop time occurred. Schedule a new download with adequate time for the downloads to complete, or select the continue daily option to allow the schedule to resume the following day.

Table continues…

Reason Code	Status	Description
4	ABORT	The terminal could not be downloaded because the schedule aborted for an unknown reason.
5	ABORT	The terminal did not respond to the download request.
6	ABORT	The terminal that was added to the download list at the scheduled start time no longer exists. This can occur when a station is removed during an active download schedule. Download to this terminal was aborted.
11	ABORT	The terminal was in firmware download mode when the layer 2 link to the terminal went down. The download was aborted as a result of the link down condition.
18	ABORT	The terminal was busied out by craft and could not be downloaded.
32	ABORT	Download to the terminal timed out due to an internal error in the station firmware download process.
1000	ABORT	Terminal was in use at the time that it was to be downloaded. Download to this terminal was aborted.
1012	ABORT	An internal error occurred while preparing to download to this station.
3841	ABORT or FAIL	The system restarted during an active download. As a result, all terminals that were not downloaded are marked with a status of ABORT with this reason code. All terminals that were actively downloading when the reset occurred are marked with a status of FAIL with this reason code.
128	FAIL	The terminal rejected the firmware because the firmware image failed the checksum test.
129	FAIL	The terminal rejected the firmware because the firmware image failed the image validity test. The firmware image may not be the right image for the hardware being downloaded to.
130	FAIL	The terminal being downloaded could not write its flash memory.
131	FAIL	The translated terminal type is valid, however the actual terminal type of the hardware is not valid for this download schedule.
513	FAIL	The terminal was not in service at the time that it was to be downloaded. Download to this terminal failed.
3584	FAIL	The terminal rejected the firmware image.

test firmware station-download

Use **`test firmware station-download`** to resolve any alarms or errors associated with the **`firmware station-download`**. See 'FW-STDL (Firmware Station Download)' in *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)* for details.

Syntax

```
test firmware station-download
```

hardware-group

cancel hardware-group

Use **cancel hardware-group** to temporarily or permanently abort the execution of **test hardware-group**. Use **resume hardware-group**, to resume the same test, or start another test with **test hardware-group**. Press **CANCEL** to cancel a hardware group test executing in the foreground.

The status of a canceled **test hardware-group** is displayed as canceled on the status hardware-group screen.

When a hardware group test is executing in the foreground with the continuously option and **CANCEL** is pressed or **cancel hardware-group** is entered, the hardware group test is canceled, and for security reasons the MT running the hardware group test is logged off. Use **resume hardware-group** to restart the canceled hardware-group test after logging back on.

Syntax

```
cancel hardware-group
```

Scheduled and Periodic Maintenance

When **test hardware-group** is entered, all activity related to scheduled background maintenance, periodic background maintenance, and data audits is suspended for the duration of the execution of **test hardware-group**. All activity related to scheduled background maintenance, periodic background maintenance, and data audits will restart if **test hardware-group** is canceled.

All-Ports Option

When **test hardware-group** all-ports is canceled, the internally generated port translations for ports that are otherwise untranslated are removed. If **resume hardware-group** is then entered, only customer-administered ports will subsequently be tested. Resume does not reinstate the port translations that were removed by the cancel.

If **test hardware-group** running in the foreground is successfully canceled with **cancel hardware-group** from another terminal, the following message is displayed on the terminal where the hardware group command was executing: `Hardware-group command aborted with cancel; command entered from another terminal.`

resume hardware-group

Use **resume hardware-group** to restart a hardware group test at the point where it was canceled. This capability is not available if another hardware group test has been started.

Halt a hardware group test (**test hardware-group**) temporarily or permanently with **cancel hardware-group** for a background test, or by pressing **CANCEL** for a foreground test. Use **status hardware-group** to see the status of a hardware group test.

When **test hardware-group all-ports** is canceled, the internally generated port translations for previously untranslated ports are removed. If **resume hardware-group** is then entered, only customer-administered ports are tested. Resume does not reinstate the port translations that were removed by cancellation of **test hardware-group all-ports**.

Syntax

```
resume hardware-group
```

When a test that was executing in the background is resumed, a success message is displayed. When a test that was executing in the foreground is resumed, test results are displayed.

status hardware-group

Use **status hardware-group** to see summary information about the active or last hardware group tests.

The information includes the number and percentage of maintenance objects tested, the percentage of tests passed/failed/aborted, the time elapsed since initiating the hardware group test, the specific hardware group test command (see **test ipserver-interface**) initiated, and the state (active/canceled/complete) of the hardware group test.

Syntax

```
status hardware-group
```

status hardware-group field descriptions

Field	Description
Hardware Group Command State	The state of a hardware-group command: • **active** — testing is in progress • **canceled** — testing has been canceled • **complete** — the command has completed and there is no testing going on.
Number of MOs Tested	The number of MOs in the specified group (see **test ipserver-interface**) that have had been tested by current hardware-group. This includes every MO that either was actually tested or was aborted due to resource contention.
Total Number of MOs to be Tested	The total number of MOs in the group that was specified in **test hardware-group**.
Percent Complete	A ratio of the number of MOs completed and the total number of MOs to test in the command.

Table continues…

Field	Description
Elapsed Test Time	The duration of the hardware-group test. If a test was canceled and then restarted this time excludes the cancel period. If hardware-group has finished it indicates the length of time it took to complete the command. The time is displayed as *HH:MM:SS* where *HH* is hours, *MM* is minutes, and *SS* is seconds.
Repetition Number	The number of iterations that have been completed corresponding to the 'repeat' or the 'continuously' option.
Percentage of Tests Passed	The percentage of tests that passed.
Percentage of Tests Failed	The percentage of tests that failed.
Percentage of Tests Aborted	The percentage of tests that were aborted.
Command	The hardware-group action/object and qualifiers that were entered.
Test Sequence	short/long.
Test Repetition	Displays either continuously or the keyword repeat along with the repeat value entered.
Output Options	Displays the selections that were chosen on the input screen: auto-page, background, or failures.
Hardware Options	Displays the selections that were chosen on the input screen (all-ports).

test hardware-group

Use **test hardware-group** to run a series of demand maintenance tests on all hardware in a specified group: a carrier, cabinet, port network, PNC (A or B), circuit pack or the entire system. The tests executed vary depending on the options chosen and types of hardware in the group. Some tests are run concurrently to speed execution, so test results for several maintenance objects may be intermixed.

A hardware-group command running in the foreground can be aborted by pressing **CANCEL** or by entering **cancel hardware-group** at another terminal. Use cancel for a test running in the background. You can restart a canceled hardware-group test at the point it left off by entering **resume hardware-group**. Hardware group tests started with the all-ports option can be resumed, but they will not always test every port that originally would have been tested.

Syntax

```
test hardware-group [ system | carrier | cabinet | port-network PN# |[ a-pnc | b-pnc ]|
board location ][ schedule ]
```

system Every maintenance object included in the specified hardware group is tested, including every circuit pack and port. When a cabinet or larger entity is specified, environmental MOs are tested.

carrier Carrier location.

cabinet	Cabinet location.
port-network ***PN#***	Physical position of the packet bus (1–3).
a-pnc	Use on a system with duplicated PNC, to distinguish between the two fibers of a duplicated pair. For an unduplicated PNC, a-pnc is the only valid qualifier.
b-pnc	Use on a system with duplicated PNC, to distinguish between the two fibers of a duplicated pair.
board ***location***	Board location.
schedule	Specify a time to run the command.

test hardware-group feature interactions

Test Hardware Group	Only one **test hardware-group** command can be active at any given time.
TTI	If **test hardware-group** is issued with the all-ports option while the TTI background task is active, some unadministered ports may not be tested. In addition, active alarms on line ports may be cleared by this task. The **status tti** command may be used to determine the state of the TTI background task.
Add Station	If **add station** is entered for an untranslated port at the same time as it is being tested by test hardware-group with the all-ports option, the request to add station will fail and the following message is displayed: `Object in use; please try later.`
Trunk Administration	If an attempt is made to add an unadministered trunk port to a trunk group at the same time as it is being tested because of **test hardware-group** with the all-ports option, the request will fail, and the following message is displayed: `Object in use; please try later`
Save Translation	If **test hardware-group** is issued with the all-ports option when a translation save operation is active, some unadministered ports may not be tested. All other hardware will be tested normally.
Hardware Alarms	When a hardware error is detected by **test hardware-group**, the hardware goes through the standard escalation strategy. Alarms will be raised on hardware that manifest hard errors. This alarming strategy is the same, regardless of whether the ports are translated or not.
System Interaction	The performance of **test hardware-group** is affected by call processing traffic, administration activity, choice of the short or long option, whether the all-ports option was chosen and other demand maintenance activity.

Table continues…

Scheduled and Periodic Maintenance	When **test hardware-group** is entered, all activity related to scheduled background maintenance, periodic background maintenance, and data audits is suspended for the duration of the execution of **test hardware-group**. When **test hardware-group** is canceled or when **test hardware-group** completes, all suspended periodic, scheduled, and data audits background maintenance activity will be restarted where it left off.

test hardware-group field descriptions

Field	Description
Test Sequence	short / long. long is more comprehensive and is not destructive.
Test Repetition	Enter repeat to enter a number of times that the entire test sequence is to be repeated. Enter continuously to cause the test sequence repeat until the command is canceled.
Count	When Test repetition is set to repeat, specify the number of repetitions.
Auto-page	**y/n** Enter **y** to display a new screen when the screen fills up with results. This option is incompatible with the background option. If **n**, once the screen fills with results, testing stops until you press **PAGE** or **CANCEL**.
Background	Enter **y** to run the tests in the background and free up the terminal for other tasks. Error results are logged in the error log but not displayed on the screen. This option is incompatible with the auto-page and **continuously** options.
Failures	Enter **y** to see failure results only on the screen.
All-ports	Enter **y** to test all customer-translated line and trunk ports and, for the following circuit packs, untranslated ports as well.

health

monitor health

Use **monitor health** to show the current system alarm summary, maintenance busy summary, user summary, critical system status, and cabinet status, that are updated every minute.

See the same information with **status health**. Press **CANCEL** to end **monitor health** and drop the management terminal login.

Note:

monitor health is not available in ASA.

Syntax

```
monitor health
```

monitor health feature interaction

If standby Emergency Transfer Select Switches change and handshakes are down, the displayed Emerg Trans field is incorrect until handshake re-initializes. When monitor health terminates, users are logged off of the system.

status health

Use **status health** to list various performance measurements in the system. Measurements include the current system alarm summary, maintenance busy summary, user summary, critical system status, and cabinet status.

Syntax

```
status health
```

status health field descriptions

Field	Description
St	Percentage of CPU time currently dedicated to high priority items such as the operating system, rounded to the nearest whole number
Sm	Percentage of CPU time currently dedicated to system management or periodic and scheduled maintenance, rounded to the nearest whole number If a large amount of periodic or scheduled maintenance testing is being performed, this number can be high without affecting service.
Cp	Percentage of CPU time currently dedicated to call processing, rounded to the nearest whole number. Call processing has priority over system management and will draw occupancy from the SM or IDLE categories.
Idl	Percentage of CPU time currently idle and available for use, rounded to the nearest whole number.
Maj	Number of major alarms logged.
Min	Number of minor alarms logged.
Wrn	Number of warning alarms logged.
Logins	Number of current users.
Trk	Number of maintenance busied-out trunks.
Stn	Number of maintenance busied-out stations.
Oth	Number of busied-out maintenance objects, excluding trunks and stations.

Table continues…

Field	Description
Cab	Cabinet number. Use **`list cabinet`** to relate cabinet numbers to port network numbers.
EmTr	Emergency Transfer shows the current setting of the switches on the PN's Maintenance circuit packs that control Emergency Transfer. See 'EMG-XFER (Emergency Transfer)' in the *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*. The following states are available: • **auto-** — Emergency Transfer is under system control and is not currently activated (normal operating state). • **auto+** — Emergency Transfer is under system control and is in effect. • **on** — Emergency Transfer has been manually activated. This setting should only be in effect during an emergency. • **off** — Emergency Transfer is manually prevented from occurring. This setting should only be in effect when a technician is on site. • **n.a.** — The setting of the switch in this PN is not available to the switch. The Expansion Archangel Link (EAL) may be down. • **NoEqp** — The cabinet has circuit packs that do not support Emergency Transfer.
Maj, Min, Wrn	Number of major, minor or warning alarms associated with the cabinet. An asterisk indicates that the number exceeds 99 or 999.
PNC	Current Port Network Connectivity (PNC) status for each of the port networks in the cabinet. When multiple port networks exist within a cabinet, Carriers A, B, and C are listed first and separated from Carriers D and E by a slash (for example, up/up). • **aa** — Points to a problem with the archangel. The control is up, but the archangel is not functioning and is not available. • **up** — Both the Expansion Archangel Link (EAL) and the Indirect Neighbor Link (INL, if applicable) are available. • **dn** — Both EAL and INL (if applicable) are not available. ne (Near End) The EAL is available but the INL is not available. • **fe (Far End)** — The INL is available but the EAL is not available. • **up/up** — 2 port networks share a cabinet. The first up is associated with the PN contained in A, B, and C carriers, and the 2nd up in D and E.

Table continues…

Field	Description
	• **up/up/up** — 3 port networks share a cabinet. The first is in carrier A, the second in B and C, and the third in D and E. • **up/up/up/up** — 4 port networks share a cabinet. The first is in carrier A, the second in B, the third in C, and the fourth in D and E. • **up/up/up/up/up** — 5 (the maximum allowed) port networks share a cabinet. The first is in A, the 2nd in B, the 3rd in C, the 4th in D, and the 5th in E. Use **list cabinet** to see the carriers and port networks in each cabinet in the system.

history

list history

Use **list history** with no options to generate a log of the most recently completed data-affecting administration and maintenance commands. This includes the history of ACTR moves, which can be used to track moves and help reduce fraud.

Syntax

```
list history [ date | time | login x | action x | object x | qualifier x ][ schedule ]
```

date	MM or MM/DD
time	HH or HH:MM
login *x*	Login ID
action *x*	Action performed
object *x*	Object acted upon
qualifier *x*	Extension, etc.
schedule	Specify a time to run the command.

list history feature interactions

The translation log is written to memory as translation data when **save translation** is executed. The translation data is time stamped when saved. This time stamp is noted when translation is loaded from memory and included in every recent change history report.

When a user requests a recent change history report, there could be other users concurrently issuing data commands and altering the contents of the transaction log. Therefore, if the user pages

the entire way through the report, the oldest entries in the transaction log (maximum 250 commands) may have been overwritten by data commands issued by these other users. If this occurs, the final entries of the report show the data commands issued by the other users since the recent change history report was originally requested.

Also, using **set time** to alter the system clock could make it look as if the recent change history report is not in true LIFO order.

list history field descriptions

Field	Description
Date	The date **list history** was issued (mm/dd).
Time	The time **list history** was issued (hh:mm).
Port	The port type to which the user was connected when list history was issued. • TTI, PSA, CTA and ACTR moves are recorded when the CTA/PSA/TTI Transactions in History Log field is y on the Feature-Related System Parameters screen. These transactions appear as two separate records: one recording the moved-from port, and the other one recording the moved-to port. • IP station registrations and unregistrations are recorded when the Record IP Registrations in History Log field is y on the Feature-Related System Parameters screen.
Login	Shows the user login or the feature that caused the logged event, such as: • **actr** for ACTR moves • **cta** for Customer Telephone Activation transactions • **psa** for Personal Station Activation transactions • **tti** for TTI transactions • **ip-a** or **ip-u** for IP registrations and events • **pms** for Property Management System events • **ad** for Abbreviated Dialing events • **reboot** for when the system rebooted
Actn	The action part of the command, specifying the operation to be performed. This field is truncated after four characters to allow enough space for objects and qualifiers and to uniquely identify each action.
Object	The qualifier (12 characters) specifying the object of the command. Where the object is multiple words in length, only the first word appears in the object field; every succeeding word is treated as a qualifier.
Qualifier	One or more qualifiers describing the characteristics of the Action/Object pair. This field is truncated after 31 characters to keep information for a command on a single line.

Communication Manager events are also logged in the Linux syslog. Syslog is a standard Linux service that supports storing event information in local files as well as sending events to an external syslog server. Syslog supports storing events in different files or 'logs' depending on the nature of the event.

Access the Communication Manager web interface log pages through Select Diagnostics > System Logs. For more information on 'Communication Manager web interface System Logs', see *Maintenance Procedures for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300432)*.

The following types of activities are logged:

- Security-related events: Communication Manager logs all events related to security to the secure log. An administrator cannot disable or change parameters related to security events.
- System Administration Terminal (SAT) interface logging: Administration changes are logged to the command history log with the date and time, the unique identify of the person making the change, the value of the parameter that is changing and the status of the operation (successful or not). The administrator can configure the level of detail that is logged.

  Communication Manager logs attempts by users to view information to which they are not permitted access or attempts to submit forms with invalid or non-acceptable values.
- Web page logging: Attempts to access the Avaya server's web pages and changes to a value in a web page are logged. Changes to a web page are logged only if the page is submitted, either successfully or unsuccessfully.

notify history

Use **notify history** to generate a continuous real-time log of the data-affecting administration and maintenance commands being executed currently.

Syntax

```
notify history
```

initcauses

display initcauses

Use **display initcauses** to see a history of recovery steps taken by the system. **display initcauses** shows information for restarts of the active processor only. When the processor resets and the system is restarted, either by a technician command or by system software, information about the recovery is stored. If the reset is escalated, only the reset that successfully completes is recorded. The error log contains information about the reset. When a reset 4 (reload) occurs, the error log is saved on the disk.

Records of the last 16 restarts are retained in the initcauses log in chronological order.

Syntax

```
display initcauses [ schedule ]
```

schedule Specify a time to run the command.

display initcauses field descriptions

Field	Description
Cause	This gives the reason for the system reset as follows: • **Craft Request** — The reset was manually initiated using reset system. • **Initialized** — A power-up. Always the first entry in the log unless more than 15 restarts have occurred since the last power up. • **Interchange** — A State of Health change caused the arbiter process to initiate the restart. • **Interchange-Craft** — An administrative session (session -i command, on-demand interchange) caused the arbiter process to initiate the restart. • **Internal Request** — Software requested the restart, usually in response to a server interchange. Internal request restarts are not initiated in direct response to an error and are non-escalating. • **Software Request** — Software requested the system restart.
Action	The level of recovery performed by the system. 1. **Reset system 1 (Warm)** — Communication Manager software is restarted, and active calls remain up. 2. **Reset system 2 (Cold)** — Communication Manager software is restarted, translations are preserved, and all calls are dropped. 3. **Reset system 4 (Reload)** — Communication Manager software is completely reloaded, and the hardware is reinitialized.
Escalated	**y/n** **y** — The restart was escalated to a higher level than originally attempted. The system's software escalation strategy can perform a higher level restart than the one initiated if problems prevent or conditions interfere with normal execution.
Mode	State of the server immediately after the interchange, at the time of the restart. Look for a change of mode to help determine when an interchange occurred. • **Active** — Mode of a simplex server and for a duplex server that is the active server. • **Standby** — Mode of a standby server in a duplex configuration.

Table continues…

Field	Description
	• **Busyout** — Mode of a standby server that has been placed out-of-service with a **busyout** command.
Time	The month, day, and time of the restart.

See **reset system** for details.

integ-annc-board

list usage integ-annc-board

Use **list usage integ-annc-board** to see information on the announcements and audio groups on an announcement circuit pack.

For more information on 'Announcements/Audio Sources screens and integrated announcement boards', see *Administering Avaya Aura®Communication Manager (03–300509)*.

Syntax

```
list usage integ-annc-board  location
```

location Board location.

list usage integ-annc-board field descriptions

Field	Description
Used By	The type of announcement source on the announcement circuit pack. • **Audio Group** with Audio Group number and Member number. • **Announcement** with Announcement number and Extension.

integ-annc-brd-loc

change integ-annc-brd-loc

Use **change integ-annc-brd-loc** to change all the currently administered 'from' board location to the **to** board location on the ANNOUNCEMENTS/AUDIO SOURCES and AUDIO GROUP screens.

Syntax

```
change integ-annc-brd-loc
```

The **change integ-annc-brd-loc** command does not physically move the announcement files. It only changes the administrative view on CM to the new location.

For example, you cannot use **change integ-annc-brd-loc** to change the location of the announcement files from an internal flash on the gateway to an external compact flash for backup and restore.

ip-board

status ip-board

Use **status ip-board** to see the activity on a board. **status ip-board** has the same syntax and output as **status clan-ip** except the list of allowed boards is larger.

Note:

status ip-board location is a SAT command that cannot be run on the MAPD board.

Syntax

```
status ip-board CCcss
```

CCcss Board location.

status ip-board field descriptions

Field	Description
Incoming datagram header errors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, and errors discovered in processing their IP options. Output type — Counter/Long MIB data — ipInHdrErrors
Outgoing datagrams with no route available	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this **no-route** criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down. Output type — Counter/Long MIB data — opOutNoRoutes

Table continues…

Field	Description
Incoming datagrams received	The total number of input datagrams received from interfaces, including those received in error. Output type — Counter/Long MIB data — ipInReceives
Incoming datagrams discarded	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly. Output type — Counter/Long MIB data — ipInDiscards
Outgoing datagrams submitted for transmission	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams. Output type — Counter/Long MIB data — ipOutRequests
Outgoing data discarded	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion. Output type — Counter/Long MIB data — ipOutDiscards
ICMP Destination unreachable messages	The number of ICMP Destination Unreachable messages received. Output type — Counter/Long MIB data — icmpDestUnreachs
ICMP Redirect message	The number of ICMP Redirect messages received. Output type — Counter/Long MIB data — icmpInRedirects

ip-codec-set

change ip-codec-set

Use **change ip-codec-set** to independently administer codec sets to use media encryption or not.

Syntax

```
change ip-codec-set [ n ]
```

n Codec set number.

change ip-codec-set field descriptions — Page 1

Field	Description
Codec set	1–7 specifies the codec set used between the network regions. If blank, there is no connectivity between the network regions.
Audio codec	Name of the audio codec in this codec-set: • G.711A (a-law) • G.711MU (mu-law) • G.722-64k • G.722.1-24k • G.722.1-32k • G.722.2 • G.723.5.3 • G.723.6.3 • G.726A-32k • G.729 • G.729A • G.729B • G.729AB • SIREN14-24k • SIREN14-32k • SIREN14-48k • SIREN14-S48k • SIREN14-S56k • SIREN14-S64k • SIREN14-S96kk
Silence Suppression	**y/n** Enter **y** to enable RTP-level silence suppression on the audio stream.
Frames Per Pkt	Number of frames per packet up to a packet size of 60 milliseconds (ms). 1–6 or blank. • G.711 default frame size is 2 (20 ms).

Table continues…

Field	Description
	• G.723 default frame size is 3 (30 ms). • G.729 default frame size is 2 (20 ms).
Packet Size (ms)	Size of the packet in milliseconds (ms).
Media Encryption	The options for each codec set apply to all codecs defined in that set. Appears when Media Encryption Over IP is `y` on the system-parameters customer-options screen. Enter the options in the order of preference. Enter `aes` in one of the fields to add AES Media Encryption. • Enter `aes` for Advanced Encryption Standard encryption, standard used by U.S. government to protect sensitive (unclassified) information. Reduces circuit-switched to IP call capacity by 25%. • Enter `aea` for Avaya Encryption Algorithm. Not as secure as AES. Use to encrypt: - all endpoints (except Avaya 46x4 IP Telephones) within a network region using this codec set. - all endpoints communicating between two network regions and using this codec set. • Enter `none` for an unencrypted media stream. Prevents encryption when using this codec set. Default value when Media Encryption Over IP is `y` for the first time on the system-parameters customer-options screen. 1. 1-srtp-aescm128-hmac80 2. 2-srtp-aescm128-hmac32 3. 3-srtp-aescm128-hmac80-unauth 4. 4-srtp-aescm128-hmac32-unauth 5. 5-srtp-aescm128-hmac80-unenc 6. 6-srtp-aescm128-hmac32-unenc 7. 7-srtp-aescm128-hmac80-unenc-unauth 8. 8-srtp-aescm128-hmac32-unenc-unauth • Or leave blank.

change ip-codec-set field descriptions — Page 2

Field	Description
Allow Direct-IP Multimedia	Allows or disallows direct multimedia using the following codecs: • H.261

Table continues…

Field	Description
	• H.263 • H.264 (video) • H.224 • H.224.1 (data, far-end camera control)
Clear-channel Mode	Enables or disables the support for this codec set for BRI data calls.
ECM	If you enter `y`, ECM-capable gateways use the T.38 protocol to relay T.30 ECM signaling and ECM frames between a local Group 3 fax machine and a far-end T.38 receiver. `y` is the default value.
FAX mode	• If you enter `off`, Communication Manager treats a fax call as an ordinary voice call. Turn off special fax handling. • If you enter `relay`, Communication Manager uses the relay mode for fax transmissions over IP network facilities only between Avaya devices. This mode may be coupled with Redundancy. • If you enter `pass-through`, Communication Manager uses the pass-through mode for in-band fax transmissions over IP network facilities only between Avaya devices. This mode may be coupled with Redundancy. • If you enter `T.38-standard`, Communication Manager uses the T.38 protocol for fax transmission over IP network facilities. • If you enter `T.38-G711-fallback`, Communication Manager uses the T.38 protocol for fax transmission only if the protocol can be successfully negotiated with the peer SIP entity. Otherwise, Communication Manager falls back to G.711 for transmission. This mode requires a G.711 codec to be administered on the ip-codec-set screen. **Note:** If you have a telephone on an IP trunk that is close to a fax machine, the telephone can pick up the tones from the fax machine and change into the fax mode. To prevent this, turn off FAX mode and place fax machines in an Automatic Route Selection (ARS) partition that uses only circuit switched trunks, even for inter-gateway fax calls.

Table continues…

Field	Description
Maximum Call Rate for Priority Direct-IP Multimedia	The system displays this field only if **Allow Direct-IP Multimedia** is set to y.
Maximum Call Rate for Direct-IP Multimedia	The system displays this field only if you set the **Allow Direct-IP Multimedia** to y.
Modem Mode	• Enter `off` if you want to use this mode to treat a modem call as an ordinary voice call. Turn off special modem handling. The default mode for new installations and upgrades is off. • Enter `relay` if you want to use this mode for transporting modem traffic over IP using V.32 relay only between Avaya devices. • Enter `pass-through` if you want to use this mode for transporting modem traffic over IP network facilities only between Avaya devices. • Enter `v150mr` if you want to use this mode to use V.150.1 protocol to transmit modem signals between modems and telephony devices. The V. 150.1 Modem-over-IP feature is used to interoperate with secure terminals and third-party SIP gateways.
Redundancy	Use this field to assign the number of duplicate or redundant packets that must be sent in addition to the primary packet. You can enter a value from 1 to 3. The default value is 0. **Note:** For the pass-through and the clear-channel modes, you can assign a value of 0 or 1. If you set the Modem Mode field to v150mr, the system sets the Redundancy field to display-only with the default value of 0.
TDD/ TTY Mode	• Enter `off` to turn off special TTY handling when using this codec set. In this case, the TTY transmission is treated like an ordinary voice call. With a codec set that uses G.711, this setting is required to send TTY calls to non-Avaya systems. However, there might be errors in character transmissions. • Enter `US` to use U.S. Baudot 45.45 mode for TTY transmissions over IP network facilities. This is the default for new installations and upgrades. • Enter `UK` to use U.K. Baudot 50 mode for TTY transmissions over IP network facilities.

Table continues…

Field	Description
	• Enter `pass-through` to use pass-through mode for TTY transmissions over IP network facilities.

change ip-codec-set field descriptions — Page 3

The system displays this page only when you set the **Modem Mode** field to `v150mr`.

Field	Description
Modem Relay Preferred (NoAudio)	If you set this field to y, Communication Manager includes the NoAudio codec in the SIP SDP offer/answer message. You must enable this feature when a gateway interoperates with the devices that support offer/answer NoAudio codec. The default value is n.
Modulation Mode	Avaya V.150.1 supports the V.32, the V.34, the V.90, and the V.92 modem modulations. For users who need other modulations, you must set the Modem Mode field to pass-through. The following fields determine whether V.150.1 is enabled to transport the respective modulations as Modem Relay.
V. 32	• Enter y to enable V.32 modem modulation. The default value is y. • Enter n to disable V.32 modem modulation.
V.34	• Enter y to enable V.34 modem modulation. The default value is y. • Enter n to disable V.34 modem modulation.
V.90	• Enter y to enable the V.90 digital modem modulation. The default value is y. **Note:** The system sets the V.34 field to display-only with the default value y. • Enter n to disable V.90 modem modulation.
V.92	• Enter y to enable the V.92 digital modem modulation. The default value is y. **Note:** The system sets the V.34 field to display-only with the default value y. • Enter n to disable V.92 modem modulation.
SPRT Retransmissions	Use this field to assign the maximum number of data retransmissions to Transport Channel 1 (TC1) and Transport Channel 2 (TC2). You can assign a value from 1 to 32. The default value is 3.

Table continues…

Field	Description
SPRT TC0 Payload Size	Use this field to assign the maximum payload size to SPRT Transport Channel 0. You can enter a value from 140 to 256. The default value is 140 bytes. **Note:** Maximum SPRT payload sizes might vary across different gateways depending on the firmware and the hardware version.
SPRT TC1 Payload Size	Use this field to assign the maximum payload size for SPRT Transport Channel 1. You can enter a value between 132 to 256. The default value is 132 bytes. **Note:** Maximum SPRT payload sizes might vary across different gateways depending on the firmware and the hardware version.
SPRT TC1 Window Size	Use this field to assign the window size to SPRT Transport Channel 1. You can enter a value from 32 to 96. The default value is 32 bytes.
SPRT TC2 Payload Size	Use this field to assign the maximum payload size to SPRT Transport Channel 2. You can enter a value from 132 to 256. The default value is 132 bytes. **Note:** Maximum SPRT payload sizes might vary across different gateways depending on the firmware and the hardware versions.
SPRT TC2 Window Size	Use this field to assign the window size to SPRT Transport Channel 2. You can enter a value from 8 to 32. The default value is 8 bytes.
SPRT TC3 Payload Size	Use this field to assign the maximum payload size to SPRT Transport Channel 3. You can enter a value from 140 to 256. The default value is 140 bytes. **Note:** Maximum SPRT payload sizes might vary across different gateways depending on the firmware and the hardware version.
SPRT Timer TC1-TA01	Use this field to set the value of the acknowledgement timer of Transport Channel 1. You can enter a value from 50 to 150 in increments of 10. The default value is 90.
SPRT Timer TC1-TA02	Use this field to set the value of the acknowledgement update timer of Transport

Table continues…

Field	Description
	Channel 2. You can enter a value from 50 to 1000 in increments of 10. The default value is 130.
SPRT Timer TC1-TR03	Use this field to set the value of the retransmit timer of Transport Channel 1. You can enter a value from 50 to 1000 in increments of 10. The default value is 500.
SPRT Timer TC2-TA01	Use this field to set the value of the acknowledgement timer of Transport Channel 2. You can enter a value from 50 to 150 in increments of 10. The default value is 90.
SPRT Timer TC2-TA02	Use this field to set the value of the acknowledgement update timer of Transport Channel 2. You can enter a value from 50 to 1000 in increments of 10. The default value is 500.
SPRT Timer TC2-TR03	Use this field to set the value of the retransmit timer of Transport Channel 2. You can enter a value from 50 to 1000 in increments of 10. The default value is 500.
SSE Inter-Packet Interval	Use this field to assign an interval between the State Signaling Events (SSE) packets. You can enter a value between 10 to 40 with the increments of 10. The default value is 20 mSec.
SSE Repetition Redundancy (Packets)	Use this field to assign the number of redundant SSE packets for transmission. The redundancy option provides robust transport of data packets across an IP-based network. You can enter a value from 0 to 3. The default value is 3.
V.42 error correction	V. 42 is an error correction protocol for V.150.1 media transport between modems. If you set this field to y, the gateways to use the V.42 error correction protocol. The default value is n.

ip-interface

change ip-interface

Use **`change ip-interface`** to see the IP-Interfaces report.

Options: You can change the value in the Enable Voice/Network Stats? from `n` (No) to `y` (Yes). The default value for Enable Voice/Network Stats? field is **n**.

Syntax

```
change ip-interface[ cabinet | carrier | slot ] or [ procr ]
```

cabinet	Cabinet location.
carrier	Carrier location.
slot	Slot location.
procr	Status of administered v4 and v6.

change ip-interface field descriptions

Field	Description
Enable VoIP/ Network Thresholds?	Enables/disables the record of Voice/Network Statistics at a single media processor board level (applies to both TN2602 boards, if duplicated).
Packet Loss (%)	Unacceptable packet loss coming into the administered media processor board.
Jitter (ms)	Unacceptable disturbance for the administered media processor board. Jitter is based on RTCP that is, time stamp and expected arrival times of packets.
RT Delay (ms)	Elapsed time for a packet to reach remote location and revert. (Round Trip Delay)

list ip-interface

Use the **list ip-interface** command to view the information on media processor and IP media resource interfaces in the system.

Syntax

```
list ip-interface [ val | clan region x| medpro region x| all region x]
```

val	The information of all VAL IP interfaces.
clan	The information of all C-LAN IP interfaces.
clan region *x*	The information of all C-LAN IP interfaces in the network region. The network region number ranges from **1** to **250**.
medpro	The information of all media processor IP interfaces.
medpro region *x*	The information of all media processor IP interfaces in the network region. The network region number ranges from **1** to **250**.
all	The information of all media processor and media resource IP interfaces.

all region *x* The information of all media processor and media resource IP interfaces in the network region. The network region number ranges from **1** to **250**.

list ip-interface field descriptions

Field	Description
ON	**y** — allows use of the Ethernet port.
Type	Type of IP interface. This field appears for **`list ip-interface all`** and **`list ip-interface all`** region *x*.
Slot	Physical port location of the IP interface.
Code/Sfx	TN identification of the circuit pack for the IP interface. Suffix identification of the circuit pack for the IP interface.
Node Name/ IP Address/ Gateway Node	Node name for the IP interface administered on the Node Names screen. The IP address of the IP Interface. For **`list ip-interface medpro`**, the IP Address and Subnet Mask fields are combined. Address of a network node that serves as the default gateway for the IP interface.
Mask	Subnet mask associated with the IP address for the IP interface. The subnet mask is a 32-bit binary number that divides the network ID and the host ID in an IP address.
Num Skts Warn	Threshold number of sockets in use for IP endpoint registration on the C-LAN before a warning message is logged. This field appears for **`list ip-interface clan`**.
Net Rgn	Network region number for the IP interface.
VLAN	This field sends VLAN instructions to C-LAN and Media Processor boards. It does not send VLAN instructions to IP endpoints such as IP telephones and softphones. This field cannot be administered for VAL boards.
Dup	**n** — the IP interface circuit is not duplicated **y** — the IP Media Resource 320 circuit pack is duplicated. The next board in this list is the associated duplicated IP Media Resource 320 circuit pack. If media processor boards are not duplicated, **n** is displayed in this column.
Virtual Address	The virtual address of the duplicated TN2602 (Crossfire) circuit pack pair. This field appears on **`list ip-interface medpro`** for duplicated TN2602 circuit packs.

Example

```
list ip-interface val
list ip-interface clan
list ip-interface clan region 168
```

```
list ip-interface all
list ip-interface all region 29
```

ip-network-region

change ip-network-region

Use **change ip-netowrk-region** to change the audio and Quality of Service (QoS) attributes of IP network region *x*, where *x* is a network region number, or to change the codec set used for connections from network region *x* to other network regions.

To troubleshoot broken inter-network region connectivity, see **status ip-network-region**, **display failed-ip-network-region** and **test failed-ip-network-region**.

Syntax

```
change ip-network-region x
```

x Region number.

See *Administering Network Connectivity on Avaya Aura®Communication Manager (555-233-504)* for administration guidelines.

list ip-network-region

Use **list ip-network-region** to list the administered network connections.

Syntax

```
list ip-network-region[monitor | direct-wan x]
```

monitor List the administered network connections.

direct-wan *x* List the network regions that are directly connected to the network region. The network region number ranges from **1** to **2000**.

status ip-network-region

Use **status ip-network-region** to see the status of the administered network connections between network region *x* and other network regions.

Syntax

```
status ip-network-region x ]
```

x IP network region number.

status ip-network-region field descriptions

Field	Description
Src Rgn	Source Region number
Dst Rgn	Destination region
Conn Type	Type of connection • direct • indirect
Conn Stat	Status of connection • pass • fail
BW-Limits	Bandwidth and limits as administered with **add ip-network-region**
BW-Used (kbits) Tx	Bandwidth used for transmission, direct connections only
BW-Used (kbits) Rx	Bandwidth used receiving, direct connections only
# Connections Tx	Number of transmission connections, direct connections only
# Connections Rx	Number of receiving connections, direct connections only
#Times BW-Limit hit Today	Number of times the CAC threshold limits reached since the previous midnight, direct connections only
IGAR Now IGAR Today	The number of active IGAR connections for the pair of Network Regions/ The number of times IGAR has been invoked for the pair of Network Regions since the previous midnight.

duplicate ip-network-region

Use **duplicate ip-network-region** to create duplicate network regions of an existing stub network region.

Syntax

```
duplicate ip-network-region x ] [-e extension]
```

x Stub network region to duplicate.

y Starting range of the new stub network region.

z Number of duplicate stub network regions that you can create. You can duplicate a maximum of 16 stub network regions.

ip-route

list ip-route

Use **list ip-route** to list the IP routes from DEFINITY ECS out to the LAN. Enter the board parameter to list the IP routes for a specific C-LAN circuit pack, for example, **list ip-route board** *location*.

Syntax

```
list ip-route  [ board location ]
```

board *location* Physical location of the circuit pack.

list ip-route field descriptions

Field	Description
Route Number	IP route number
Destination Node	Destination of the route. The name is administered on the Node Name screen and can include the keyword `Default` indicating the default route. The Destination Node field supports the V6 node names.
Gateway	The node name of the Gateway through which the destination is to be reached. The Gateway is a name administered on the Node Name screen. The Gateway field supports the V6 node names.
Subnet Mask	The destination IP subnet address. Identifies which portion of an IP address is a network address and which is a host identifier.
C-LAN Port	Indicates the C-LAN port location that provides the interface for the route.
Metric	Specifies the desirability of the IP route in terms of the efficiency of data transmission over the route. Valid entries are 0 (a simple route) and 1 (a complex route). A metric value of 1 is used only when the switch has more than one C-LAN board installed. A metric-1 route diverts usage of the route to a metric-0 route, if available.
Network Bits	
Accepted by C-LAN	Indicates whether a C-LAN circuit pack has accepted the administered IP-route. Routes for a link are downloaded to the C-LAN circuit pack when the link comes into service. Possibilities include: • **accepted** — the route has been accepted by the C-LAN circuit pack. • **rejected** — the route has been rejected by the C-LAN circuit pack. The Gateway may not be on the attached ethernet subnet or may not be the IP address of the far end of the PPP link.

Table continues…

Field	Description
	• **pending** — the route has not been sent to the C-LAN circuit pack, or it has been sent but no reply has been received. Typically, this status changes to `accepted` or `rejected` when some condition changes, such as a link coming up. • **obsolete** — the route is no longer needed (some host routes were needed in R7 but are no longer needed in subsequent releases, or are duplicates of existing routes).

netstat ip-route

Use **`netstat ip-route`** to see the routing tables that are resident in the C-LAN and/or VAL circuit packs. Without the board option, all C-LAN and VAL circuit packs are displayed. With the board option, only the specified C-LAN or VAL circuit pack appears.

Syntax

```
netstat ip-route  [ board location ]
```

board *location* Specific C-LAN or VAL circuit pack.

(none) — Display routing tables for all C-LAN and VAL circuit packs.

netstat ip-route field descriptions

Field	Description
Bd/Pt	The circuit pack location for the pack that provides the interface for the route.
Destination	Fixed field giving the destination of the route. The destination is a name administered on the Node Name screen which can include the keyword **Default**, indicating the default route.
Gateway	The node name of the Gateway by which the Destination can be reached. The Gateway must be a name administered on the Node Name screen.
Subnet Mask	Subnet mask information entered on the IP Interfaces screen.
Intfc/Err	• **pppn** — represents one of the PPP interfaces on the C-LAN, which is administered as port n+1. • **cpm0** — represents the ethernet interface on the C-LAN which is administered as port 17. • **motfec0** — represents the internet interface on the VAL circuit pack, which is administered as port 33. • **lo0** — represents the loopback interface on the C-LAN or VAL. • **LPBK_IP** — Loopback request failed, typically because the RSCL is down. • **Timeout** — Query timed out.

Table continues…

Field	Description
	• **SNMP** — SNMP call failed. • **BD BUSY** — Board was busied out.

refresh ip-route

Occasionally, tables that route IP messages become corrupted and/or contain stale routes which will delay packet delivery. Use **refresh ip-route** to remove dynamic (learned) routes from C-LAN circuit pack route tables and replace any administered routes that have been corrupted.

Syntax

```
refresh ip-route [ all | board location ]
```

all Refreshes route tables in all C-LAN circuit packs.

board *location* Refreshes ip-route tables in a specific C-LAN circuit pack.

refresh ip-route field descriptions

Field	Description
Board Location	The physical location of the C-CLAN circuit pack.
Routes Deleted	Number of routes that were deleted from the C-LAN route tables.
Routes Added	Number of routes that were added from the C-LAN route tables.
Failure Reason	The refresh failed for the following reasons: • **Add** — Adding a route failed. • **Delete** — Deleting a route failed. • **Loopback** — Failed to acquire loopback address. RSCL is probably down. • **Brd Busy** — the CLAN-BD has been busied out. • **SNMP** — SNMP query to the board failed. • **Timeout** — SNMP query timeout.

ipserver-interface

add ipserver-interface

Use **add ipserver-interface** to administer a port-network n to be IPSI controlled.

Syntax

```
add ipserver-interface x
```

x Port network

Description

See **change ipserver-interface** for field descriptions.

busyout ipserver-interface

Use **busyout ipserver-interface** to force an IPSI circuit pack to be out of service.

Caution:

Busying out an IPSI board takes down the port network.

Syntax

```
busyout ipserver-interface Uc
```

Uc Cabinet number and carrier for the server

Description

If the IPSI is not duplicated:

- **busyout** causes a fallback to traditional control where the Expansion Interface is the ArchAngel
- PKT-INT functionality is moved to an IPSI in another port network

If the IPSIs are duplicated in the port network (the required argument is a cabinet/carrier):

- the active IPSI cannot be busied out
- the standby Tone-Clock is busied out

change ipserver-interface

Use **change ipserver-interface** to change the QoS parameters, the IPSI circuit pack, and socket encryption.

Syntax

```
change ipserver-interface x
```

x Port network

change ipserver-interface field descriptions

Field	Description
IP Control	**y** — All port networks have an IPSI that provides control. • Display-only, if IP-PNC is y on the display system-parameters customer-options screen **n** — This IPSI is used only for Tone Clock / Tone Detector functions • Remaining fields on this screen do not display when IP Control is **n** and IP-PNC is **n** on the display system-parameters customer-options screen • **n** when the port network contains a DS1 Converter (DS1C) circuit pack
Encryption	Enter **y** to turn on socket encryption for the server and IPSI link.
Primary IPSI	
DHCP?	DHCP client identifier **y** — The DHCP client identifier is populated. This is a display-only value. **n** — The DHCP client identifier is not populated.
Host	Name of the host computer. The Host field supports the IPv6 addresses.
Location	Location of the IPSI board.
Subnet Mask	If you have set the value of DHCP to **y**, the Subnet Mask value is read-only (if applicable for users to see). If you have set the value for DHCP as **n** and attempt to change the Subnet Mask value, upon form validation, check if the IP server is busied out. If IP server is not busied out, the system does not accept the changes and displays the message — `ipserver must be busied out`.
IP Address	If you have set the value of DHCP to **y**, the IP address value is read-only. If you have set the value for DHCP as n and attempt to change the IP Address value, upon form validation, check if the ip server is busied out. If ip server is not busied out, the system does not accept the changes and displays the message — `ipserver must be busied out`.
Gateway	If you have set the value of DHCP to **y**, the Gateway value is read-only. If you have set the value for DHCP as n and attempt to change the Gateway value, upon form validation, check if the IP server is busied out. If IP server is not busied out, the system does not accept the changes and displays the message — `ipserver must be busied out`.

Table continues…

Field	Description
Secondary IPSI	
DHCP?	DHCP client identifier • **y** — The DHCP client identifier is populated. This is a display-only value. • **n** — The DHCP client identifier is not populated.
Host	Name of the host computer.
Location	Location of the IPSI board
Subnet Mask	If you have set the value of DHCP to **y**, the Subnet Mask value is read-only (if applicable for users to see). If you have set the value for DHCP as **n** and attempt to change the Subnet Mask value, upon form validation, check if the IP server is busied out. If IP server is not busied out, the system does not accept the changes and displays the message — `ipserver must be busied out`.
IP Address	If you have set the value of DHCP to **y**, the IP Address value is read-only. If you have set the value for DHCP as **n** and attempt to change the IP Address value, upon form validation, check if the IP server is busied out. If IP server is not busied out, the system does not accept the changes and displays the message — `ipserver must be busied out`.
Gateway	If you have set the value of DHCP to **y**, the Gateway value is read-only. If you have set the value for DHCP as **n** and attempt to change the Gateway value, upon form validation, check if the IP server is busied out. If IP server is not busied out, the system does not accept the changes and displays the message — `ipserver must be busied out`.
QoS and Ethernet Settings	
Use System QoS Values?	If set to **y**: 802.1p and DiffServ fields are displayed. The values for these fields are read-only. If you attempt to change the values, the system displays the following message: `value set in system-parameters ipserver-interface`. If set to **n**: 802.1p and DiffServ fields are displayed. The values for these fields are modifiable. • 802.1p default value is 6. Range for 802.1p is 0–7 (null value not permitted). • DiffServ default value is 46. Range for DiffServ is 0–63 (null value not permitted).

Table continues…

Field	Description
802.1p	This value is downloaded to the IPSI. This value is the priority value and does not enable 802.1p. You must enable 802.1p from the IPSI CLI interface. The default value for 802.1p is 6 and the range is 0–7 (whole numbers).
DiffServ	This value is downloaded to the IPSI and applied to Communication Manager, from the IPSI to CM and vice versa.
Auto?	If set to **y**, the Speed and Duplex fields do not display. If set to **n**, the Speed and Duplex fields are displayed. The default values are: • Speed — 100Mbps • Duplex — Full If the IP server is not busied out, the values are read-only. If you attempt to change the values, the system displays a message — `ipserver must be busied out.` If the IP server is busied out, you can change the values.
Speed	If the IP server is not busied out, this value is read-only. If you attempt to change this value, the system displays a message — `ipserver must be busied out.` If the IP server is busied out, you can change the value. The default value is 100 Mbps. Range is 10–100Mbps.
Duplex	If the IP server is not busied out, the value is read-only. If you attempt to change the value, the system displays a message — `ipserver must be busied out.` If the IP server is busied out, you can change the value.
QoS and Ethernet Settings	
Use System QoS Values?	If set to **y**: The 802.1p and DiffServ fields are displayed. The values for these fields are read-only. If you attempt to change the values, the system displays the following message — `value set in system-parameters ipserver-interface`. If set to **n**: The 802.1p and DiffServ fields are displayed. The values for these fields are modifiable. • 802.1p default value is 6. Range for 802.1p is 0–7 (null value not permitted). • DiffServ default value is 46. Range for DiffServ is 0–63 (null value not permitted).

Table continues…

Field	Description
802.1p	This value is downloaded to the IPSI. This value is the priority value and does not enable 802.1p. You must enable 802.1p from the IPSI CLI interface. The default value for 802.1p is 6 and the range is 0–7 (whole numbers).
DiffServ	This value is downloaded to the IPSI and applied to communication manager from the IPSI to CM and from CM to the IPSI.
Auto?	If set to **y**, Speed and Duplex fields do not display. If set to **n**, Speed and Duplex fields are displayed. The default values are: • Speed – 100Mbps • Duplex – Full If the IP server is not busied out, the values are read-only. If you attempt to change the values, the system displays a message — `ipserver must be busied out.` If the ipserver is busied out, you can change the values.
Speed	If the IP server is not busied out, this value is read-only. If you attempt to change this value, the system displays a message — `ipserver must be busied out.` If the IP server is busied out, you can change the values. The default value is 100 Mbps. The range of the value is 10–100Mbps.
Duplex	If the IP server is not busied out, the value is read-only. If you attempt to change the value, the system displays a message — `ipserver must be busied out.` If the IP server is busied out, you can change the values.

display ipserver-interface

Use **`display ipserver-interface`** to see administration data for a port-network to be IPSI controlled.

Syntax

```
display ipserver-interface x [ schedule ]
```

x Port network (1–64)

schedule

Description

See **`change ipserver-interface`** for field descriptions.

get forced-takeover ipserver-interface

Use **get forced-takeover ipserver-interface** to manually take control of IPSI port networks.

Caution:

Moving a port network from one server to another causes a level 2 reset of the Port Network. This resets every board in the port network and drops any established calls carried by the port network. Shuffled IP calls are not dropped, but during the reset they will not have access to any features such as Hold, Transfer, Conference, etc.

Syntax

```
get forced-takeover ipserver-interface [ all | port-network n <1-64>]
```

schedule (Optional) Specify a start time for the command.

Description

get forced-takeover ipserver-interface is issued from the server intended to control the port network.

If the Port Network targeted by get forced-takeover ipserver-interface is already controlled by the Main server or Survivable Core Server where the command is issued, Test #1605 will immediately PASS.

If the Port Network is not controlled by the Main server or Survivable Core Server where get forced-takeover ipserver-interface is issued, the server shows the test result as IN PROGRESS.

Important:

On a Survivable Core Server administered as Local Only, the **get forced-takeover ipserver-interface** command will only attempt to gain control of port networks with the same community number as the Local Only server.

See survivable-processor and system-parameters port-networks for Local Only and community assignments.

A test result of IN PROGRESS will be shown for Port Networks in other communities, but the **get forced-takeover ip-server** command will not attempt to gain control of these Port Networks.

Use **status ess port-networks** or **list ipserver-interface** to verify that the **get forced-takeover ipserver-interface** command was successful.

Error Codes

The following table contains a description for the Error Codes which may be returned from Test 1605:

Error Code	Description
1995	Survivable Core Server cluster is disabled

Table continues…

Error Code	Description
1996	Port network does not exist
1997	Not an IPSI port network

list ipserver-interface

Use **list ipserver-interface** to list all administered IPSIs in the system.

Syntax

```
list ipserver-interface [ schedule ]
```

schedule (Optional) Specify a start time for the command.

list ipserver-interface field descriptions

Field	Description
Serv State	Shows the current service state: busy out, in service, out of service
Control State	active or standby
Primary/ Secondary IP Address	n/a if the IPSI is not in control. All other fields are blank. The Primary/ Secondary IP Address field and the Primary/Secondary Host Name field supports the IPv6 addresses.
State of Health C P E G	Shows the state of health of the clock (C), packet interface (P), the expansion archangel link (E), and the Tone Generator (G) 0=healthy, 1=unhealthy

list measurements ipserver-interface

Use **list measurements ipserver-interface** to add monitoring to the IP Server Interface (IPSI)–Packet Control Driver (PCD) socket to identify and troubleshoot network-related problems.

Syntax

```
list measurements ipserver-interface hourly [ 1-64 | schedule ] | summary  [ yesterday-peak | today-peak | last-hour ]
```

Description

You can assess the health of the IPSI socket and its underlying network connection by using the **list measurements ipserver-interface** command and the corresponding SAT display. The round-trip delay information between the PCD and the IPSI is an indicator of the network health and includes the average, maximum, and threshold-exceeded values. The IPSI socket sanity timeout values are also included to show occurrences of the IPSI socket bounce. The throughput from the PCD and IPSI and from the IPSI and PCD are listed under the downlink and uplink traffic rates respectively. The IP Server Interface report shows activity on network ports for a specified hour or on a summary basis for today or yesterday, peak or worst periods.

list measurements ipserver-interface field descriptions

Field	Range/ Default	Description
Network Delay RTT Avg.	0–9999	Network Delay Round-Trip Time (RTT) in milliseconds. It is the measure of the sample time for packets to go back and forth and averaged per hour between the PCD and IPSI.
Network Delay RTT Max	0–9999	Network Delay Round-Trip Time (RTT) in milliseconds. It is the measure of the hourly maximum sample time for packets to go back and forth between the PCD and IPSI.
Network Delay CNT > 300	0–9999	Network Delay Count of how many times within an hour the sample delay was greater than 300 milliseconds.
Network Indicator HB MSD	0–3600	Network Indicator HeartBeats Missed measures how many once per second “heartbeats” between the IPSI and PCD were missed.
Network Indicator Ntwk Outg	0–1800	Network Indicator Network Outage measures the number of times there was at least a one second outage.
Network Indicator Outg > 3s	0–1200	Network Indicator Network Outage > 3 seconds (subset of number above) measures the number of times there was an outage of greater than 3 seconds duration.
Network Indicator SNTY TO	0–999	Network Indicator Sanity Timeout (subset of number above) measures the number of times there was an outage greater than the value administered for the “IPSI Socket Sanity Timeout” (4–15 seconds). If a value is not administered, this number is the same as the preceding column.
Throughput Down	0–999.9	Throughput for the downlink. This measures the “application” level traffic from CM to IPSI in kilobytes per second (KBps). Not included are the IP and TCP headers or retransmission traffic. Data is shown to the nearest tenth of a decimal place, rounded up if there is any traffic. If there is no traffic, a 0 is displayed.
Throughput Up	0–999.9	Throughput for the uplink. This measures the “application” level traffic from IPSI to CM in kilobytes per second (KBps). Not included are the IP and TCP headers, or retransmission traffic. Data is shown to the nearest tenth of a decimal place, rounded up if there is any traffic. If there is no traffic, a 0 is displayed.

release ipserver-interface

Use **release ipserver-interface** to return an IPSI circuit pack to service after it has been busied out.

Syntax

```
release ipserver-interface UUc
```

UUc The cabinet/carrier location of the IPSI board to be released.

remove ipserver-interface

Use **remove ipserver-interface** to remove a port network from IPSI control.

Syntax

```
remove ipserver-interface x
```

x Port network (1–64)

remove ipserver-interface field descriptions

Field	Description
Socket Encryption	y/n Indicates whether socket encryption is turned on or off for the duplex server pair and IPSI link.
Enable QoS	y/n Indicates whether quality of service (QoS) is turned on or off.
Primary IPSI	
Location	Location of the IPSI board
Host	Name of the host computer
DHCP ID	DHCP client identifier
Secondary IPSI: These fields are displayed	
Location	Location of the IPSI board
Host	Name of the host computer
DHCP ID	DHCP client identifier
QoS Parameters	
Call Control 802.1p	Call priority setting (1-7)
Call Control DiffServ	DiffServ code point (DSCP)

reset ipserver-interface

Use **reset ipserver-interface** to reset an IPSI in the named cabinet/carrier.

Syntax

```
reset ipserver-interface UUc
```

UUc The cabinet/carrier location of the IPSI board to be reset.

set ipserver-interface

Use **set ipserver-interface** to set a specified IPSI to be active for a given cabinet carrier.

Syntax

```
set ipserver-interface UUc | a-all | b-all
```

UUc The cabinet/carrier location of the IPSI board to be released.

a-all Sets all “a” side IPSIs active.

b-all Sets all “b” side IPSIs active.

Description

Use set **ipserver-interface** a-all or b-all to set all the a- or b-side IPSIs in the control network to be active. This is useful in preparation of hub/subnet maintenance.

Use **list ipserver-interface** to see the IPSI Control State and verify that the interchange occurred. See the IPSV-CTL (IP Server Interface Control) section on *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers* for additional information on any error codes that occur.

test ipserver-interface

Use **test ipserver-interface** to perform a board test for an IPSI in the named cabinet/carrier. It tests all clock and PKT-INT components.

Syntax

```
test ipserver-interface Uc
```

Uc Cabinet and carrier you want to test.

ip-stations

reset ip-stations

Use **reset ip-stations** to simultaneously unregister and reset all IP endpoints on a system, or a certain group of IP stations. You can limit the reset to only IP phones, to IP phones in a specific network region, to all IP endpoints in a specific network region, or within a range of ip addresses. Each defined ip station receives a reset message and is unregistered.

Use **reset ip-stations** to initiate simultaneous firmware upgrades to many IP stations, or a certain group of IP stations. You can reset IP stations on one ip-network region to prevent overloading a system with large numbers of IP station resets.

Syntax

```
reset ip-stations [ ip-phones | all | tti ] [ ip-network-region n | all-regions
| ipaddr n n ]
```

ip-phones	Reset IP phones only.
all	Reset all IP endpoints.
tti	Reset phones in TTI state only.
ip-network-region *n*	Reset IP endpoints in specified IP network region.
all-regions	Reset IP endpoints in all network regions.
ipaddr *n n*	Reset IP endpoints within an IP address range.
status	Verify if the **reset ip-stations** command is completed in the background.
type 4620 all-ip	Reset a specified IP phone type only.
unauth all-ip	Reset all unauthenticated IP stations.

Example

```
reset ip-stations ip-phones
reset ip-stations ip-network-region 2
reset ip-stations ip-phones ip-network-region 2
reset ip-stations ip-phones ipaddr 135.9.76.70 135.9.77.70
reset ip-stations status
reset ip-stations type 4620 all-ip
reset ip-stations unauth all-ip
```

Use **reset ip-stations** to reset H.323 stations including:

- IP phones
- IP soft phones
- IP agents
- IP e-consoles
- All endpoints that appear as IP stations to Communication Manager.

When **reset ip-stations** is issued:

- The system unregisters each station.
- Each station individually resets.
- **Command completed successfully** appears immediately on the screen. However, not all IP stations have already been reset.
- An event is logged in the Events Report (**display events**).

If **reset ip-stations** is executed a second time before all stations have reset, **Command already running. Please try again later** appears. When **reset ip-stations** is submitted, the **Command completed successfully** message appears, but all the resets are not complete. If the system resets while **reset ip-stations** is running, resubmit the command to restart the process.

reset ip-stations feature interactions

Network regions

When setting up IP-network regions, you must take into account the number of IP endpoints assigned to each region. Network regions are associated with specific media processing resources. Administer IP-network regions to a size that DHCP and TFTP servers can handle, and limit the performance impacts of simultaneously resetting large numbers of IP stations.

Duplicated systems

In duplicated systems, submit **reset ip-stations** on the processor where the IP endpoints are registered. For example, if there are IP endpoints registered to both a main processor and a Survivable Remote Server, and **reset ip-stations** is run on the main processor, the IP endpoints registered to the Survivable Remote Server are not reset. This also applies on G3R only to IP stations registered to C-LANs controlled by an ATM WAN Spare Processor, and C-LANS controlled by the processor on a Survivable Remote EPN.

ip-synchronization

status ip-synchronization

Use **status ip-synchronization** to see the information about the status of the various gateways that are part of IP synchronization.

Syntax

```
status ip-synchronization [ master | member [ media-gateway | port-network ] n |
oos-members | source [ media-gateway | port-network ] n | system-information ]
```

master	Master sync sources in the system.
member media-gateway | port-network *n*	Timing source for a given gateway or port-network.
oos-members	Members who are not synchronized and their service states.
source media-gateway | port-network *n*	All gateways and port-networks whose sync is sourced by the given gateway.
system-information	Global status of the sync over IP feature.

status ip-synchronization field descriptions — system information

Field	Description
Master domain count	Number of master IP sync domain count
Total domain count	Number of overall IP sync system count
Member count	Number of gateways in sync domains
Max level	Highest hop count by any member
Out of Sync	Number of members not in sync
Building domains	Indicates whether the new sync domains are created after the feature flag is turned on. When the field is set to **n**, the process is finished.
Removing domains	Indicates if the feature is removing the IGC streams and sync domains when the feature is turned off.

status ip-synchronization field descriptions — source | member [media-gateway | port-network]

Field	Description
Member	Displays all master sources of the system
Ref Stat	Displays the health of the reference board, whether the member is in service and setup to source IGC streams
DSP Status	Displays the status of the DSP
Input	Provides information about the incoming IGC stream
Inp	• **R** – Receiving stream • **N** – No stream detected • **D** – Stream detected
Jit	Jitter detected
Bad	Bad packets detected
Ord	Out of order packets detected
Dup	Duplicated packets detected
Loss %	Percentage loss of incoming stream
Output Lock	Provides information about the outgoing IGC stream. • **Yes** – Locked to input • **No** – Not locked, no output • **Pnd** – Pending lock • **S** – (sync) Indicates if the sync lead is connected
Sync ref	Displays whether the clock is synchronized to the synch lead of the PN and MG
Tandem	Displays whether the member is a tandem clock

status ip-synchronization field descriptions — oos-members

Field	Description
Member	Displays all master sources of the system
Ref Stat	Displays the health of the reference board, whether the member is in service and setup to source IGC streams
DSP Status	Displays the status of the DSP
Input	Provides information about the incoming IGC stream
Inp	• **R** – Receiving stream • **N** – No stream detected • **D** – Stream detected
Jit	Jitter detected
Bad	Bad packets detected
Ord	Out of order packets detected
Dup	Duplicated packets detected
Loss %	Percentage loss of incoming stream
Output Lock	Provides information about the outgoing IGC stream. • **Yes** – Locked to input • **No** – Not locked, no output • **Pnd** – Pending lock • **S** – (sync) Indicates if the sync lead is connected
Sync ref	Displays whether the clock is synchronized to the synch lead of the PN and MG
Role	Displays the role of the member
Reason fail	Displays why the member is out of synch with other members

isdnpri-testcall

clear isdnpri-testcall

Use **clear isdnpri-testcall** to cancel in-progress ISDN-PRI test calls. Once a running test call is cleared, another can begin.

Syntax

```
clear isdnpri-testcall [ group number / member number ]
```

group number Trunk group number.

Comments on this document? infodev@avaya.com

member number Member within the trunk group.

Example

```
clear isdnpri-testcall  80 / 1
clear isdnpri-testcall 78 / 2
```

list isdnpri-testcall

Use **list isdnpri-testcall** to display the ISDN-PRI trunks currently in use for outgoing ISDN test calls.

Syntax

```
list isdnpri-testcall [ schedule ]
```

schedule Specify a time to run the command.

list isdnpri-testcall field descriptions

Field	Description
B-Channel	The trunk-group number and member number of the trunk in use.
Start Time	Day of the month, hour and minute when the test call began.
Duration	Expected duration, in minutes, of the test call.
M/T Port	Cabinet, carrier, slot and circuit number of the port on the Maintenance/Test circuit pack in use for the outgoing test call.

status isdnpri-testcall

Use **status isdnpri-testcall** to display the progress of an outgoing ISDN-PRI test call on the specified trunk. The tested ISDN-PRI B-channel's port number, bit error rate, number of bits transmitted, block error rate, number of blocks transmitted, start time, duration specified, duration of test call, and reason of termination are displayed on the status screen.

Syntax

```
clear isdnpri-testcall [ group number / member number ]
```

group number Administered trunk group number.

group member number Administered group member within the trunk group.

status isdnpri-testcall feature interactions

If the bit error rate or block error rate is greater than zero, the ISDN-PRI trunk **may** be in a troubled state. Based on the statistical information displayed on the terminal, it can be decided to take the ISDN trunk out of service. This is subjective data because the ISDN trunk may be used for data or voice. If the trunk is used for data and the rates are high, the trunk should be taken out of service. If

the trunk is used for voice, the trunk may not have to be taken out of service. High rates may also be due to some type of power hit on the line.

status isdnpri-testcall field descriptions

Field	Description
Port	This field specifies the physical address of the ISDN-PRI B-channel.
Bit Error Rate	The measured bit error count according to the comparison of the sent and received bit pattern. The number appears in scientific notation.
Number of Bits Generated	The number of bits generated. The number appears in scientific notation.
Block Error Rate	The measured block error count according to the comparison of the sent and received bit pattern. The number appears in scientific notation.
Number of Blocks	The number of blocks generated. The number appears in scientific notation.
Start Time	The time the test call started (dd/hh:mm).
Duration Specified	The duration specified in minutes for how long the test call should run. Valid durations are 1-120 (minutes) or blank (to indicate the default amount of minutes was used to run the test).
Duration of Test	The duration specified in minutes for how long the test call has been running. A blank indicates that the default amount of time was used to run the test.
Reason of Termination	The reason of termination indicates why the test call has terminated. Valid reasons of termination are: • **finished** — the test finished in the specified time. • **canceled** — the test call has been canceled with **clear isdnpri-testcall**. • **overflow** — the bits transmitted have overflowed buffer allocation. • **no bits** — no bits have been received because the ISDN-PRI test call circuit connection is bad. • **transmission** — there has been a data transmission interruption, probably caused from a power hit. • **internal fail** — there is an internal error on the Maintenance/Test circuit pack. • **in progress** — the test is still running. • **data corrupt** — used for any other error condition.

Example

```
status isdnpri-testcall  78 / 1
```

test isdnpri-testcall

Use **test isdnpri-testcall** to start an outgoing ISDN-PRI test call.

Only one ISDN trunk in each port network can be tested at one time. The maximum number of asynchronous outgoing test calls that can be run simultaneously depends on the number of maintenance/test circuit packs in the system.

Syntax

```
test isdnpri-testcall  [ group number / member number ] [ minutes  num-minutes ] [ schedule ]
```

group number	Administered trunk group number.
member number	Administered member within the trunk group.
minutes *num-minutes*	Specify the duration of the test call in minutes from 1 to 120. The duration defaults to 8.4 or 9.6 seconds.
schedule	Specify a time to run the command.

For more information, see 'Test #258 under the ISDN-TRK (DS1 ISDN Trunk)' section in the *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*.

Example

```
test isdnpri-testcall  78 / 2 minutes 10
```

Table 7: test isdnpri-testcall output field descriptions

Field	Description
Result	**PASS** — The test call was successfully initiated. **ABORT** — Resources were not available (for example, a B-channel or maintenance/ test circuit pack). **FAIL** — An outgoing test call could not be initiated.

journal-link

status journal-link

Use **status journal-link** to see the operational status of a wakeup-log or a pms-log printer link. If the link is down, the number of times the switch has tried to re-establish the link will be shown.

A journal printer is used to document automatic wake-up events, emergency access to attendant events and, if the Property Management System is not functional, housekeeping events. When the system includes two printers, one is for the housekeeping events and the other is used for automatic wake-up events and emergency access events.

See **status link** for more details on links.

Syntax

```
status journal-link [ wakeup-log |  pms-log ]
```

wakeup-log Status the printer that handles automatic wakeup events, emergency access events, and scheduled reports.

pms-log Status the printer that handles housekeeping events while the PMS is down.

status journal-link field descriptions

Field	Description
Link State	The operational status of the link: • **up** — normal operational state, the link is established and is capable of supporting the application. • **down** — link is physically down. • **extension not administered** — extension number for the printer has not been assigned on the hospitality system parameters.
Maintenance Busy	Whether there is any maintenance testing being performed upon the link.

Example

```
status journal-link  wakeup-log
status journal-link pms-log
```

journal-printer

busyout journal-printer

Use **busyout journal-printer** to put the link to the Property Management System log or wakeup log printers in a maintenance busy state. When busied out, the link is dropped and no data transfer can take place over it.

Use **busyout journal-printer** to prevent unwanted interference between different maintenance processes. Maintenance software may put a component that is part of a link in a busy state, causing link setup to fail, and resulting in attempts by the system to reestablish the link. If a maintenance test requires that the component be idle, frequent attempts at re-setup may delay the recovery of a faulty component. Busyout the link to prevent re-setup attempts.

Syntax

```
busyout journal-printer [ pms-log | wakeup-log ]
```

pms-log	Busies out the link to the Property Management System printer.
wakeup-log	Busies out the link to the Wakeup Log printer.

release journal-printer

Use **release journal-priner** to return to service a busied out link to the Property Management System (PMS) log or wakeup log printers. See Busyout and Release Commands.

Syntax

```
release journal-printer[ wakeup-log  |  pms-log ]
```

wakeup-log	The printer that handles automatic wakeup events, emergency access events and scheduled reports.
pms-log	The printer that handles housekeeping events while the PMS is down.

For general information on journal printer links, see **busyout pms-link**. For information on journal printers, see **status journal-link**.

Note:

Specific component maintenance performed on a link sometimes conflicts with link maintenance, because busied-out objects create link setup failure. Frequent link re-setup attempts may delay component recovery. For best results, busyout the link to disable attempted link re-setup.

test journal-printer

Use **test journal-printer** to perform hardware diagnostics on the link between the switch and a specified journal printer link to either the pms-log printer or the wakeup-log printer.

Syntax

```
test journal-printer pms-log | wakeup-log [ short | long ] [ repeat # | clear ] [ schedule ]
```

pms-log	Test the link to the Property Management System printer, whose maintenance name is PMS-PRNT.
wakeup-log	Test the wakeup-log printer, whose maintenance name is JNL-PRNT.
short	Execute a series of nondestructive diagnostic tests.
long	Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
repeat #	The number of times to repeat the command. The default is 1.
clear	Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.
schedule	Specify a time to run the command.

led

test led

Use **test led** to verify that a specified cabinet, port network, PNC, or switch node is recognized by the system. Also use **test led** to identify a port network, cabinet, or PNC (A or B).

When **test led** is entered, the red, green and yellow circuit pack LEDs are turned on until all administered carriers in the specified group have been lit for 2 seconds. They are turned off in the same order in which they came on. The cycle can be repeated a number of times with the **repeat** option. Once every repeat cycle is completed, every affected LED is restored to reflect its current status.

Syntax

```
test led [ all | cabinet UU | port-network PN# | switch-node SN# | media gateway # | a-pnc | b-pnc ] [ repeat # ]
```


Comments on this document? infodev@avaya.com

all	Parameter description.
cabinet *UU*	Cabinet number (1–2 digits).
port-network *PN#*	Port network number.
switch-node *SN#*	Switch node number.
media-gateway #	Gateway number.
a-pnc/b-pnc	For an unduplicated PNC, a-pnc is the only valid qualifier. Use on a system with duplicated PNC, to distinguish between the two fibers of a duplicated pair. Use b-pnc on a system with duplicated PNC, to distinguish between the two fibers of a duplicated fiber pair.
repeat #	(Optional) The number of times to repeat the command. The default is 1.

license

test license

Use **`test license`** to run a license file check on the server so you do not have to wait for the next hourly update to see if certain license errors have been cleared.

Syntax

```
test license [ long | short ]
```

long	Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
short	Execute a series of nondestructive diagnostic tests.

If the test results are:

- PASS — the system is in License-Normal mode.
- FAIL — the system is in License-Error or No-License mode, depending on the **Error** value.

link

busyout link

Use **busyout link** to put a specified packet gateway link in a maintenance busy state. For more information, see Busyout and Release Commands.

Caution:

Busyout of a link drops all calls and packet traffic dependent on that link. The application, adjunct, or switch connected to the link will be inaccessible and the link will have to be re-established later when returned to service. See status link on page 360 for more details on links.

Syntax

```
busyout link link#
```

link# A number assigned to the link on the Communication Interface Links screen.

clear link

Use **clear link** to clear the counters associated with a numbered PPP C-LAN link. The statistical counters cannot be cleared for a C-LAN's Ethernet link.

See **status link** for more details on links.

Use **clear clan-port** to clear the counters associated with a numbered PPP C-LAN link.

Syntax

```
clear link n
```

n The number of the administered link.

status link

Use **status link** to see:

- Static information about the link.
- Data extension and port used, connect speed, and protocol information.
- A counter of CHAP failures for PPP links.
- Time information for PPP and Ethernet links, including the time of the last reset.
- Type and number of active applications.

The same information that is displayed by status link can also be invoked with **status clan-port** or **netstat link** for C-LAN links.

Syntax

```
status link [link# | procr]
```

link# Number of the administered link.

procr Status of administered v4 and v6.

status link field descriptions, page 1

Field	Description
Link Number	Administered link number (assigned by **add/change data-module**)
Link Status	no, yes, unavail, connected, disconnected, enabled, out-of-service, or restarting
Link Type	The type of interface according to the physical/link protocol(s) immediately **below** the network layer in the protocol stack (Ethernet or PPP)
Link Name	Administered link name (assigned by **add/change data-module**)
Service Port Location	Administered port location (assigned by **add/change data-module**)
Service Port Data Extension	Administered extension number (assigned by **add/change data-module**)
Service State	in-service/idle, in-service/active, disconnected, out-of-service, maintenance busy, in-service, inactive, active, idle
Node Name	Administered node name for TCP/IP endpoint (assigned by **add/change data-module**)
Source IP Address	IP address administered for node name (assigned with change node-name or **add/change data-module**)
Enabled	**y/n**
Maintenance Busy	**y/n**
Active Channels	Number of active channels

status link field descriptions, page 2

Field	Description
Incoming received Unicast packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Incoming received multicast packets	The number of non-unicast (subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
Incoming dropped octets	The total number of octets received on the interface, including framing characters.

Table continues…

Field	Description
Incoming errored packets	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Incoming packets discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Outgoing Transmitted unicast packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Outgoing multicast packets	The total number of packets that higher-level protocols requested be transmitted to a non- unicast (subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
Outgoing transmitted octets	The total number of octets transmitted out of the interface, including framing characters.
Outgoing errored packets	The number of outbound packets that could not be transmitted because of errors.
Outgoing packets discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

status link field descriptions, page 3

The processor or hop channel status information can take either 1 or 2 pages on this screen, depending on the number of links being reported and their condition.

Note:

A dash (–) or a colon (:) between numbers indicates all numbers including and between the indicated numbers.

Field	Description
UP	Channels are up.
DOWN	Channels are down.
PND	Channels are in a pending state from the down to the up state (processor channels only)

status link field descriptions, page 4

The following is an example of the output of page 4 of **`status link`**. The screen displays every TCP/IP socket link that is currently up and active and that is using the Ethernet link n via the C-LAN board or the Processor Ethernet interface. Note that the service type of DOLAN reflects the total of IP endpoints and H323 signaling groups on that C-LAN.

Field	Description
Service Type	
Sessions	

test link

Use **test link** to verify that the specified link is administered and performs a series of tests on the link. See **status link** for more details on links.

Syntax

```
test link link# [ short  |  long ] [ repeat  #  |  clear ] [ schedule ]
```

link# Each link is identified by a number (1–16) assigned on the communication-interface links screen. **display communication-interface links** shows the location and identification of each link.

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

schedule Specify a time to run the command.

locations

list locations

Use **list locations** to view a list of administered locations.

Syntax

```
list locations
```

logging-levels

change logging-levels

Use **change logging-levels** to control how much information is logged for SAT activity.

Syntax

```
change logging-levels
```

change logging-levels field descriptions

Field	Description
Enable Command Logging	**y/n** Enter **y** to enable SAT activity logging. Enter **n** to disable SAT activity logging.
Log Data Values	This value applies to EVERY field on a form. • **both** — causes both the value prior to a change and the value after a change to be logged. • **new** — causes only the value following a change to be logged. The value prior to the change is not logged. • **none** — neither the value prior to the change nor the value after the change is logged. However the form access is logged.
Display Logging Levels	**y/n** Enter **y** to log these commands and transactions to the Command History log. The Command History log is stored via syslog and is available from the server web pages only.

display logging-levels

Use **display logging-levels** to see what SAT activities are being logged to the Command History log.

Syntax

```
display logging-levels
```

See **change logging-levels** for screen and field descriptions.

login-id

reset login-id

Use **reset login-id** to terminate a SAT session on a TCP/IP link, or other traditional connection. Use **status logins** to see the ID number of all active SAT sessions.

Syntax

```
reset login-id n ]
```

n The number (0–999) of the SAT session.

Example

```
reset login-id 9
```

logins

status logins

Use **status logins** to see information about all of the users that are currently using the Communication Manager SAT.

The screen does not automatically update, and is a reflection of the system at the time the request was made. Users may have logged off, or on, or the command may have finished executing while the information is being displayed. This screen shows only those users who have a SAT session active. It does not show users that may be accessing the server but have no SAT session active. This screen also displays the IPv6 addresses.

Syntax

```
status logins
```

status logins field descriptions

Field	Description
Login	Login name.
Profile	The user profile number assigned to the login.
User's Address	User’s IP address (correct regardless of whether the user is connected through a CLAN or a processor interface).

Table continues…

Field	Description
Active Command	Current or last command issued by the login. This field may not be accurate, and updates are not reflected until the next execution of status logins.
Session ID	The session number assigned by the system, in chronological order of access.

maintenance

reset maintenance

Use **reset maintenance** to reset a specified maintenance circuit pack. Specify a cabinet, 1 through 44, to reset the PN's Maintenance circuit pack in the **a** carrier of the specified cabinet, dropping any local login to that circuit pack.

Syntax

```
reset maintenance  UUC
```

UUC Cabinet number and letter designation of the carrier.

test maintenance

Use **test maintenance** to perform hardware diagnostic tests on the PN's maintenance circuit packs.

For a PN's maintenance circuit pack, the MT interface, EI link, reset, and sanity functions are tested. The long test resets the PN's maintenance circuit pack, dropping the local login via the maintenance board.

Syntax

```
test maintenance [ C ] [ short  |  long ] [ repeat #  |  clear ] [ schedule ]
```

C Cabinet number.

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

schedule Specify a time to run the command.

marked-ports

list marked-ports

Use **list marked-ports** to list every port that has been marked unusable with **mark port**.

Syntax

```
list marked-ports [ schedule ]
```

schedule Specify a time to run the command.

list marked-ports field descriptions

Field	Description
Port	The physical location (cabinet-carrier-slot-port circuit) of the marked port.
Board-Type	The type of circuit pack with the marked port.

mct-history

list mct-history

Use **list mct-history** to display the data associated with the Malicious Call Trace (MCT) feature chronologically, with the newest data displayed first.

MCT enables customers to collect information that could be used to identify a calling party whose conversation is deemed to have a malicious intent. Several scenarios are possible:

- Communication Manager software records information about the caller, including the Calling Number whenever possible for incoming trunk calls. This information can be viewed using the Malicious Call Trace History report.

- If the Communication Manager server is connected directly to a public ISDN that follows the ETSI protocol standard, Communication Manager software sends a message to the network requesting that the source of the incoming call be identified and the call be registered.
  1. If the public ISDN sends an acknowledgement, the ISDN Notification field on the MCT History report will show `acknowledged`.
  2. If the public ISDN sends a rejection (perhaps because the feature was not subscribed), the ISDN Notification field on the MCT History report will show `rejected`.
  3. If the public ISDN does not send any response, the ISDN Notification field on the MCT History report will show `no response`.
- If the Communication Manager server is **not** connected directly to a public ISDN that follows the ETSI protocol standard, the ISDN Notification field on the MCT History report will display `not sent`. Note that this includes the following two cases:
  1. If the Communication Manager server is directly connected to a public ISDN that follows the Australian ISDN protocol standard (Country Protocol 2), the public ISDN is notified when MCT is activated, but the ISDN Notification field displays `not sent`.
  2. If the Communication Manager server is **indirectly** connected via a QSIG or DCS private network to a public ISDN that follows the ETSI or Australian ISDN protocol standard, a message is sent through the private network to the gateway server. The gateway server then notifies the public ISDN that MCT has been activated, but the ISDN Notification field displays `not sent`. Note that in the QSIG case, the private-network message is proprietary, so all servers between the user activating MCT and the gateway must be Communication Manager servers.

Syntax

```
list mct-history
```

list mct-history field descriptions

Field	Description
Date	The date of the occurrence.
Time	The time of the occurrence.
Contr Ext	Controlling Extension: The extension of the user who enabled the MCT control feature. The controlling extension user then has access (via display messages) to the information regarding the malicious call.
Active Ext	The extension of the user that activated the MCT feature.
Recorder Port	The port of a voice recorder being used to record the malicious call.
Redir From	For redirected calls, the party from which the malicious call was redirected (for example, coverage, forwarding).
Actual Party	The extension of the user who received the malicious call.
Parties on Call	The extensions of other parties connected to the malicious call when the MCT feature was activated.
ISDN Notification	Whether an ISDN notification was sent to the PSTN notifying them of the call, and whether the network responded.

measurements

list measurements aca

Use **list measurements aca** to identify possible trunk malfunctions.

Syntax

```
list measurements aca
```

For more information about using ACA, refer to 'Automatic Circuit Assurance' in *Avaya Aura®Communication Manager Feature Description and Implementation (555-245-205)*.

list measurements clan ethernet

Use **list measurements clan ethernet** to see a 24-hour history of important packet-level statistics. Use the list to infer some LAN performance characteristics. For example:

- high collision counts could indicate high traffic on the LAN segment, or congestion on the bus.
- high Cyclic Redundancy Check (CRC — detects and corrects errors on every frame) errors could suggest that:
  - the LAN connection may be **noisy**
  - a wire connection is loose
  - a wire is frayed or broken

The 24-hour history gives the ability to look back at these measures if the trouble cleared.

The data is collected at 15-minute intervals over 24 hours for the CRC (Cyclic Redundancy Check) and collisions for ethernet connections. If the data cannot be retrieved for the 15-minute interval, N/A is displayed. The delta (the change from the last inquiry) and the total are provided for each error count. After the occurrence of **N/A** (not available), the delta equals the total.

The primary use of this command is to quickly and unambiguously determine whether the fault lies within the Avaya-provided equipment or with the LAN or LAN administration to which the system is connected.

Syntax

```
list measurements clan ethernet board location [ schedule ]
```

board *location*	Cabinet-carrier-slot address of the C-LAN circuit pack.
schedule	Specify a time to run the command.

list measurements clan ethernet field descriptions

Field	Description
Date	The date that the data was collected.
Time	The current 15-minute interval in which the action was performed.
CRC Check	The error count for CRC errors.
Total	The total value of the counter on the board The counter value can be up to 11 digits long because of the 32-bit counter on the board. After an N/A occurs, the delta equals the total. Busying out or releasing a board or a port, using **reset board**, and resetting the board all clear the firmware counters.
Delta	The difference between the current and the previous sample.
Collision Count	The error count for collisions on the ethernet.

list measurements clan ppp

Use **list measurements clan ppp** to list a 24-hour history of important packet-level statistics from which you can infer some LAN performance characteristics. For example:

- **Invalid frames** — the number of frames that are misaligned.
- **CHAP failures** — Challenge Handshake Authentication Protocol—the number of attempts for ppp authentication that failed.
- **High Cyclic Redundancy Check (CRC)** — detects and corrects errors on every frame; errors could suggest that the connection may be **noisy**.

The 24-hour history gives the ability to look back at these measures.

Data is retrieved at 15-minute intervals for 24 hours for CRC, Invalid Frame, and Chap Failures for PPP connections. If the data cannot be retrieved for the 15-minute interval, N/A is displayed. The delta (the change from the last inquiry) and the total are provided for each error count. After the occurrence of an **N/A**, the delta equals the total.

Syntax

```
list measurements clan ppp board location[ schedule ]
```

board *location* Cabinet-carrier-slot port address of the C-LAN circuit pack.

schedule Specify a time to run the command.

list measurements clan ppp field descriptions

Field	Description
Date	The date that the data was collected.
Time	The current 15-minute interval in which the action was performed.

Table continues…

Field	Description
CRC Check	The error count for CRC errors.
Total	Total value of the board counter. The counter value can be up to 7 digits long because the 16- bit counter on the board. After the occurrence of an “N/A” the delta equals the total. Busying out or releasing a board or a port, using **reset board**, and resetting the board all clear the firmware counters.
Delta	The difference between the current and the previous sample.
Invalid Frame	The number of invalid frames detected. Invalid frames are the frames that are misaligned.
CHAP Failures	The number of failed attempts for ppp authentication.

list measurements clan sockets

Use **list measurements clan sockets** on IP Media Processor and Medpro.

Syntax

```
list measurements clan sockets hourly location [ summary | detail ][ yesterday-peak | today-peak | last-hour ]
```

hourly *location*	Lists the measurements for the last 24 hours, from current hour backwards, for the indicated board.
summary [*yesterday-peak* | *today-peak* | *last-hour*]	Lists the measurements for the previous day’s peak, in socket usage (Erl), for the C-LAN boards administered on the IP interfaces screen. The screen output may reflect multiple C-LAN boards.
detail[*yesterday-peak* | *today-peak* | *last-hour*] *loc*	Lists the measurements for the previous day’s peak for the specified board. If the switch clock is changed, the report shows asterisks.

list measurements clan sockets field descriptions

Field	Description
Meas Hour	The hour the measurement was taken. Switches in multiple time zones are treated as in the current MMI reports. We do not assume that the customer has made any correlation between LAN regions and time zones.
Board	The cabinet, carrier, and slot for the specified board.
Region	The network region where the C-LAN for this measurement resides.
Socket Usage (Erl)	The total time, in Erlangs, that is available from sockets on this C-LAN board. Calculated by: (Total Socket Seconds of usage) / 3600.

Table continues…

Field	Description
Socket peg	Total number of times a C-LAN socket on the board was allocated to a call or link.
Socket Denial peg	Total number of times a C-LAN socket on the board was needed for a call or link, but was not available.
% Denials	(Socket Denial peg)/(Socket Denial peg + Socket peg).
% Time ASB	The percentage of time during the measured interval that every C-LAN socket on the board was unavailable for use.

list measurements ds1

Use **list measurements ds1** to list performance measurements on a DS1 link. The performance measurements of a DS1 link indicate the quality of the DS1's physical interface between the system and a far-end system.

Use **list measurements ds1-facility** to see link performance measurements on a DS1 Converter facility. The DS1 Converter complex consists of two DS1Cs connected by one to four DS1 facilities. Using this complex, you can extend the distance between two port networks up to 100 miles, thereby extending the range of the optical fiber link within limited bandwidth (96 channels). A DS1C complex can be used in a direct connectivity configuration or a Center Stage Switch configuration. The DS1 converters may be connected to an Expansion Interface (EI) or a Switch Node Interface (SNI) via a metallic connection.

Syntax

```
list measurements ds1 [ ds1-log ] location [ schedule ]
list measurements ds1-facility  location [ log | summary ][ schedule ]
```

log Detailed report generated.

summary Summary report generated.

location The physical location of a DS1 circuit pack entered as cabinet-carrier-slot, or of a DS1 converter facility where location of the circuit pack is entered and f is a letter (a-d) designating one of the four DS1 facilities.

schedule Specify a time to run the command.

Examples

```
list measurements ds1 log  2a18
list measurements ds1 summary
list measurements ds1-fac summary  2a18
```

list measurements ds1 field descriptions

Field	Description
Counted Since	The start time and date when the associated measurement counters were cleared or the DS1 circuit pack or facility was administered.
Valid 15-Minute Intervals in Last 24 Hours	The total number of 15-minute intervals int he past 24-hour period that contain valid data. (0–96)
Seconds Elapsed In Current Interval	The number of seconds from the beginning of the current 15-minute interval. (0–900)
ESF Error Events	
Test	
Pattern	
Synchronized	
Loopback/Span Test Bit-Error Count	
Test Duration	
Worst 15-Minute Interval (Date, Time, Count)	The date, end time, and error count (from 0 to 900 in increments of four) of the 15-minute interval in the previous 24-hour period that contains the maximum value for each error category.
24-Hour Count	The sum of all valid 15-minute counts for the previous 24-hour period for each error category. (0–65535)
Current Interval Count	The error count for the current (incomplete) 15-minute interval for each of the four error categories. (0–900 or N/A if data for the 15-minute interval is invalid)
Category	The categories correspond to measurement error counters: • **Errored Seconds** — the value of the errored seconds counter for the specified 15-minute interval (0 - 900 or N/A if data for the 15-minute interval is invalid). • **Bursty Errored Seconds** — the value of the bursty errored seconds counter for the specified 15-minute interval (0 - 900 or N/A if data for the 15-minute interval is invalid). • **Severely Errored Seconds** — the value of the severely errored seconds counter for the specified 15-minute interval(0 - 900 or N/A if data for the 15-minute interval is invalid). • **Unavailable/Failed Seconds** — the value of the failed seconds counter for the specified 15-minute interval (0 - 900 or N/A if data for the 15-minute interval is invalid). • **Controlled Slip Seconds** • **Loss of Frame Count**

list measurements ip codec

Use **list measurements ip codec** to see IP media processing codec resource measurements. The **list measurements ip codec** command works on IP Media Processor and Medpro.

The IP media processing codec resource measurements are listed by software. The report output may span multiple IP Media Processor or Medpro boards. A single report output combines statistics from IP Media Processor and Medpro circuit packs. Codecs are part of a common pool.

To estimate the amount of IP traffic used on IP trunks versus IP stations, compare the list measurements ip codec report with the lines of the list measurements trunk-group, list performance trunk-group, list measurements outage-trunk, and monitor traffic trunk-groups reports corresponding to IP trunk groups. It is required that the switch not have mixed IP and non-IP ports in a single trunk group.

Syntax

```
list measurements ip codec hourly-region# [ summary | detail ][ yesterday-peak | today-peak | last-hour ][ reg# ]
```

hourly-region#	Lists the measurements for the last 24 hours, from current hour backwards, for the indicated region. If the switch clock is changed, the report shows asterisks.
summary [*yesterday-peak* | *today-peak* | *last-hour*]	Lists the measurements for the previous day's peak, for every region with MEDPRO resources administered on the IP Interfaces screen. The peak hour in a given region is the hour at which [G.711 Usage (Erl) + G. 711 Usage (Erl)] is a maximum for that region. If the switch clock is changed, the report shows asterisks.
detail [*yesterday-peak* | *today-peak* | *last-hour*]	Lists the measurements for the previous day's peak for the indicated region. If the switch clock is changed, the report shows asterisks.

list measurements ip codec field descriptions

Field	Description
Meas Hour	The hour the measurement was taken. Switches in multiple time zones are treated as in the current MMI reports. We do not assume that the customer has made any correlation between LAN regions and time zones. Range: 0000–2300.
Region	The network region that the IP Media Processors and Medpros for this measurement are in.
DSP Rscs	Total IP codec resources (voice channels) in the region. (22 or 31) * # Medpro + 64 * #IP Media Processors. The 22 or 31 multiplier for Medpro depends on admin of codec preferences. For R10, a G711 call takes 1 resource, while a G723/729 call or a Fax relay call takes 2 resources.

Table continues…

Field	Description
G.711 Usage (ERL)	Usage in Erlangs of G.711 codecs during the measurement interval. Includes time that the voice channels are on a call. Usage shall be measured from the time the voice channel is allocated until it is released. Calculated by: (Total Call Seconds) / 3600 where Total Call Seconds is a sum of the following: total time (in seconds) that a G.711 resource on a Medpro is in use total time (in seconds) that a G.711 resource on an IP Media Processor is in use
G.711 In Reg Peg	Total number of times an IP media processor port in the region was allocated to a G.711 call.
G.711 Out of Reg peg	The total number of times an IP media processor port was needed in the region for a G.711 call, but was successfully allocated to a resource in another region. Out of Region does not include denials. If “Network regions are interconnected” is n, Out of Region is always 0.
G.723/9 Usage (ERL)	Usage in Erlangs of G.723 or G.729 codecs during the measurement interval. Includes time that the voice channels are on a call. Usage shall be measured from the time the voice channel is allocated until it is released. Calculated by: (Total Call Seconds) / 3600 where Total Call Seconds is a sum of the following: total time (in seconds) that a G.723 or G.729 resource on a Medpro is in use twice the total time (in seconds) that a G.723 or G.729 resource on an IP Media Processor is in use
G.723/9 In Reg peg	Total number of times an IP media processor port in the region was allocated to a G.723 or G.729 call.
G.723/9 Out of Reg peg	The total number of times an IP media processor port was needed in the region for a G.723 or G.729 call, but was successfully allocated to a resource in another region. Out of Region does not include denials. If Network regions are interconnected is **n**, Out of Region is always **0**.

list measurements ip dsp-resource

Use **`list measurements ip dsp-resource`** on IP Media Processor and Medpro to see the following:

- IP media processing DSP resource measurements
- G.711 equivalent peak usage at the network region level

The **`list measurements ip dsp-resource`** measurements are displayed by software. The report output may span multiple IP Media Processor or Medpro boards. A single report output combines statistics from both IP Media Processor and Medpro boards. Codecs are part of a common pool.

Syntax

```
list measurements ip dsp-resource hourly [summary|detail][yesterday-peak|today-peak|last-hour][reg#][pn summary][gn summary]
```

hourly	Lists the measurements for the last 24 hours, from current hour backwards, for the indicated region. If the switch clock is changed, the report shows stars.
summary [*yesterday-peak* | *today-peak* |*last-hour*]	Lists the measurements for the previous day's peak DSP Usage (Erl) for every regions with MEDPRO resources administered on the ip-interfaces screen. The peak hour in a given region is the hour at which DSP Usage (Erl) is a maximum for that region. If the switch clock is changed, the report shows stars. If you are running 3FQ08 CM software or later, the list measurements ip dsp-resource summary report shows G.711 equivalent peak usage at the network region level. It shows the peak hour of DSP resource activity per network region.
detail *reg#* [*yesterday-peak* | *today-peak* |*last-hour*]	Lists the measurements for the previous day's peak for the indicated region. If the switch clock is changed, the report shows stars.
pn sumamry	Lists the cumulative/total line of output that shows the hour with the greatest dsp usage for all of the fiber-connected port networks based on the highest Erlang usage.
gn sumamry	Lists the gateway summary report that shows the peak hour DSP usage for a specific H.248 branch gateway.

Description

Insert a description of the command, including what it does and when to use it.

list measurements ip dsp-resource hourly report field descriptions

Field	Range	Description
Net Reg	1–2000 or 1–250 depending on server configuration	The network region represents the network region of the IP media processors being measured. The region number is assigned on the ip-interface screen during switch administration.
Meas Hour	0000–2300	Hour for which data is collected.
G711 Equivalent DSP Rsrc Capcty	0–99999 *	DSP resource capacity indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given network region. The asterisk (*) indicates that the media processor capacity changed during the measurement hour.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the

Table continues…

Field	Range	Description
		measurement hour. The “spike” traffic pattern helps to determine when resources should be added.
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on).
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour.
Endpoint In Reg Pegs	0–65535	The total number of times an IP media processor port in the region was allocated to a call/request within that same network region during the measurement hour. Endpoint calculations also include IP/SIP trunks and IGCs.
Endpoint Out Reg Pegs	0–65535	The total number of times an endpoint request for an IP media processor port from a specific network region was allocated to a media processor in a different region. This might occur when there are no available resources in the requested network region, a call has been re-directed to another port network. If the Region fields on the Inter Network Region Connection Management screen are blank, then this measurement will always be 0.
Endpoint Denied Pegs	0–65535	The total number of times an IP media processor port was requested for a call, but was denied because there were no media processing resources available in the system. **Note:** Calls that were re-directed are not counted as denied calls Denied peg counts are against the network region or the IP endpoint that is requesting the resource. Denied peg counts for IGCs are against the network region of the cabinet that is requesting the resource.

list measurements ip dsp-resource summary report field descriptions

Field	Range	Description
Net Reg	1–2000 or 1–250 depending on server configuration	The network region represents the network region of the IP media processors being measured. The region number is assigned on the ip-interface screen during switch administration.
Peak Hour	0000–2300	The measurement hour with the highest Erlang usage for a specific network region.
G711 Equivalent DSP Rsrc Capcty	0–99999 *	DSP resource capacity indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given network region. The asterisk (*) indicates that the media processor capacity changed during the measurement hour.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the measurement hour. The “spike” traffic pattern helps to determine when resources should be added.
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on).
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour.
Endpoint In Reg Pegs	0–65535	The total number of times an IP media processor port in the region was allocated to a call/request within that same network region during the measurement hour. Endpoint calculations also include IP/SIP trunks and IGCs.
Endpoint Out Reg Pegs	0–65535	The total number of times an endpoint request for an IP media processor port from a specific network region was allocated to a media processor in a different region. This might occur when there are no available resources in the requested network region, a call has been re-directed to another port network.

Table continues…

Field	Range	Description
		If the Region fields on the Inter Network Region Connection Management screen are blank, then this measurement will always be 0.
Endpoint Denied Pegs	0–65535	The total number of times an IP media processor port is requested for a call, but was denied because there were no media processing resources available in the system. **Note:** Calls that were re-directed are not counted as denied calls Denied peg counts are against the network region or the IP endpoint that is requesting the resource. Denied peg counts for IGCs are against the network region of the cabinet that is requesting the resource.
% Denied	0–99	Percentage Denied: The percent of pegs which were denied during the measurement period. **Note:** It is possible to have denied calls even though Peak DSP usage has not been exceeded. For example, Peak DSP is 479 out of 480. The next call that comes in could be denied because it needs two DSP resources and only one is available (for example, if the call used a G.729 codec).
% Out of Srv	0–99	Percentage Out of Service: The percent of total resource time that ports were out of service during the measurement period. This percent includes ports that were manually busied out or maintenance busy during the measured interval.

list measurements ip dsp-resource pn summary report field descriptions

Field	Range	Description
PN#- Type	1–64 F(iber) or I (P)	Indicates the port network of the media processor being measured. A port network number followed by **F** (for example, 1–F) indicates that this is a fiber-connected PN. Similarly, a port network number followed by **I** (for example 4–I) indicates that this is a IP-connected PN. Up to five rows of data is shown for each PN, based on the five lowest network region numbers administered. **C** — Cumulative total of all fiber connected PNs (that is, CCS).

Table continues…

Field	Range	Description
Net Reg	All 1–250 or 1–2000 = future develmt	Shows data for a given PN across all network regions in that PN (note that typically media processors in a port network are administered for a single network region. However, that is not always the case). The network region column represents the network region of the IP media processors being measured; not the network region of the cabinets. The region number is assigned on the ip-interfaces screen during switch administration.
Peak Hour	0000–2300	The measurement hour with the highest Erlang usage for the specific port network/network region combination.
G711 Equivalent DSP Rsrc Capcty	0–99999	G.711 Equivalent Digital Signaling Processor Resource Capacity. Indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given port network. The asterisk (*) in this column indicates that media processor capacity changed during the measurement hour. Totals are shown for all fiber- and IP-connected PNs in cases where a port network has multiple media processors across different network regions.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the measurement hour for that port network. This is helpful to customer with **spike** traffic patterns to determine when resources should be added.
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	G.711 Equivalent DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on).
G711 Equivalent DSP IGC Usage	0–999.9 Erlangs	Total usage of a port-network or gateway for its involvement in Inter-PN or Inter-GW connections. Channel usage may be from IP endpoints or an IGC.
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour.

Table continues…

Field	Range	Description
IGC Pegs	0–65535	Inter-Gateway Connection Pegs. The number of times media processor resources were allocated in a port network to connect two endpoints via an IGC (this is a subset of total DSP pegs).
PN Denied Pegs	0–65535	The total number of times an IP media processor port is needed in the port network for a call, but was denied because there were no media processing resources available in that port network.
% Den	0–99 (pegs)	Percentage Denied: The percent of pegs which were denied during the measurement period.
% Out of Srv	0–99	Percentage Out of Service: The percent of total resource time that ports were out of service during the measurement period. This percent includes ports that were manually busied out or maintenance busy during the measured interval.

list measurements ip dsp-resource hourly pn summary report field descriptions

Field	Range	Description
PN#- Type	1–64 F(iber) or I (P)	Indicates the port network of the media processor being measured. A port network number followed by **F** (for example, 1–F) indicates that this is a fiber-connected PN. Similarly, a port network number followed by **I** (for example 4–I) indicates that this is a IP-connected PN. Up to five rows of data is shown for each PN, based on the five lowest network region numbers administered. **C** — Cumulative total of all fiber connected PNs (that is, CCS).
Meas Hour	0000–2300	The hour for which data is collected for the port network.
G711 Equivalent DSP Rsrc Capcty	0–99999	G.711 Equivalent Digital Signaling Processor Resource Capacity. Indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given port network. The asterisk (*) in this column indicates that media processor capacity changed during the measurement hour. Totals are shown for all fiber- and IP-connected PNs in cases where a port network has multiple media processors across different network regions.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the

Table continues…

Field	Range	Description
		measurement hour for that port network. This is helpful to customer with **spike** traffic patterns to determine when resources should be added.
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	G.711 Equivalent DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on).
IGC Usage	0–999.9 Erlangs	Total usage of a port-network or gateway for its involvement in Inter-PN or Inter-GW connections. Channel usage may be from IP endpoints or an IGC.
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour.
IGC Pegs	0–65535	Inter-Gateway Connection Pegs. The number of times media processor resources were allocated in a port network to connect two endpoints via an IGC (this is a subset of total DSP pegs).
PN Denied Pegs	0–65535	The total number of times an IP media processor port is needed in the port network for a call, but was denied because there were no media processing resources available in that port network.
% Den	0–99 (pegs)	Percentage Denied: The percent of pegs which were denied during the measurement period.
% Out of Srv	0–99	Percentage Out of Service: The percent of total resource time that ports were out of service during the measurement period. This percent includes ports that were manually busied out or maintenance busy during the measured interval.

list measurements ip dsp-resource gw summary report field descriptions

Field	Range	Description
GW Num	G001–G250	Indicates the number of the administered H.248 branch gateway for which DSP resource usage is being reported for the given measurement hour.
GW Type	g700 g350	Indicates the H.248 branch gateway type containing the DSP resource being used.

Table continues…

Field	Range	Description
	g250 g430 g450 ig550 trm480	
Peak Hour	0000–2300	The measurement hour with the highest Erlang usage for the specific gateway.
Net Reg	1–2000 or 1–250 depending on server configuration	The network region represents the network region of the IP media processors being measured. The region number is assigned on the ip-interface screen during switch administration.
G711 Equivalent DSP Rsrc Capcty	0–99999	G.711 Equivalent Digital Signaling Processor Resource Capacity. Indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given port network. The asterisk (*) in this column indicates that media processor capacity changed during the measurement hour. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the measurement hour for that port network. This is helpful to customer with **spike** traffic patterns to determine when resources should be added. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	G.711 Equivalent DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on). Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.

Table continues…

Field	Range	Description
IGC Usage	0–999.9 Erlangs	Total usage of a port-network or gateway for its involvement in Inter-PN or Inter-GW connections. Channel usage may be from IP endpoints or an IGC. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
IGC Pegs	0–65535	Inter-Gateway Connection Pegs. The number of times media processor resources were allocated in a port network to connect two endpoints via an IGC (this is a subset of total DSP pegs). Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
GW Denied Pegs	0–65535	The total number of times an IP media processor port is needed in the gateway for a call, but was denied because there were no media processing resources available in that gateway. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
% Den	0–99 (pegs)	Percentage Denied: The percent of pegs which were denied during the measurement period. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
% Out of Srv	0–99	Percentage Out of Service: The percent of total resource time that ports were out of service during the measurement period. This percent includes ports that were manually busied out or maintenance busy during the measured interval. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.

list measurements ip dsp-resource hourly gw summary report field descriptions

Field	Range	Description
GW Num	G001–G250	Indicates the number of the administered H.248 branch gateway for which DSP resource usage is being reported for the given measurement hour.
GW Type	g700 g350 g250 g430 g450 ig550 trm480	Indicates the H.248 branch gateway type containing the DSP resource being used.
Meas Hour	0000–2300	The measurement hour with the highest Erlang usage for the specific gateway.
Net Reg	1–2000 or 1–250 depending on server configuration	The network region represents the network region of the IP media processors being measured. The region number is assigned on the ip-interface screen during switch administration.
G711 Equivalent DSP Rsrc Capcty	0–99999	G.711 Equivalent Digital Signaling Processor Resource Capacity. Indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given port network. The asterisk (*) in this column indicates that media processor capacity changed during the measurement hour. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the measurement hour for that port network. This is helpful to customer with **spike** traffic patterns to determine when resources should be added. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	G.711 Equivalent DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the

Table continues…

Field	Range	Description
		media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on). Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
IGC Usage	0–999.9 Erlangs	Total usage of a port-network or gateway for its involvement in Inter-PN or Inter-GW connections. Channel usage may be from IP endpoints or an IGC. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
IGC Pegs	0–65535	Inter-Gateway Connection Pegs. The number of times media processor resources were allocated in a port network to connect two endpoints via an IGC (this is a subset of total DSP pegs). Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
GW Denied Pegs	0–65535	The total number of times an IP media processor port is needed in the gateway for a call, but was denied because there were no media processing resources available in that gateway. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
% Den	0–99 (pegs)	Percentage Denied: The percent of pegs which were denied during the measurement period. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
% Out of Srv	0–99	Percentage Out of Service: The percent of total resource time that ports were out of service during the measurement period. This percent includes

Table continues…

Field	Range	Description
		ports that were manually busied out or maintenance busy during the measured interval. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.

list measurements ip signaling-groups

Use **list measurements ip signaling-groups** to see the 10 worst signaling groups for each hour of today, starting with the most recent whole hour. The forms for the today and yesterday qualifiers are 24 pages, one for each hour. The groups for each hour will be rank-ordered from worst to least worst based on the Hour Average Latency.

Syntax

```
list measurements ip signaling-groups [ current-hour | last-hour | today yesterday ]
```

current-hour Shows the 10 worst signaling groups for the current hour.

last hour Shows the 10 worst signaling groups for the last full hour.

today yesterday Shows the 10 worst signaling groups for each hour of today, starting with the most recent whole hour, or yesterday.

list measurements ip signaling-groups field descriptions

Field	Description
Sig Grp No	The group number, rank ordered.
Region	The network region of the group.
Hour Average Latency (ms)	The average latency for the whole hour.
Hour Packets Sent	The number of packets sent during the whole hour.
Hour Packets Lost (%)	The percent lost packets for the whole hour (if 100% the corresponding latency is shown as ****).
Hour/Worst Interval	The hour and worst 3 minute interval within the hour. (The interval is identified by the last minute of the interval.)
Interval Average Latency (ms)	The average latency for the interval.
Interval Packets Sent	The number of packets sent during the interval.
Interval Packets Lost (%)	The percent lost packets during the interval (if 100% the corresponding latency is shown as ****).

list measurements ip voice-stats

Use **list measurements ip voice-stats** to see the Voice/Network Statistics reports that record the voice statistics for the TN media processor boards.

Syntax

```
list measurements ip voice-stats [ hourly | summary ][ jitter | rtdelay | pktloss | data ]
[ network-region  # | processor  location ][ last-hour | today | yesterday ]
```

hourly jitter network-region# **hourly rtdelay network-region#** **hourly pktloss network-region#** **hourly data network-region#**	Assesses the following at the network region per hour during a call: • jitter • round trip delay • packet loss • data calls which exceeded a threshold event
hourly jitter processor *location* **hourly rtdelay processor *location*** **hourly pktloss processor *location*** **hourly data processor *location***	Assesses the following at the media processor per hour during a call: • jitter • round trip delay • packet loss • data calls which exceeded a threshold event
summary jitter [*last-hour* | *today* | *yesterday*] **summary rtdelay [*last-hour* | *today* | *yesterday*]** **summary pktloss [*last-hour* | *today* | *yesterday*]** **summary data [*last-hour* | *today* | *yesterday*]**	Summarizes the following for a given media processor board (for up to 24 hours) in the network region for the corresponding peak hour: • five worst jitter calls • five worst round trip delay calls • five worst packet loss calls • five worst data calls

Description

Insert a description of the command, including what it does and when to use it.

list measurements ip voice-stats hourly jitter at the network region field descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.
Date	Time and date that data is requested
Meas Hour	The hour (military time) in which data was collected.

Table continues…

Field	Description
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Calling Number	The number of the endpoint initiating the call (near end).
Called# / FE Addr	The number of the endpoint that received the call (far end), followed by the associated far-end IP address.
Codec	The codec used for the call.
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Time of Call	A time stamp when threshold was first exceeded for the associated call, shown in MMSS (minutes seconds)
Jitter Buffer Size (ms)	The size of the jitter buffer used for the call, measured in milliseconds.
Jitter Buffer Orn	The number of jitter buffer overruns occurred for the call. Overruns occur when many packets arrive into the jitter buffer very quickly, causing the jitter buffer to fill up. When this happens, the jitter buffer is unable to handle additional traffic/packets. If the number of overruns exceeds 99, the value in this field is **99+**.
Jitter Buffer Urn	The number of jitter buffer underruns occurred for the call. When the arrival time of packets goes beyond the size of the jitter butter, a jitter buffer underrun occurs. This results in silence until there are additional packets in the jitter buffer to process. If the number of underruns exceeds 99, the value in this field is **99+**.
Avg Jitter (ms)	The average amount of jitter recorded for the call over a 10-second reporting interval, measured in milliseconds.
Peak Jitter (ms)	The peak amount of jitter recorded for the call, measured in milliseconds.

list measurements ip voice-stats hourly rtdelay at the network region field descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.
Date	Time and date that data is requested
Src Reg	The network region associated with the media processor for which data is being recorded.
Meas Hour	The hour (military time) in which data was collected.
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Calling Number/ Called# / FE Addr	The number of the endpoint initiating the call (near end). The number of the endpoint that received the call (far end), followed by the associated far-end IP address.

Table continues…

Field	Description
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Dst Reg	The network region where the destination media processor is located.
Codec	The codec used for the call.
Avg RT Delay (ms)	The average round trip delay recorded for the call.
Peak RT Delay (ms)	The peak round trip delay recorded for the call.
Time of Call	A time stamp when threshold was first exceeded for the associated call, shown in MMSS (minutes seconds)
Data Call	Indicates whether the call is a data call.
Encryp	Indicates whether media encryption was used for the call.
EC	Indicates whether the echo cancellation is on/off for the call.

list measurements ip voice-stats hourly pktloss at the network region field descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.
Date	Time and date that data is requested
Meas Hour	The hour (military time) in which data was collected.
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Calling Number/ Called# / FE Addr	The number of the endpoint initiating the call (near end). The number of the endpoint that received the call (far end), followed by the associated far-end IP address.
Codec	The codec used for the call.
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Dst Reg	The network region where the destination media processor is located.
Time of Call	A time stamp when threshold was first exceeded for the associated call, shown in MMSS (minutes seconds)
UDP Port	The UDP port used by the media processor for the call.
Total #Lost Pkts	The total number of packets lost for this call.
Pkt Loss (%)	The peak packet loss for the call. The packet loss percentage is calculated at 10-second intervals.
Sil Sup	Indicates whether the silence suppression was used for the call.

list measurements ip voice-stats hourly data at the network region field descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.

Table continues…

Field	Description
Date	Time and date that data is requested
Meas Hour	The hour (military time) in which data was collected.
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Calling Number/ Called# / FE Addr	The number of the endpoint initiating the call (near end). The number of the endpoint that received the call (far end), followed by the associated far-end IP address.
Codec	The codec used for the call.
Data Type	Indicates the type of data call. Valid options include: • ttyrel (TTY Relay) • mod-pt (Modem pass-through) • fax-pt (FAX pass-through) • tty-pt (TTY pass-through) • t38fax (T.38 FAX) • faxrel (FAX relay) • modrel (Modem relay)
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Pkt Loss (%)	The packet Loss for the call. The packet loss percentage is calculated at 10-second intervals.
Peak Jit (ms)	The peak amount of jitter recorded for the call.
Peak Dly (ms)	The peak round trip delay recorded for the call, measured in milliseconds.
EC	Indicates whether the echo cancellation was turned on or off for the call.

list measurements ip voice-stats hourly jitter for media processor field descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.
Date	Time and date that data is requested
Net Reg	The network region associated with the media processor for which data is being recorded.
Meas Hour	The hour (military time) in which data was collected.
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Calling Number	The number of the endpoint initiating the call (near end).

Table continues…

Field	Description
Called# / FE Addr	The number of the endpoint that received the call (far end), followed by the associated far-end IP address.
Codec	The codec used for the call.
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Time of Call	A time stamp when threshold was first exceeded for the associated call, shown in MMSS (minutes seconds)
Jitter Buffer Size (ms)	The size of the jitter buffer used for the call, measured in milliseconds.
Jitter Buffer Orn	The number of jitter buffer overruns occurred for the call. Overruns occur when many packets arrive into the jitter buffer very quickly, causing the jitter buffer to fill up. When this happens, the jitter buffer is unable to handle additional traffic/packets. If the number of overruns exceeds 99, the value in this field is **99+**.
Jitter Buffer Urn	The number of jitter buffer underruns occurred for the call. When the arrival time of packets goes beyond the size of the jitter butter, a jitter buffer underrun occurs. This results in silence until there are additional packets in the jitter buffer to process. If the number of underruns exceeds 99, the value in this field is **99+**.
Avg Jitter (ms)	The average amount of jitter recorded for the call over a 10-second reporting interval, measured in milliseconds.
Peak Jitter (ms)	The peak amount of jitter recorded for the call, measured in milliseconds.

list measurements ip voice-stats hourly rtdelay for media processorfield descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.
Date	Time and date that data is requested
Net Reg	The network region associated with the media processor for which data is being recorded.
Meas Hour	The hour (military time) in which data was collected.
Calling Number/ Called# / FE Addr	The number of the endpoint initiating the call (near end). The number of the endpoint that received the call (far end), followed by the associated far-end IP address.
Codec	The codec used for the call.
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Dst Reg	The network region where the destination media processor is located.
Avg RT Delay (ms)	The average round trip delay recorded for the call.
Peak RT Delay (ms)	The peak round trip delay recorded for the call.

Table continues…

Field	Description
Time of Call	A time stamp when threshold was first exceeded for the associated call, shown in MMSS (minutes seconds)
Data Call	Indicates whether the call is a data call.
Encryp	Indicates whether media encryption was used for the call.
EC	Indicates whether the echo cancellation is on/off for the call.

list measurements ip voice-stats hourly pktloss for media processor field descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.
Date	Time and date that data is requested
Src Reg	The network region associated with the media processor for which data is being recorded.
Meas Hour	The hour (military time) in which data was collected.
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Calling Number/ Called# / FE Addr	The number of the endpoint initiating the call (near end). The number of the endpoint that received the call (far end), followed by the associated far-end IP address.
Codec	The codec used for the call.
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Dst Reg	The network region where the destination media processor is located.
Time of Call	A time stamp when threshold was first exceeded for the associated call, shown in MMSS (minutes seconds)
UDP Port	The UDP port used by the media processor for the call.
Total #Lost Pkts	The total number of packets lost for this call.
Pkt Loss (%)	The peak packet loss for the call. The packet loss percentage is calculated at 10-second intervals.
Sil Sup	Indicates whether the silence suppression was used for the call.

list measurements ip voice-stats hourly data for media processor field descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.
Date	Time and date that data is requested
Src Reg	The network region associated with the media processor for which data is being recorded.
Meas Hour	The hour (military time) in which data was collected.

Table continues…

Field	Description
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Calling Number/ Called# / FE Addr	The number of the endpoint initiating the call (near end). The number of the endpoint that received the call (far end), followed by the associated far-end IP address.
Codec	The codec used for the call.
Data Type	Indicates the type of data call. Valid options include: • ttyrel (TTY Relay) • mod-pt (Modem pass-through) • fax-pt (FAX pass-through) • tty-pt (TTY pass-through) • t38fax (T.38 FAX) • faxrel (FAX relay) • modrel (Modem relay)
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Pkt Loss (%)	The packet Loss for the call. The packet loss percentage is calculated at 10-second intervals.
Peak Jit (ms)	The peak amount of jitter recorded for the call.
Peak Dly (ms)	The peak round trip delay recorded for the call, measured in milliseconds.
EC	Indicates whether the echo cancellation was turned on or off for the call.

list measurements ip voice-stats summary jitter today field descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.
Date	Time and date that data is requested
Src Reg	The network region associated with the media processor for which data is being recorded.
Meas Hour	The hour (military time) in which data was collected.
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Calling Number/ Called# / FE Addr	The number of the endpoint initiating the call (near end). The number of the endpoint that received the call (far end), followed by the associated far-end IP address.
Codec	The codec used for the call.

Table continues…

Field	Description
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Dst Reg	The network region where the destination media processor is located.
Time of Call	A time stamp when threshold was first exceeded for the associated call, shown in MMSS (minutes seconds)
Jitter Buffer Size (ms)	The size of the jitter buffer used for the call, measured in milliseconds.
Jitter Buffer Orn	The number of jitter buffer overruns occurred for the call. Overruns occur when many packets arrive into the jitter buffer very quickly, causing the jitter buffer to fill up. When this happens, the jitter buffer is unable to handle additional traffic/packets. If the number of overruns exceeds 99, the value in this field is **99+**.
Jitter Buffer Urn	The number of jitter buffer underruns occurred for the call. When the arrival time of packets goes beyond the size of the jitter butter, a jitter buffer underrun occurs. This results in silence until there are additional packets in the jitter buffer to process. If the number of underruns exceeds 99, the value in this field is **99+**.
Avg Jitter (ms)	The average amount of jitter recorded for the call over a 10-second reporting interval, measured in milliseconds.
Peak Jitter (ms)	The peak amount of jitter recorded for the call, measured in milliseconds.

list measurements ip voice-stats summary rtdelay today field descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.
Date	Time and date that data is requested
Src Reg	The network region associated with the media processor for which data is being recorded.
Meas Hour	The hour (military time) in which data was collected.
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Calling Number	The number of the endpoint initiating the call (near end).
Called# / FE Addr	The number of the endpoint that received the call (far end), followed by the associated far-end IP address.
Codec	The codec used for the call.
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Dst Reg	The network region where the destination media processor is located.
Avg RT Delay (ms)	The average round trip delay recorded for the call.
Peak RT Delay (ms)	The peak round trip delay recorded for the call.

Table continues…

Field	Description
Time of Call	A time stamp when threshold was first exceeded for the associated call, shown in MMSS (minutes seconds)
Data Call	Indicates whether the call is a data call.
Encryp	Indicates whether media encryption was used for the call.
EC	Indicates whether the echo cancellation is on/off for the call.

list measurements ip voice-stats summary pktloss today field descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.
Date	Time and date that data is requested
Src Reg	The network region associated with the media processor for which data is being recorded.
Meas Hour	The hour (military time) in which data was collected.
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Calling Number/ Called# / FE Addr	The number of the endpoint initiating the call (near end). The number of the endpoint that received the call (far end), followed by the associated far-end IP address.
Codec	The codec used for the call.
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Dst Reg	The network region where the destination media processor is located.
Time of Call	A time stamp when threshold was first exceeded for the associated call, shown in MMSS (minutes seconds)
UDP Port	The UDP port used by the media processor for the call.
Total #Lost Pkts	The total number of packets lost for this call.
Pkt Loss (%)	The peak packet loss for the call. The packet loss percentage is calculated at 10-second intervals.
Sil Sup	Indicates whether the silence suppression was used for the call.

list measurements ip voice-stats summary data today field descriptions

Field	Description
Switch Name	The name of system from which data is being collected/reported.
Date	Time and date that data is requested
Src Reg	The network region associated with the media processor for which data is being captured.
Meas Hour	The hour (military time) in which data was collected.
Calling Number/	The number of the endpoint initiating the call (near end).

Table continues…

Field	Description
Called# / FE Addr	The number of the endpoint that received the call (far end), followed by the associated far-end IP address.
Dst Reg	The network region where the destination media processor is located.
Codec	The codec used for the call.
Data Type	Indicates the type of data call. Valid options include: • ttyrel (TTY Relay) • mod-pt (Modem pass-through) • fax-pt (FAX pass-through) • tty-pt (TTY pass-through) • t38fax (T.38 FAX) • faxrel (FAX relay) • modrel (Modem relay)
Pkt Size (ms)	The packet size for each steam of data for the associated call, measured in milliseconds.
Pkt Loss (%)	The packet Loss for the call. The packet loss percentage is calculated at 10-second intervals.
Peak Jit (ms)	The peak amount of jitter recorded for the call.
Peak Dly (ms)	The peak round trip delay recorded for the call, measured in milliseconds.
EC	Indicates whether the echo cancellation was turned on or off for the call.

list measurements tone-receiver

Use **`list measurements tone-receiver`** to see how many tone receiver ports the server is using and has available.

Syntax

```
list measurements tone-receiver [ detail | summary ][ yesterday-peak | today-peak | last-hour ][ schedule ]
```

detail [*yesterday-peak* | *today-peak* | *last-hour*]	Lists a detail of the number of tone receiver ports the server used and had available for the previous day's peak, today's peak, or the last-hour.
summary [*yesterday-peak* | *today-peak* | *last-hour*]	Lists a summary of the number of tone receiver ports the server used and had available for the previous day's peak, today's peak, or the last-hour.
schedule	Specify a time to run the command.

list measurements tone-receiver detail yesterday-peak field descriptions

Field	Description
Switch Name	Name of switch
Date	Time and date of report
Hour	The hour of peak tone-receiver usage per port for the time period specified (in this case, yesterday's peak)
PN	Port Network
Type	Type of tone-receiver being measured
PN Req	Port Network Requests. The number of requests for DTMF, GPTD, CC-TTR, CC-CPTR, or MFCR receivers within the port network during the listed hour.
PN Alloc	Port Network Total Allocation. The total number of DTMF, GPTD, CC-TTR, CC-CPTR, or MFCR receivers located in the listed port network allocated for use during the listed hour.
Peak Alloc	Peak Allocation. The peak number of DTMF, GPTD, CC-TTR, CC-CPTR, or MFCR receivers located in the listed port network in use simultaneously during the listed hour.
Total Off-PN	Total Off-Port Network. For the identified hour and port network, this is the total number of DTMF, GPTD, CC-TTR, CC-CPTR, or MFCR receivers allocated on a different port network for requests originated on this port network. With ideal conditions, this field shows 0. With more practical conditions, the field displays a larger number. **Suggested actions:** Locate communities of interest within the same port network. Provide sufficient tone receivers for each port network.
Peak Off-PN	Peak Off-Port Network. For the identified hour and port network, this is the peak number of DTMF, GPTD, CC-TTR, CC-CPTR, or MFCR receivers simultaneously allocated on a different port network for requests originated on this port network. A desirable goal is to minimize (within reason) the number displayed with this field. **Suggested actions:** Locate communities of interest within the same port network. Provide sufficient tone receivers for each port network. Perhaps you should move one TN748 and TN420 circuit pack (or, if you are working with a CC-TTR, CC-CPTR, and MFCR, move a TN744 circuit pack) to the PN with the Off-PN counts to minimize Off-PN allocations.

list measurements tone-receiver summary last-hour field descriptions

Field	Description
Switch Name	Name of switch
Date	Time and date of report
Hour	The hour the measurement was taken
Meas Type	Type of tone-receiver being measured
Total Req	Total Requests. The system-wide total number of requests, by call processing, for DTMF, GPTD, CC-TTR, CC-CPTR, or MFCR receivers during the listed hour. The total number of requests is calculated by incrementing a counter for each request.
Peak Req	Peak Requests. The system-wide peak number of simultaneous requests for DTMF, GPTD, CC-TTR, CC-CPTR, or MFCR receivers that occurred at any one time for the listed hour. The peak (or maximum) number is calculated by incrementing a counter for each request and decreasing the counter when the request fails or a tone receiver is released. If the Peak Req field indicates a number higher than listed in the Avail field, certain requests were either queued or denied during the peak time interval. Denied requests fail and are given the reorder tone.
Total Queued	The system-wide total number of requests queued during the listed hour. A request is queued when there are no receivers immediately available. Only DTMF and CC-TTR requests are queued. If a request for a receiver is made in one port network, and no receivers are available, then the request is offered to the next port network. If no receivers are available on any port network, then the request is queued. Queued call requests do not receive dial tone until a tone receiver becomes available.
Peak Queued	The system-wide maximum number of call requests queued at any one time during the listed hour. Maximum queue size: • TMF requests = 4 • CC-TTR call vectoring requests = 80
Total Denied	The system-wide total number of requests denied because no receivers were available during the listed hour. For DTMF-receiver or CCTR requests, this happens only after the queue is full. Those requests denied are given reorder tone.
Peak Denied	The system-wide peak number of requests denied because no receivers were available during the listed hour. Suggested action: • Increase the number of tone receivers by the number displayed in the Peak Denied field.

Table continues…

Field	Description
	• Administer the system as **non-blocking** for tone receivers: increase the number of tone receivers (the Avail field) so all requests receive service immediately and no requests are queued. For example, keep the value displayed in the Avail field greater than that displayed in the Peak Req field.
TR Type	Type of tone-receiver
Total Avail	Number of tone-receivers of each type available for use
Capabilities	Tone capabilities of each tone-receiver

media-gateway

add media-gateway

Use **add media-gateway** on the primary server to add a gateway to the system.

Syntax

```
add media-gateway [ x | next ]
```

x Number of the assigned gateway.

next Next available number.

add media-gateway field descriptions

Field	Description
Controller IPv4 Address / Controller IPv6 Address	(Display only) Blank until the gateway registers for the first time. The Controller IP Address field supports the IPv6 addresses. This is the IP address the that the gateway is registered to on the server. • For Duplex servers and other External Call Controllers (ECC), this is a CLAN address. • For Simplex servers, Survivable Remote Server and other servers providing Processor Ethernet (PE), this is the native NIC address.
Enable CF?	Appears only for G450 and G430 gateways and only when the announcement module is administered in the V9 slot. The Enable CF? field indicates if you have enabled a compact flash to backup or restore the announcement files. The valid responses are **y**

Table continues…

Field	Description
	and **n**, where **n** is the default response. Enter **y** to enable a Compact Flash. If you are using a G450 Release 1.*x*, where the compact flash is not a valid option, the Enable CF? field is display-only and the value is set to **n**.
Encrypt Link	The valid values are **y** and **n**. Enter **y** to encrypt the H.248 link on the gateway. **y** is the default value when the gateway is added.
FW Version / HW Vintage	(Display only) Current firmware and hardware versions on the gateway.
IP Address	(Display only) The IP address of the gateway. Blank until the gateway registers for the first time. Once the gateway has registered, that IP address always appears, even if the gateway becomes unregistered, until a gateway with a different IP address is validly registered with the same administered identifier. The populated IP address is persistent over reboots.
Link encryption type	**Note:** This field complies with the Unified Capabilities Requirements (UCR) 2008 Change 3 requirements and is approved by Joint Interoperability Test Command (JITC). This field is available only for the USA Department of Defense (DoD) and approved Federal government customers. The following are the valid entries for this field: • none: No encryption • any-ptls/tls: any-ptls/tls is the default value when Communication Manager is in the non-FIPS mode. • ptls-only: ptls is Avaya Proprietary Encryption Algorithm. • tls-only: tls-only is the default value when Communication Manager is in the FIPS mode.
Location	1 through 250 — (Depending on your server configuration, see *Avaya Aura®Communication Manager System Capacities Table (03-300511)*.) Refers to a time-zone offset, day-light savings rule, and number plan area code. See the Location sections in *Avaya Aura®Communication ManagerFeature Description (555-245-205)*, for the other ways, and for a list of features that use location. **Warning:** If you change the Location field while the gateway is registered, you must reboot the gateway to ensure optimal audio quality.

Table continues…

Field	Description
	Blank — The location is obtained from the cabinet containing the CLAN or the gateway that the endpoint registered with. By default, the value is blank.
MAC Address	(Display only) MAC address of the gateway. Blank until the gateway registers for the first time. Once the gateway has registered, that MAC Address appears, even if the gateway becomes unregistered, until a gateway with a different MAC Address is validly registered with the same administered identifier.
Max Survivable IP Ext.	Appears when Type is **G250**, **G350**, **G450**, **J2320**, and so on. Limits the number of simultaneous endpoint registrations for the gateway in SLS mode. VoIP resources in SLS can handle a limited number of simultaneous endpoint registrations. Administering this field above the default value can result in system performance problems. For information about SLS, see *Administration for the Avaya G250 and Avaya G350 Media Gateways (03-300436)*.
MGP IPv4 Address / MGP IPv6 Address	This is the IP address of the H.248 branch gateway platform. The platform could reside in a network component which has its own IP address. The field supports the IPv4 and IPv6 addresses.
Module Type	Type of Avaya Media Module in the slot. Refer to the administration guide of the gateway being added for valid media modules and slot configuration. If an administered Media Module is in conflict with the inserted Media Module, a pound sign (#) appears to the left of the Module Type field on the Media Gateway screen.
Mutual Authentication	**Note:** This field complies with the Unified Capabilities Requirements (UCR) 2008 Change 3 requirements and is approved by Joint Interoperability Test Command (JITC). This field is available only for the USA Department of Defense (DoD) and approved Federal government customers. If the **Link Encryption Type** field is set to `none` or `ptls-only`, then the **Mutual Authentication** field is unavailable. The **Mutual Authentication** field is optional. If this field is set to `n`, the gateway registers to Communication Manager in FIPS mode. During the TLS handshake, Communication Manager requires the gateway to authenticate by using a digital certificate. Both the Communication Manager server as the TLS host and the gateway as the TLS client have to exchange valid Identity certificates. When the value of this field is set to `n`, Communication Manager accepts a TLS registration without the gateway Identity certificate. By default, the value of this field is `n`.

Table continues…

Field	Description
Name	Name assigned to the gateway.
Name (Controller)	Name assigned to the controller.
Network Region	Network Region assigned to the gateway. Used by the primary server to allocate resources from the nearest gateway. The number of characters is dependent upon the type of primary server.
Number	(Display only) Number assigned to the gateway.
Recovery Rule	Number of the auto-fallback recovery rule that applies to this gateway. The recovery rule is set on the system-parameters mg-recovery-rule screen. **none** — no automatic fallback registrations are accepted. See *Administering Avaya Aura®Communication Manager (03-300509)* and *Administering Network Connectivity on Avaya Aura®Communication Manager (555-233-504)*.
Registered?	(Display only) **y** — The gateway is currently registered with the primary server. **n** — The gateway is not currently registered with the primary server. **pd** — The gateway registration is pending, subject to the Recovery Rule assigned on the set on the system-parameters mg-recovery-rule screen.
Serial No	Used for the controller to identify the gateway
Site Data	General site information
Slot	(Display only) Slot number for the identified Media Module. Slots V8–V9, for virtual media modules, are listed after Slots V1–V4.
Type	Type of gateway. Use the help key to see the list of valid gateway types.
Use for IP Sync	Appears when the Synchronization over IP field is enabled. Indicates whether or not the G430 and G450 branch gateways are exempted from IP sync. By default, this field is enabled.

change media-gateway

Use **change media-gateway** to change the administration of a gateway.

Syntax

```
change media-gateway x
```

x Number of the assigned gateway.

See **add media-gateway** for an explanation of the field descriptions.

display media-gateway

Use **display media-gateway** to see information for a specific gateway.

Syntax

```
display media-gateway x [ schedule ]
```

x	Number of the assigned gateway.
schedule	Specify a time to run the command.

display media-gateway field descriptions

Field	Description
Registered?	(Display only) **ad** — The gateway is in a network region that was automatically disabled by the split registration solution feature. To enable the network region (if the network region has a gateway administered for time-day-window), the administrator does not need to perform any action . The region re-enables itself. **rd** — The gateway is in a network region that was both manually and automatically disabled. In this case, the status form shows only the manual status rd. To enable the network region, the administrator must run the **enable nr-registration** command. **ap** — The gateway is in a network region that was automatically disabled by the split registration solution feature and is now communicating with CM. To enable the network region (if the network region has a gateway administered for time-day-window), the administrator does not need to perform any action . The region re-enables itself. **rp** — The gateway is in a network region that was manually disabled by the **disable nr-registration** command and is now communicating with CM. If a network region is both manually and automatically disabled, the status form shows only the manual status rp. To enable the network region, the administrator must run the **enable nr-registration** command.

list media-gateway

Use **list media-gateway** from the primary server to see all administered gateways.

Syntax

```
list media-gateway [ type x ] [ region #  ] [ schedule ]
```

type *x* Type of gateway (g250, g430, g450).

region # Region number.

schedule Specify a time to run the command.

list media-gateway field descriptions

Field	Description
Number	The number assigned to the gateway by the primary server administration.
Name	The name given to the gateway by the user.
Serial No	The serial number of the gateway. Use the **`show system gateway CLI`** command or see the sticker on the back of the unit to locate the gateway serial number.
Rec Rule	Recovery Rule that applies to the gateway, as set on the system-parameters mg-recovery-rule screen. See *Administering Avaya Aura®Communication Manager (03–300509)* and *Administering Network Connectivity on Avaya Aura®Communication Manager (555-233-504)*.
FW Ver/ HW Vint	Firmware version and hardware vintage.
Cntrl IP Addr	IP address of the C-LAN or NIC.
IPv4 Address/ IPv6 Address	The IP address of the gateway. The IP address field is blank until the gateway registers for the first time. Once the gateway registers, the IP address appears, even if the gateway becomes unregistered. That IP address changes when a gateway with a different IP address is validly registered with the same administered identifier. The populated IP address is persistent over reboots. The IPv6 addresses of the gateways are supported.
Type	Type of gateway. Use the help key to list the valid types of gateways.
NetRgn	The network region number assigned to the gateway.
Reg?	**y** — A gateway is currently registered with the primary server. **n** — A gateway is not currently registered with the primary server. **pd** — A gateway registration is pending, subject to the Recovery Rule as assigned on the set on the system-parameters mg-recovery-rule screen. **ad** — The gateway 1 is in a network region that was automatically disabled by the split registration solution feature and the gateway 2 is in a network region that was manually disabled by the **`disable nr-registration`** command. To enable the network region (if the network region has a gateway administered for time-day-window), the

Table continues…

Field	Description
	administrator does not need to perform any action . The region re-enables itself. **rd** — The gateway is in a network region that was both manually and automatically disabled. In this case, the status form shows only the manual status **rd**. To enable the network region, the administrator must run the **enable nr-registration** command. **ap** — The gateway is in a network region that was automatically disabled by the split registration solution feature and is now communicating with CM. To enable the network region (if the network region has a gateway administered for time-day-window), the administrator does not need to perform any action. The region re-enables itself. **rp** — The gateway is in a network region that was manually disabled by the **disable nr-registration** command and is now communicating with CM. If a network region is both manually and automatically disabled, the status form shows only the manual status **rp**. To enable the network region, the administrator must run the **enable nr-registration** command.

reset media-gateway

Use **reset media-gateway** from the primary server to add a gateway to the system.

Syntax

```
reset media-gateway [ x | all ] [level 1|2|3]
```

x Number of the gateway to reset.

all Reset all registered gateways.

level 1 Forces a reset of the entire platform and is destructive to user connections. The gateway attempts to register with the gateway controllers on its MGC list.

level 2 Resets the H.248 link and does not tear-down calls. The gateway attempts to register with the gateway controllers on its MGC list. Use **reset media-gateway** level 2 to force a gateway off of a Survivable Remote Server.

level 3 Resets all media modules and tears down all calls.

status media-gateway

Use **status media-gateway** to see the alarm status of the administered gateways.

status media-gateways lists alarms, busyout summary, and H.248 link status for the gateways. The alarms are associated only with board-type alarms on the media modules. Status for VoIP and MGP alarms are provided via the Media Gateway Processor CLI.

Syntax

```
status media-gateway
```

status media-gateway field descriptions

Field	Description
ALARM SUMMARY	Current number of alarms (Major/Minor/Warning) for all administered gateways
BUSYOUT SUMMARY	Current number of trunks/stations in a busy-out state for all administered gateways
H.248 LINKSUMMARY	Current number of H.248 links that are down and up for all administered gateways
GATEWAY STATUS Alarms (Mj, Mi, Wn)	Number of major alarms, minor alarms, and warnings that exist on each administered gateways.
GATEWAY STATUS Lk	Status of the H.248 link on each administered gateways **up** — the link is up **dn** — the link is down **pd** — the gateway has not yet returned to the primary call controller after having at least one registration request denied. **ad** — The gateway 1 is in a network region that was automatically disabled by the split registration solution feature and the gateway 2 is in a region that was manually disabled by the **disable nr-registration** command. To enable the network region (if the network region has a gateway administered for time-day-window), the administrator does not need to perform any action . The region re-enables itself. **rd** — The gateway is in a network region that was both manually and automatically disabled. In this case, the status form shows only the manual status **rd**. To enable the network region, the administrator must run the **enable nr-registration** command. **ap** — The gateway 1 is in a network region that was automatically disabled by the split registration solution feature and is now communicating with CM and the gateway 2 is in a network region that was manually disabled by the **disable nr-registration** command and is now communicating with CM. To enable the network region (if the network region has a gateway administered for time-day-window), the administrator does not need to perform any action . The region re-enables itself. **rp** — The gateway is in a network region that was both manually and automatically disabled. In this case, the status form shows only the

Table continues…

Field	Description
	manual status **rp**. To enable the network region, the administrator must run the **enable nr-registration** command.

test media-gateway

Use **test media-gateway** from the primary server to run a board audit, an H.248 link audit, and an H.248 context audit.

- The link (test 1527) and context audits run successfully and no error codes are associated with the tests. Use **test media-gateway** to run an H.248 link audit when there is an alarm against a gateway for being unregistered when it actually is registered. If there is an interchange while a gateway is registering or unregistering, the alarm may appear and **status media-gateway** and **list media-gateway** may incorrectly show the gateway to be unregistered.
- Results of **test media-gateway** vary depending upon the configuration of the gateway.

Syntax

```
test media-gateway x
```

x Number of the assigned gateway

test media-gateway results

Gateway operating as	and is	Test result
main server	registered	pass
survivable remote server	registered	fail with error code 257
main server	unregistered, and the Link Loss Delay Timer period has not expired (link bounce is occurring)	fail with error code 769
main server	unregistered, and the Link Loss Delay Timer period has expired	fail with error code 1

media-processor

set media-processor

Use **set media-processor** to request a demand interchange of TN2602AP IP Media Resource 320 circuit packs. Use **set media-processor** *location* **lock** to prevent an undesired interchange.

Syntax

```
set media-processor  location [ lock | unlock ] [ override ]
```

location Location of the media resource to be active boards remain in their current state (active/standby).

lock Lock the current state.

unlock Clear the locked state.

override Force an interchange to a less-healthy board.

If **set media-processor** does not produce an interchange, an error message appears.

set media-processor error messages

SAT Error Message	Description
Command only supported by a TN2602 AP and greater board	The board location specified is not a TN2602 IP Media Resource. Use **list config** to verify the TN code and identify the board in this location.
Duplication not administered for this media-processor	This IP Media Resource is not administered as a duplicated board. Use **display ip-interface** to verify administration of the board.
Invalid duplication state for this media-processor pair	This pair of duplicated IP Media Resources has not transitioned to a state where one is active and one is standby. Use **status media-processor** to verify the duplication status of the IP Media Resources.
standby media-processor is not refreshed; use **override**	The standby IP Media Resource does not have the same set of calls up as the active board. An interchange making the standby active would cause a loss of some or all of the calls. Use **set media-processor** *location* override to ignore the warning and continue the interchange.

If the **set media-processor** interchange fails, the TEST RESULTS screen appears with a result of FAIL and an error code.

set media-processor test results error codes

Error Code	Description
1	Mode not configured. The board indicates that it has not been configured to be duplex mode.
2	Requested state not recognized. The message to the board to go active or standby is corrupted (neither active nor standby).
3	Board locked active. To prevent interchanges when certain operations are being performed, it is possible to disable interchanges with **set media-processor** lock. Error Code 3 appears when a demand interchange is requested and the board is locked in the active state. Use **set media-processor** unlock to unlock the boards.
4	Board locked standby. To prevent interchanges when certain operations are being performed, interchanges are disabled with **set media-processor** lock. Error Code

Table continues…

Error Code	Description
	4 is returned when a demand interchange is requested and the board is locked in the standby state. Use **set media-processor unlock** to unlock the boards.
5	Peer state of health better. The process to make this board standby was denied because the health of the current active board is better. Use **set media-processor override** to force the interchange if necessary. Use **set media-processor lock** within 20 seconds; otherwise the boards will automatically interchange back.
6	Peer state of health worse. A request to make this board active was denied because the health of the current standby board is worse. Use **set media-processor override** to force the interchange if necessary. Use **set media-processor lock** within 20 seconds; otherwise the boards will automatically interchange back.
7	Interchange prevented by the damping timer. To prevent interchange oscillation, and to allow for locking of less health boards in the active state, a damping timer of 20 seconds is started after each interchange. If an interchange request is received during that period, it is prevented and this error code is returned. Use **set media-processor override** to bypass this operation.
8	Internal error prevented interchange. An internal error in the board prevented the interchange.
9	Incorrect network configuration. For duplex configurations, additional network configuration data values are required, and they must be valid. Specifically, both boards must be on the same subnet and they each must have their peer addresses. If this information has not been configured or it is invalid, the interchange fails with this code.
10	Interchange in progress. If a state transition is already in progress when an interchange request is received, the state requested by the command is compared with the state currently being transitioned to. If the states are not the same, the interchange request is ignored and this error code is returned.
11	Internal error. This error is reported if an interchange request is received and the duplication subsystem on the board is stuck in the arbitration state, unable to go either active or standby as a result of a mode downlink from CM software
12	Internal error. This error is reported if an interchange request is received and the duplication subsystem on the board is stuck in the arbitration state, unable to go either active or standby as a result of a previous interchange request.
501	Internal error. This error is reported when no response is received from the active-going-standby board.
502	Internal error. This error is reported when no response is received from the standby-going-active board.

status media-processor

Use **status media-processor** to see the busyout status of the specified MedPro or IPMedPro media processor board.

Syntax

```
status media-processor [ location | all ]
```

location	Location of the media processor.
all	All media processors in a system.

status media-processor field descriptions

Field	Description
If a circuit pack is duplicated, this screen indicates which is the active board. na — non-duplicated circuit packs.	
Slot	Location of the media processor circuit pack
Code	TN code for the media processor circuit pack
Alarms	Mj — major alarms Mn — minor alarms Wn — warnings
Links	Status of the circuit pack links for single and duplicated circuit packs. Pr — Peer Link Cl — Control Link El — Ethernet Link up — the link is up dn — the link is down na — not applicable
Dup	na — not applicable, for single circuit packs The slot location of the duplicated media processor circuit pack, If the circuit pack is duplicated.
St	Status of the media processor circuit pack act — active sby — standby dis — disabled bsy — busied out ini — init

status media-processor board

Use **`status media-processor board`** to see the status of the specified MedPro or IPMedPro media processor board. List the circuit pack and digital signal processor (DSP) usage, and the active and standby circuit pack usage for duplicated circuit pack

Syntax

```
status media-processor board location
```

location Location of the media processor.

status media-processor board field descriptions

Field	Description
Duplication State	Status of each duplicated circuit pack. active/standby/init
Links	Status of the circuit pack link, for single or duplicated circuit packs: • **up/down** • **mpcl** — Media Processor Control Link • **eth** — Ethernet link • **peer** — peer-to-peer link (applies only to duplicated circuit packs)
Alarms	The number of major alarms, minor alarms, or warnings. • 0–99 • **mj** — major alarms • **mn** — minor alarms • **wn** — warnings
Standby Refreshed	**y/n** **y** — the standby circuit pack in a duplicated pair is in sync with Communication Manager. Appears for duplicated circuit packs.
Network Region	The network region number of the duplicated circuit packs. 1–250.
Shared IP Address	The virtual IP address that is shared between the two duplicated circuit packs. Appears for duplicated circuit packs.
Shared Virt-MAC	The virtual MAC address that is shared between two duplicated circuit packs. Appears for duplicated circuit packs.
Locked	**y/n** **y** — **set media-processor override** or **set media-processor lock** command is in use. Appears for duplicated circuit packs.

meet-me-vdn

reset meet-me-vdn

Administrators use the **reset meet-me-vdn** command to disconnect all the members of a given meet-me conference and then place that conference back into an idle/active state. The maintenance commands **status meet-me-vdn** *xxxx* and **reset meet-me-vdn** *xxxx* are added for the meet-me conference VDNs; where *xxxx* is the extension.

Type the command **reset meet-me-vdn** *xxxx* and then type the command **status meet-me-vdn** *xxxx*.

Syntax

```
reset meet-me-vdn  xxxx
```

xxxx Extension number.

mg-announcements

status mg-announcements

Use **status mg-announcements** to see the status of the announcements of the administered gateways.

Syntax

```
status mg-announcements
```

status mg-announcements field descriptions

Field	Description
Announcements Enabled?	Displays whether the announcements for the gateway have been enabled by using the **enable announcement-board** command. If Announcements Enabled? is **y**, announcements for the gateway have been enabled. If Announcements Enabled? is **n**, announcements for the gateway have not been enabled.
CF Storage Usage (MB)	If the gateway is G450 or G430 and the Enable CF? field on the change media-gateway screen is **y**, the memory data of the compact

Table continues…

Field	Description
	flash is displayed. If CF Storage Usage(MB) field is not applicable for a gateway, **n/a** is displayed. CF Storage Usage (MB) has the following fields: • **Total** — displays the total memory of the compact flash • **Annc** — displays how much memory of the compact flash is currently used for the announcements • **Avail** — displays how much memory of the compact flash is left for use There could be other things along with the gateway announcements which are stored on the compact flash. So, it is not necessary that the total memory of **Annc** and **Avail** adds up to to the total memory of the compact flash. Also, the numbers that are represented are block-sized numbers and different compact flash cards could have different block sizes.
CF Status	Displays the status of the compact flash. The status of the compact flash is displayed as one of the following: • **Ins** — the compact flash is inserted on the gateway and is recognizable. • **Act** — the compact flash is being used. • **Err** — The compact flash: - is either not present or not recognized - does not have sufficient space on the compact flash - does not have sufficient RAM available for usage

mg-return

enable mg-return

Use **enable mg-return** to perform automatic return of gateways to the main or Survivable Core Server without needing to reset each Survivable Remote Server.

The administrator can force the main or Survivable Core Server to accept the gateways and telephones.

Syntax

```
enable mg-return  network-region R | all
```

network-region *R*	Enable all gateways within network region R.
all	Enable all the gateways.

The **enable mg-return** command overrides the gateway recovery rules that block registration if Survivable Remote Servers are active or inactive. Such overriding can be applied per region.

If there are no gateways in the region and the command **enable mg-return network-region R** is run, the following error message is shown:

```
IP network region has no gateways administered.
```

The administrator can run the command **disable nr-registration** on any region. If the status of a gateway in that region is already **ad** or **ap**, the status changes to **rd**. For information on the gateway registration statuses — **ad**, **ap**, and **rd** — see the field descriptions of **display media-gateway**, **list media-gateway**, and **status media-gateway**.

Important:

The **enable mg-return** command remains active for a period of 60 minutes. During this period of 60 minutes, if you want to move the gateways and phones from server to server, you must run the **disable mg-return** command first to end the 60 minutes timer. If you do not run the **disable mg-return** command, the timer either ends itself after a period of 60 minutes or after the Survivable Remote Server reports to the main Communication Manager server that the gateways have unregistered from the Survivable Remote Server.

mis

busyout mis

Use **busyout mis** to busyout a management information system.

Syntax

```
busyout mis [ processor-channel identifier | all]
```

processor-channel identifier	Busyout an MIS link.
all	Busyout all MIS links.

release mis

Use **release mis** to activate management information systems. Hardware tests are executed to verify that equipment is functioning properly.

Syntax

```
release mis [ processor-channel identifier | all ]
```

processor-channel identifier	Release an individual MIS link.
all	Release all MIS links.

modem-pool

release modem-pool

Use **release modem-pool** to deactivate specified modem pool groups or group members. Specify group numbers and member numbers to release single group members. Specify modem pool group numbers to release members in a modem pool group.

For more information see Busyout and Release Commands.

Syntax

```
release modem-pool  group # | member #
```

group #	1–5. Pair of analog and digital line ports (or two pairs for the Integrated modem-pool case).
member #	1–32.

test modem-pool

Use **test modem-pool** to performs hardware diagnostic tests on the specified modem pool group or an individual member of a specified group (Combined or Integrated). A combined modem-pool group consists of pairs of analog and digital line ports. One pair of analog and digital line ports used for modem-pooling is called a conversion resource. An Integrated group consists of modem-pool circuit packs, each containing two conversion resources. Therefore, when a member number is specified for a combined modem-pool group, one conversion resource is tested, and when a member number is specified for an integrated modem-pool group, two conversion resources are tested.

Syntax

```
test modem-pool[ group # | member # ][ short | long ][ repeat  # | clear ][ schedule ]
```

group #	The administered group number (1–5).

member # 1–32.

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

schedule Specify a time to run the command.

moh-analog-group

list moh-analog-group

Use **list moh-analog-group** to list **Music On Hold** groups and see how many members (audio sources) are in each group.

For more information on the Music On Hold Groups screen, see *Administering Avaya Aura® Communication Manager*.

Syntax

```
list moh-analog-group {[ 1-Max ] ( number n |( to-number  n )|  count n )}[ schedule ]
```

1-Max Music On Hold number.

number *n* to-number *n* Range of Music On Hold group numbers to see on the page.

count *n* Number of Music On Hold groups to see on the page.

schedule Specify a time to run the command.

list moh-analog-group field descriptions

Field	Description
Number	Number of the Music On Hold group.
Name	Name of the Music On Hold group.
Number of Sources	Number of members (sources) in the Music On Hold group

monitored-station

list monitored-station

Use **list monitored-station** to see information on stations controlled by domain-controlled associations. Each station can have a maximum of four domain-controlled associations.

Syntax

```
list monitored-station  [ start extension ] [  count xxxx ]
```

start *extension* Starting extension for the list.

count *xxxx* Number of stations on the list.

list monitored-station field descriptions

Field	Description
Ext	The extension number of the station.
Link Ext	Index to a table where the information about a particular ASAI link is stored.
CRV	ISDN Call Reference Value

mst

clear mst

Use **clear mst** before a trace. If **clear mst** is active during a trace, it clears unwanted data.

Syntax

```
clear mst
```

disable mst

Use **disable mst** to stop the message trace facility. If the trace was not already disabled, the command inserts a GAP marker into the trace. The user should execute **disable mst** when the trace is complete. If left enabled, the trace continues to use CPU time until the time limit expires. Entering **disable mst** has no effect on the system if the trace is already disabled. To view the results of the trace, enter **list mst**.

Syntax

```
disable mst
```

display mst

Use **display mst** to provide message tracing for SIP.

Syntax

```
display mst
```

display mst field descriptions

Field	Description
Signalling Group	The assigned signaling group number which provides message tracing for all SIP messaging on the signaling group. The signaling group number is from 1 to 999, or leave blank.
Message Bodies	Indicates if SDP encoding is included in the trace. The default value is **y**.
Calling User	Allows entry for user portion of incoming URI. The length of the URI is from 0 to 20, or leave blank.
Called User	Allows entry for user portion of outgoing URI. The length of the URI is from 0 to 20, or leave blank.

list mst

Use **list mst** to see the messages in the trace buffer while a trace is active or disabled. If the trace is active, older messages may be sporadically omitted if wraparound is selected and the message rate is high. The integrity of the buffer remains intact even when **list mst** is used repeatedly.

Syntax

```
list mst  [ from message number ] [ count  number ][ continuous | LIFO | FIFO | auto-page ]
```

from *message number* First message in the list. List indicates if the number is not in the buffer, and no additional messages appear.

If no message number is entered, the list begins with the oldest FIFO message.

count *number* The number of messages in the list.

Use this number to limit the trace.

continuous	Display updates as new messages enter the trace buffer (FIFO). This option is most useful in conjunction with **auto-page**. The command terminates when canceled by the user.
LIFO	Show newest message first.
FIFO	Show messages in the order received.
auto-page	The screen will automatically page when full. Use with **continuous** to see messages arrive.

MST message descriptions

The terminology Message [**n**] used in this section refers to the byte at offset **n** in the message being displayed.

MST message types contain a version number. When the structure of the MST message changes, the version field in the MST buffer also changes. Version 1 displays a blank in the version field immediately after the MST message type field. Subsequent versions display the version number after the MST message type field and are connected with a hyphen (-). For example: Version 2 of the X.25 Application error/notification message added the text of the pm state table stimulus, which was ignored.

list mst field descriptions

Field	Description
Number	The sequence number for the message.
Date/Time	The date/time of the message.
Type	MST message type: 60 = ISDN uplink 62 = ISDN downlink 6C = ISDN level 2 primitive
Message	Message text in hexadecimal.

Example

```
list mst continuous
list mst continuous auto-page
list mst LIFO
list mst from 222 count 7
```


Comments on this document? infodev@avaya.com

multimedia

list multimedia

Use **list multimedia** to see the list of multimedia endpoints, h.320-multimedia endpoints, multimedia IP endoints, or unregistered multimedia IP endpoints.

Syntax

```
multimedia [ endpoints | h.320-stations | ip-stations | ip-unregistered ][ ext x ]
[ to-ext x ] [ count n ] [ schedule ]
```

endpoints	List multimedia endpoints.
h.320 endpoints	List multimedia H.320 endpoints.
ip-endpoints	List multimedia IP endpoints.
ip-unregistered	List unregistered multimedia IP endpoints.
ext *x*	List information for a specific extension.
to-ext *x*	when used with `[ext x]`, list information for all multimedia endpoint types beginning with one extension and ending with another.
count *n*	List a certain number (***n***) of multimedia endpoints.
schedule	Specify a time to run the command.

list multimedia field descriptions

Field	Description
IP STATION	
Ext	Extension of the IP station.
Registered	Show the current registration status of the endpoint.
Port	Port information for the IP telephone when an IP telephone and IP Softphone are in service on the same extension simultaneously.
Registered	Shows the current registration status of the endpoint.
MEDIA COMPLEX	
Ext	Extension of the endpoint.
Port	Port information for the IP telephone when an IP telephone and IP Softphone are in service on the same extension simultaneously.
Registered	Shows the current registration status of the endpoint.

night-service

list night-service attendant

Use **list night-service attendant** to see all the attendants that are in night service.

Syntax

```
list night-service attendant
```

list night-service attendant field descriptions

Field	Description
No.	The night service attendant number.
Extension	The extension of the voice or data endpoint associated with the night service attendant.
Name	The name of the night service attendant.
Group NO	The attendant group number.

list night-service hunt-group

Use **list night-service hunt-group** to see all the hunt groups that are in night service.

Syntax

```
list night-service hunt-group
```

list night-service hunt-group field descriptions

Field	Description
No.	The night service hunt group number.
	The night service destination. The night service destination can be an extension, a recorded announcement extension, a vector directory number, a hunt group extension, or **attd** if you want to direct calls to the attendant.

list night-service trunk-group

Use **list night-service trunk-group** to see all the trunk groups that are in night service.

Syntax

```
list night-service trunk-group
```

list night-service trunk-group field descriptions

Field	Description
No.	The night service trunk group number.
Destination	The night service destination. The night service destination can be an extension, a recorded announcement extension, a vector directory number, a hunt group extension, or **attd** if you want to direct calls to the attendant.

node-names

display node-names

Use **display node-names** to see a list of the administered node names.

Syntax

```
display node-names  [ schedule ]
```

schedule Specify a time to run the command.

display node-names field descriptions

Field	Description
Name	Identifies the name of the adjunct or switch node. Enter 1–7 characters for audix or msa; Enter 1–20 characters for others. Default is blank. Node name for CMS nodes, DCS nodes, and so forth.
IP Address	IP address for the adjunct or switch. Enter 0–255 or leave blank.

nr-registration

disable nr-registration

Caution:

disable nr-registration can cause momentary service disruption. It causes all gateways and IP phones in a network region to unregister from the server where the command is executed. **disable nr-registration** is automatically saved across system restarts even without **save translation**.

Use **disable nr-registration** to deny gateways and IP-phones within a specified IP Network Region from registering on the primary server or survivable processor. This causes the gateways and IP phones to register instead with an alternate server or Survivable Remote Server. This is useful when network outages cause gateways and IP phones to disconnect and reregister with the primary server in an interval that is too short for the endpoints to fail over to a Survivable Remote Server.

Use **disable nr-registration** on a primary server and a Survivable Core Server. The disabled network region registration state on the primary server is not file-synced to the Survivable Remote Server or associated Survivable Core Server.

A gateway must be assigned to the specified network region.

If you have set the value of the Force Phones and Gateways to Active LSPs? field in the system-parameters ip-options screen as y and then run the **disable nr-registration** command on one network region, Communication Manager applies this command to all the network regions associated with the Survivable Remote Server. For example, a single Survivable Remote Server is the backup server for multiple network regions—network region 1 and network region 2. A system administrator runs the **disable nr-registration 1** command. The Communication Manager server disables region 2. A gateway in network region 1 is unregistered from the Communication Manager server and registers to the Survivable Remote Server. The Survivable Remote Server reports to the main Communication Manager server that the Survivable Remote Server is active. The Communication Manager server then automatically disables network region 2.

The **disable nr-registration** command causes a disable network region warning alarm to appear in the alarm log.

Note:

When the Enable Detection and Alarms field is y on the system-parameters ip-options screen (**change system-parameters ip-options**) the detection of the hyperactive link bounce is enabled which will cause associated gateway and network region alarms.

Syntax

```
disable nr-registration x
```

x IP network region number. A gateway must be assigned to the network region.

enable nr-registration

Use **enable nr-registration** to end an active **disable nr-registration** command.

This enables the gateways and IP-phones within the specified IP Network Region to register with the primary server or survivable processor.

However, the **enable nr-registration** command can only end an active **disable nr-registration** command. This command cannot override any other condition that prevents the gateways and IP phones to register with the primary server or survivable processor.

For example, if the time-day-window prevents the gateways and IP phones to register with the primary server, you cannot use the **enable nr-registration** command to register the gateways and IP phones with the primary server.

If you have set the value for the Force Phones and Gateways to Active LSPs? field in the system-parameters ip-options screen as y and then run the **enable nr-registration** command when the Survivable Remote Server is active, the command does not immediately enable the network region. Instead, the **enable nr-registration** command puts the network region into an auto-disabled state. Communication Manager does this so that if the Survivable Remote Server is backing up more than one region, the **enable nr-registration** command does not cause a split registration by allowing endpoints in that one region to return to the Communication Manager server while endpoints in other regions backed up by the same Survivable Remote Server stay on the Survivable Remote Server.

Use **enable nr-registration** on a primary server, a Survivable Core Server, and a Survivable Remote Server Survivable Remote Server. The enabled network region registration state on the primary server is not file-synced to the Survivable Remote Server or associated Survivable Core Server.

Syntax

```
enable nr-registration x
```

x IP network region number.

A gateway must be assigned to the network region.

status nr-registration

Use **status nr-registration** to view information about the status of the network regions and the link status of the gateways in the network regions.

Note:

To disable network regions manually, use the command **disable nr-registrations [network region number]**. To enable a network region manually, use the command **enable nr-registrations [network region number]**.

The Split Registrations Prevention Feature (SRPF) automatically disables certain network regions when those regions are controlled by a Survivable Remote Server which has gone active.

To enable SRPF, set Force Phones and Gateways to Active LSPs? to n on the system-parameters ip-options screen. For more information about SRPF, see *Administering Avaya Aura®Communication Manager (03–300509)*.

status nr-registration all-regions

Use **status nr-registration all-regions** to view the status of the network regions.

Syntax

```
status nr-registration   all-regions
```

all-regions Status of all network regions.

status nr-registration all-regions field descriptions

Field	Description
NR	Displays the network region number.
St	Displays the status of a network region. The following are the available values for a network region: • **en** — network region is enabled • **rd** — network region manually disabled • **prd** — pending manual disable • **pen** — pending manual enable • **pae** — pending auto-enable • **pad** — pending auto-disable • **ad** — network region auto-disabled

status nr-registration network-region

Use **status nr-registration network-region** to view the link status of the gateways in a specific network region.

Syntax

```
status nr-registration network-region x
```

network-region *x* Network region number.

status nr-registration network-region field descriptions

Field	Description
MG	Displays the gateway number.
St	Displays the status of a gateway. The following are the possible values for the link status of a gateway: • **n** — not registered • **y** — gateway is registered • **p** — attempting to fallback from a Survivable Remote Server or other backup server • **rd** — network region disabled, link status unknown • **ad** — the region is auto-disabled, link status unknown • **ap** — the region is auto-disabled and the gateway is attempting to fallback from a Survivable Remote Server or other backup server

Note:

If the status of all the gateways is in a **p** or **ap** state, the gateways fall back to the server according to the recovery rules. The user can run **enable mg-return** to enable the gateways to register to the network regions immediately. This command allows the user to override any recovery rules including the case where none are defined. The command has two arguments: all and network-region NR-num.

status nr-registration survivable-processor node-name

Use **status nr-registration survivable-processor node-name** to view the link status of the gateways using a survivable processor.

If the Split Registration Prevention Feature (SRPF) is enabled, a survivable processor, which can either be a Survivable Remote Server or a Survivable Core Server acting as a Survivable Remote Server, can cover multiple network regions. **status nr-registration survivable-processor node-name x** displays the status of all the gateways for all the network regions on the server.

Syntax

```
status nr-registration survivable-processor node-name x
```

x Node name of the survivable processor.

status nr-registration survivable-processor node-name field descriptions

Field	Description
MG	Displays the gateway number.
St	Displays the status of a gateway.

Table continues…

Field	Description
	The following are the possible values for the link status of a gateway: • **n** — not registered • **y** — gateway is registered • **p** — attempting to fallback from a Survivable Remote Server or other backup server • **rd** — network region disabled, link status unknown • **ad** — the region is auto-disabled, link status unknown • **ap** — the region is auto-disabled and the gateway is attempting to fallback from a Survivable Remote Server or other backup server

Note:

If the status of all the gateways is in a **p** or **ap** state, run **`enable mg-return`** to enable the gateways to register to the network regions.

options

set options

Use **`set options`** to administer the levels of alarm reporting.

Syntax

```
set options
```

set options field descriptions

Field	Description
Major	Set the alarm reporting type for the following major alarms: • On-board station alarms • Off-board station alarms • On-board trunk alarms (Alarm group 1) • Off-board trunk alarms (Alarm group 1) • On-board trunk alarms (Alarm group 2) • Off-board trunk alarms (Alarm group 2) • On-board trunk alarms (Alarm group 3) • Off-board trunk alarms (Alarm group 3) • On-board trunk alarms (Alarm group 4)

Table continues…

Field	Description
	• Off-board trunk alarms (Alarm group 4) • On-board adjunct link alarms • Off-board adjunct link alarms • Off-board DS1 alarms • Off-board TCP/IP link alarms • Off-board alarms (other)
Minor	Set the alarm reporting type for the following minor alarms: • On-board station alarms • Off-board station alarms • On-board trunk alarms (Alarm group 1) • Off-board trunk alarms (Alarm group 1) • On-board trunk alarms (Alarm group 2) • Off-board trunk alarms (Alarm group 2) • On-board trunk alarms (Alarm group 3) • Off-board trunk alarms (Alarm group 3) • On-board trunk alarms (Alarm group 4) • Off-board trunk alarms (Alarm group 4) • On-board adjunct link alarms • Off-board adjunct link alarms • Off-board MASI link alarms • Off-board DS1 alarms • Off-board TCP/IP link alarms • Off-board alarms (other) • Off-board ATM network alarms

Alarm reporting options

Option	Description
Minor	Alarms are raised as maintenance testing discovers them and the severity of the alarm is upgraded or downgraded to a minor. Alarmed resources that are normally taken out of service are still taken out of service. LEDs on the port board and maintenance board follow the normal minor alarm LED strategy and there is a call to the receiving OSS.
Warning	Alarms are raised as maintenance testing discovers them, and the severity of the alarm is downgraded to a warning. The advantage is

Table continues…

Option	Description
	that the Alarm Log can still be used to pinpoint trunk or station problems. Alarmed resources that are normally taken out-of-service are still taken out-of-service. Alarm LEDs light on the port circuit pack and Maintenance circuit pack as before, but no attendant LEDs or stations reporting alarms are affected. There is no call to INADS.
Report	Downgrade the alarm to a warning and report the warning to INADS. This is not supported by Avaya.
Yes	Alarms are raised in the normal manner. There is no filtering of alarm data.
No	Alarms raised on a trunk, station, or adjunct in this category are dropped. Error information is provided, but there is no trace of an alarm. There is no LED activity and no call to INADS. Because resources are taken out-of-service without any record, you must use this option only when other options do not provide the desired result.

off-pbx-telephone

status off-pbx-telephone station

Use **status off-pbx-telephone station** to see the service state and connected ports of an Extended Access (off-PBX and on-PBX) station.

Note:

The on-PBX station support only applies to One-X application types.

Extended Access applications include:

- Extension to Cellular
- Cellular Service Provider (CSP)
- Session Initiation Protocol (SIP)
- Seamless Converged Communications Across Network (SCCAN)
- Avaya One-X® Client Enablement Services (Avaya One-X® CES)

Syntax

```
status off-pbx-telephone station x
```

x Station extension.

Comments on this document? infodev@avaya.com

status off-pbx-telephone station field descriptions

Field	Description
No.	The order in which the Extension to Cellular, EC500 application was administered on the Stations with Off-PBX Telephone Integration (**add off-pbx-telephone station-mapping**) screen.
Type	The type of Extended Access application.
Trunk/Member Group	The number of the Trunk Group and Trunk Group member associated with the station. If there is no active outside call, the message appears: `No trunks associated with this off-pbx telephone station`
Port	The port connected to the physical station. This physical station is mapped to an Extended Access telephone such as a cellular phone.
Connected Ports	The connected ports of Extended Access calls.

list off-pbx-telephone station-mapping

Use **list off-pbx-telephone station-mapping** to see the application associated with administered stations.

Syntax

```
list off-pbx-telephone station-mapping x[countn] [schedule]
```

x The complete extension, or the partial extension plus asterisk (*).

count *n* This is an optional parameter. Use the count parameter to specify the number of stations you want the system to display.

schedule This is an optional parameter. Use the schedule parameter to print the output.

list off-pbx-telephone station-mapping field descriptions

For additional information about the following fields, see 'Stations with Off-PBX Telephone Integration' section in *Avaya Aura®Communication Manager Screen Reference (03-602878)*.

Field	Description
Station Extension	The extension assigned to the user.
Appl	The type of application used for mapping the OPTIM station to off-PBX telephone and on-PBX telephone. • **CSP** — cell phone with Extension to Cellular provided by the cellular service provider • **EC500** — cell phone with Extension to Cellular • **HEMU** — Home Enterprise Mobility User • **OPS** — SIP Enablement Services (SES) enabled phone

Table continues…

Field	Description
	• **PBFMC** — Public Fixed Mobile Convergence • **PVFMC** — Private Fixed Mobile Convergence • **SCCAN** — wireless SIP Enablement Services (SES) phone and cell phone • **VEMU** — Visited Enterprise Mobility User • **VIEMU** — Visited Initial Enterprise Mobility User • **One-X** — Used by Avaya one-X® Client Enablement Services
CC	The country code associated with the off-PBX telephone.
Phone Number	The phone number of the off-PBX telephone or the extension of the on-PBX telephone.
Config Set	The configuration set to be used for mapping. This field can be blank if not administrable.
Trunk Select	The trunk group that connects to the off-PBX telephone or the extension when applicable for the on-PBX telephone.
Mapping Mode	The direction for calls allowed at the off-PBX telephone or on-PBX telephone. On-PBX telephones mapping mode is always set to termination only.
Calls Allowed	The number of simultaneously active calls on the off-PBX telephone.

packet-interface

reset packet-interface

Use **reset packet-interface** to reset and initialize the Packet Interface (PKT-INT) module on the IPSI (TN2312AP) circuit packs.

A standby PKT-INT can always be reset. An active PKT-INT can be reset if it has been taken out of service by the software. There is no **busyout** command for the PKT-INT. When the PKT-INT goes out of service due to errors, the IPSI has a bad PKT-INT state of health, and the IPSI goes out of service.

Taking an IPSI out of service also takes the PKT-INT out of service. Attempts to reset the PKT-INT on a busied-out IPSI are ignored because **release ipserver-interface** resets the PKT-INT.

Syntax

```
reset packet-interface UUc
```

UUc The cabinet/carrier location of the IPSI board to be released.

status packet-interface

Use **status packet-interface** to see the status of the IPSIs in the servers.

Use **status packet-interface** to see the status of all packet-interface circuit packs in the system along with link information. The service state appears for both active and standby packet-interface circuit packs. Link status information including total, active and failed links are displayed for active packet-interface circuit packs only.

If there are no standby Packet Interface circuit packs, or if the standby is inaccessible (due to handshake failure or incomplete memory refresh) the standby packet-interface circuit packs will be in the uninstalled state.

When a packet-interface circuit pack is out-of-service or uninstalled, it is not used to establish and maintain links. When the circuit pack returns to in-service status, new links are again assigned to it.

status packet-interface currently provides status for up to five packet interfaces. The command line takes a cabinet number as an argument and displays information about all packet interfaces for the cabinet. If there are no IPSIs in the requested cabinet, an error displays.

Syntax

```
status packet-interface UU
```

UU Cabinet number.

On the **status packet-interface** screen, separate columns identify each Packet Interface circuit pack slot. Service state appears for both active and standby packet-interface circuit packs. A cabinet number must be specified. If there are no IPSIs in the cabinet, the `No IPSI in cabinet specified message` appears. Locate the IPSI using **list ipserver-interface**.

status packet-interface field descriptions

Field	Description
Location	The packet-interface cabinet, carrier and circuit pack position number.
Service State	One of the following states appears: in-service, out-of-service or uninstalled. The standby state is used in place of in-service for standby packet-interface circuit packs.
Total Links	The total number of links.
Active Links	The number of links that are in use.
Failed Links	The number of links that failed to be established. These links are in a recovery state and not active. The failures can arise from problems in the packet-interface, EI or center stage hardware. The number of failed links is the number of total links minus the number of active links.

test packet-interface

Use **test packet-interface** to perform hardware diagnostic tests on any or all of the Packet Interface circuit packs in a specified carrier. Tests performed include local memory checksum tests, loop-around tests, and checks of failure counters. On Linux platforms, **test packet-interface** tests the IPSI circuit packs.

The Maintenance Loop-Around test (#886) is included in the test sequences of active packet-interface circuit packs only. The Active-Standby Peer Link test (#888) is included in the test sequences of the standby packet-interface circuit packs only.

If the packet-interface circuit pack is in the out-of-service or uninstalled states, no demand tests as well as scheduled, periodic and error tests will run. See also **reset packet-interface** and **status packet-interface**.

Syntax

```
test packet-interface UUc [ short  |  long ] [ repeat #  |  clear ] [ schedule ]
```

UUc	The cabinet/carrier location of the IPSI board to be released.
short	Execute a series of nondestructive diagnostic tests.
long	Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
repeat #	Number of times to repeat the test, between 1 and 100.
clear	Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.
schedule	Specify a time to run the command.

periodic-scheduled

status periodic-scheduled

Use **status periodic-scheduled** to see summary information about currently active and recently completed background testing. Periodic tests run every hour, and scheduled tests run daily. Starting and stopping times, and other parameters for daily scheduled testing, are administered with **change system-parameters maintenance**.

Syntax

```
status periodic-scheduled
```

status periodic-scheduled field descriptions

Field	Description
PERIODIC MAINTENANCE section	This data reflects the status of periodic maintenance which is performed hourly, according to the selections made on the change system-parameters maintenance screen. See *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)* for more information.
Pre-SCHEDULED MAINTENANCE section	The data in this section reflects the status of pre-scheduled maintenance. Pre-scheduled maintenance can include interchanges of duplicated components and backup of translation data. It is performed according to selections made on the change system-parameters maintenance screen.
SCHEDULED MAINTENANCE section	The data in this section reflects the status of scheduled maintenance which is performed daily. Scheduled maintenance is performed according to the selections made on the change system-parameters maintenance screen.
System Critical	System-critical resources are those whose health affects the entire system such as the processor. These are always tested first.
Shared Resource	Shared resources are those that are used by many users, such as trunks. These are tested after system critical resources.
Single User	Single-user resources are those whose health affects only one user, such as voice stations.
Total	Total duration of previous periodic or scheduled maintenance cycle. Note: Scheduled maintenance total does not include pre-scheduled maintenance duration.
Current Cycle % Complete	The ratio of the number of maintenance objects tested to the total number of maintenance objects tested during a cycle. For periodic tests, the ratio is for the current cycle, if active; or for the last completed cycle if not. For scheduled tests, the ratio is for the last completed cycle.
Current Cycle Active	Reflects whether the current cycle of periodic, pre-scheduled or scheduled maintenance is currently running. Value is `y` if currently running or `n` if it is not.
Previous Cycle Duration	Reflects how long the system critical, shared resource, or single user maintenance activities took for the previous cycle of maintenance.
Rate of Completed Cycles	Reflects how often maintenance cycle is performed.
Start Time of Current or Previous Cycle	Time at which maintenance cycle began in *month/day/ hour:minute:second* format. For scheduled maintenance, this time reflects when the pre-scheduled maintenance began.

pin

change pin

Use **change pin** to change the PIN for the dadmin login or for the second craft login. The PIN should be a minimum of seven characters and a maximum of 32 characters. You can use only upper and lower case characters, numbers, and special characters. PINs do not expire. PINs must conform to the minimum and maximum lengths and must contain at least one letter and one number. PINs are not displayed when typed on the screen or when changed.

The dadmin and init logins can change the PIN for dadmin or the second craft login.

The second craft login can change the PIN for only the second craft login.

Syntax

```
change pin [dadmin] | [second craft login name]
```

dadmin	The dadmin login.
second craft login name	The craft2 login.

reset pin

The **reset pin** command resets the PIN for the dadmin login or the second craft login. The old PIN is not required. When a PIN is reset, it returns to the state where the PIN must be re-created on the next SAT access. The PIN of the second craft login can be changed but cannot be reset to an uninitialized value.

The command is accessible only to the init and dadmin logins, and either login may reset the PIN. When the command is typed, the system displays the `Command completed successfully` message.

Syntax

```
reset pin [dadmin] | [second craft login name]
```

dadmin	The dadmin login.
second craft login name	The craft2 login.

ping

ping

When debugging connectivity problems, **ping** command helps to indicate low-level connectivity. If an external ping works but higher-level applications such as DCS, CMS, or INTUITY do not, there probably is connectivity to the board. Interrogate the switch for other clues as to why the higher-level application is not working.

The ping command checks low-level connectivity between two IP-connected peers: a destination and a source.

- The destination can be:
  - an IP address (ip-address addr)
  - a node (node-name name)
- The source can be:
  - a C-LAN or IP Medpro board (board *location*)
  - a Softphone, IP telephone or Remote Office (R300) telephone (source port-id).

  If no source is specified, the first C-LAN in the same region as the IP address that is being pinged is used as the source.

Use this test to check the circuitry in the data path for a peer-to-peer IP layer connection. This test is nondestructive.

Note:

Pings from an IP Medpro board reflect audio transport performance. Pings from a C-LAN board reflect control information transport performance. The recipient of a ping will reply with the same Quality of Service (QoS) value found in the received packet, so the time measurements reported should reflect the behavior of the type of packets sent. When an IP Medpro board is used as the source, the default DiffServ and 802.1p/Q parameters downloaded to that board are used in the execution of the **ping**.

Caution:

Repeated ping tests can consume a lot of bandwidth and can bog down a network as a result. If the network is already heavily loaded, a ping test can fail even if there is connectivity between the source and destination.

Syntax

```
ping ip-address addr | node-name name [ board location | source port-id ] [
packet-length len ] [ repeat # ]
```

ip-address *addr* Specify a valid IPv4 or IPv6 address of the device to ping, *www.xxx.yyy.zzz*.

node-name *name* The name of the node to ping. Use **`display node-names ip`** to see what IP nodes are administered.

board *location* The location of the C-LAN or IP Medpro board (*location*) used as the source of the ping. Specify the board if there are multiple C-LAN or IP Medpro boards. If neither board nor source is given, the first C-LAN in the same region as the IP address that is being pinged will be the source of the ping.

source *port-id* The virtual endpoint port ID to use as the source of the ping. This can be the virtual endpoint port ID of a softphone, IP telephone, or Remote Max (R300) telephone. Use **`status station ext`** to determine the virtual endpoint port ID of a telephone. If neither board nor source is given, the first C-LAN in the same region as the IP address that is being pinged will be the source of the ping.

packet-length *len* The packet length of the ping packet, from 64 to 1500. If packet-length is not given, the default packet length is 64 bytes. Specifying a longer packet length in the command line can show:

- if a router or host has a problem fragmenting or reassembling transferred packets.
- a more complete indication of the link status.

repeat # The number of times to repeat the **`ping`** test. See **Caution** above before using.

ping field descriptions

Field	Description
End-pt IP or End-pt Node-name	The destination of the **`ping`** command.
Port	The source's slot or port.
Port Type	The source port's maintenance object name.
Result	PASS, FAIL, or ABORT
Time (ms)	The round-trip time (in milliseconds) of the ping.
Error Code	Identifies problems associated with the circuitry in the data path for a peer-to-peer IP layer connection. For the meaning of the error code and troubleshooting procedures, see the Port Type's maintenance object description in the *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*. The MO description indicates the type of **`ping`** test used and the meaning of that ping test's error codes.

Error messages

Message	Description
www.xxx.yyy.zzz IP address not assigned	The system cannot find the IP address.

Table continues…

Message	Description
IP address not reachable from this board	The IP address is not in the route table of the specified board.
Local IP address not supported	The C-LAN board does not support ping of a local PPP IP address.
More than one route exists, specify board	The IP address is not in the route table, and more than one C-LAN circuit pack has a default route.
“xxxx” Invalid IP address	Invalid IP address parameter. Must be in www.xxx.yyy.zzz format.
“CCcss” is an invalid identifier; please press HELP	Invalid board location (when using board).
Board not inserted	Valid board location, but there is no board in that slot.
Error encountered, could not complete request	An internal error, the port through which the IP address is reached could not be found.
Invalid range	The packet size is greater than 1500 or less than 64 bytes in length, or there are invalid or unrecognized parameters.
WARNING Default packet length of 64 bytes used for TN799DP	The default packet length of 64 bytes is used for a TN799DP board.

Example

```
ping  ip-address 192.68.3.26
ping ip-address 2001:0db8:3333:4444:5555:6666:7777:8888
ping ip-address 192.68.3.26 board 1C05
ping ip-address 168.24.3.66packet-length 1500
ping node-name gert_clan1source S00015
```

pkt

clear pkt

Use **clear pkt** to resolve packet bus problems and send a forced packet bus **clear stimuli** over the packet bus.

Syntax

```
clear pkt   port-network  location
```

port-network *location* Physical position of the packet bus (1–3).

Example

```
clear pkt  port-network 1
```

test pkt

Use **test pkt** to run a series of tests on the packet bus of the specified PN or PPN.

Warning:

Since clear long clears every counter if the test passes, it is possible for firmware counters to be cleared even though a problem exists. In some cases, customer service might degrade since calls may be routed over defective equipment.

Syntax

```
test pkt port-network  nn [ short  |  long ] [ repeat  #  |  clear ][ schedule ]
```

port-network *nn*	The packet bus to be tested: *nn (1)*.
short	Execute a series of nondestructive diagnostic tests.
long	Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
repeat #	Number of times to repeat the test, between 1 and 100.
clear	Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.
schedule	Specify a time to run the command.

Example

```
test pkt port-network 1 1
test pkt port-network 1 sh r 2
test pkt port-network 1 l r 25
test pkt port-network 1
test pkt port-network 1 c
```

pms-down

list pms-down

Use **list pms-down** to see every event that has meaning to the Property Management System (PMS) that has occurred while the link between the switch and the PMS was down. For example, room status codes entered by hotel housekeeping staff during a PMS outage is displayed in this report.

Syntax

```
list pms-down [ start-time ] [ stop-time ]
```

start-time The starting time in 24-hour notation from which events are to be listed.

stop-time The time in 24-hour notation up to which events are to be listed.

list pms-down field descriptions

Field	Description
Extension	The extension associated with the reported event.
Event	The PMS event that was reported to the switch, but which could not be sent to the PMS.
Reason	The reason that the event could not be reported by the switch to the PMS.
Time	The time at which the event was reported.

pms-link

busyout pms-link

Use **busyout pms-link** to place every maintenance object associated with a property management system link in the maintenance busy state. No periodic or scheduled maintenance is performed on the busied out maintenance objects until they are released. When the object is maintenance busy the object is deactivated (no call processing activity may include the busied object) and the link is dropped. Warning alarms (error type 18) are generated on each busied out maintenance object, so that the Initialization and Administration System (INADS) can determine the state of the objects. Use **release pms** link to reactivate the busied out objects on the link.

These links provide asynchronous data connections from switches to peripherals, and they are composed of the following:

- Far-end data module
- Simulated data channel
- Manager that initiates and maintains the link
- Controller/protocol that services the link

For information about what a property management system (PMS) is and what it does, see **status pms-link**. See **status link** for more details on links.

Note:

Specific component maintenance performed on a link sometimes conflicts with link maintenance, because busied-out objects create link setup failure. Frequent link re-setup attempts may delay component recovery. For best results, busyout the link to disable attempted link re-setup.

Syntax

```
busyout pms-link
```

release pms-link

Use **release pms-link** to reactivate the busied out maintenance objects on the property management system (PMS) link. The **busyout pms-link** command places all maintenance objects associated with a PMS link in the maintenance busy state. Once released, periodic and scheduled maintenance can be performed on the maintenance objects.

See Busyout and Release Commands. See **status link** for more details on links.

Use **release pms-link** to deactivate MOs that are associated with a property management system link. These links provide asynchronous data connections from switches to peripherals; they are composed of a

- Far end data module
- Simulated data channel on a NETCON board
- Manager that initiates and maintains the link
- Controller/protocol that services the link

Note:

Specific component maintenance performed on a link sometimes conflicts with link maintenance, because busied-out objects create link setup failure. Frequent link re-setup attempts may delay component recovery. For best results, busyout the link to disable attempted link re-setup.

Syntax

```
release pms-link
```

status pms-link

Use **status pms-link** to see the status of the property management system interface link.

Status of the property management link will be up, whether or not a data base swap is taking place between the switch and PMS. If the link is down, the number of attempts made to set up the link is displayed. A property management system (PMS) is a stand alone computer system that can be integrated with the switch to enhance the service capability for a hotel/motel.

For general information on PMS links, see **busyout pms-link**. See **status link** for more details on links.

Syntax

```
status pms-link
```

status pms-link field descriptions

Field	Description
Physical Link State	up, down, extension not administered. The PMS link is listed as administered only if an extension is given in the System Hospitality screen.
Protocol State	up, down The state of the C-LAN protocol. Blank if not administered.
Number of Retries	Number of times the switch has tried to set up the link. Displayed when the link is down.
Maintenance Busy	y, n If y, maintenance testing is being performed on the link.

test pms-link

Use **test pms-link** to verify that the link to the Property Management System (PMS) is administered and performs a series of tests on the link.

See **status pms-link** for information about the PMS and interpreting its status. See **busyout pms-link** for information on PMS links. See **status link** for more details on links.

Syntax

```
test pms-link [ short  |  long ] [ repeat #  |  clear ][ schedule ]
```

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test, between 1 and 100.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

schedule Specify a time to run the command.

Note:

Specific component maintenance performed on a link sometimes conflicts with link maintenance, because busied-out objects create link setup failure. Frequent link re-setup

attempts may delay component recovery. For best results, busyout the link to disable attempted link re-setup.

pnc

set pnc

On critical-reliability systems (duplicated PNC), **set pnc** lock locks the active port network connectivity in the active state. PNC interchanges are prevented, and the active PNC remains active regardless of its state of health. Duplicate call setup takes place, though the standby is not available for service. This condition can also be initiated with **reset pnc interchange override-and-lock**. Use the Software Locked field on the **status pnc** screen to see if the PNC is locked. The Interchange Disabled field refers to the antithrashing mechanism.

set pnc unlock releases the lock and enables subsequent interchanges to take place. If the health of the active PNC has degraded to worse than that of the standby pnc, unlocking the active port network connectivity can cause an immediate PNC interchange This condition can be foreseen by use of **status pnc**.

System restarts remove a PNC lock.

Caution:

If the active PNC experiences problems while in the locked state, service disruptions may occur that would ordinarily be prevented by PNC interchange.

Syntax

```
set pnc  lock| unlock
```

lock PNC interchanges are prevented, and the active port network connectivity is locked online.

unlock Releases the PNC lock.

status pnc

Use **status pnc** to see a summary of conditions on the active and standby Port Network Connectivities (PNC). If the PNC is not duplicated, the B-PNC column and other duplication-related fields are blank.

Syntax

```
status pnc
```

status pnc field descriptions

Field	Description
Duplicated	Whether or not the system has a duplicated PNC (critical-reliability option).
Software Locked	On a system with duplicated PNC, whether the PNCs are locked by means of the **set pnc lock** or **reset pnc override-and-lock**. When this field is y, spontaneous or demand PNC interchanges are not possible. To enable interchanges, use **set pnc unlock**.
Standby busied	On a system with duplicated PNC, whether or not the standby PNC is busied out with **busy pnc**. Interchanges are prevented when the standby is busied out.
Direct Connect	Whether the system uses direct-connect connectivity or a center stage switch.
Standby Refreshed	On a duplicated system, this field indicates whether the standby PNC has completed a global refresh of duplicated call setup after being released from a busyout, or after a system reset. This field does not indicate if a partial unrefresh has taken place in response to a problem on the standby. Only a functional state of health on the standby (all zeros in the **State of Health** vector) guarantees that the standby's call setup matches completely that of the active.
Interchange Disabled	This field is y when the anti-thrashing mechanism is in effect, preventing PNC interchanges. This is the case for 5 minutes after a spontaneous PNC interchange, and for 30 seconds after a demand interchange. The **reset pnc interchange override-and-lock** command overrides antithrashing. This field does not indicate whether a PNC interchange is currently prevented by a software lock, by insufficient state of health of the standby, or by busyout of the standby.
Mode	This field displays active or standby, depending on whether or not that PNC controls active call processing.
State of Health	On a system with duplicated PNC, the state of health of each PNC. For the standby PNC, service effects mentioned below are those that would occur if that PNC were to become active via an interchange. • **Functional** — the indicated PNC has no service disrupting alarms against it. The state-of-health vector is all zeros, and call setup on the standby PNC matches that of the active. • **Partially functional** — the health of the PNC is less than perfect. The source and severity of the problem is indicated by the state-of-health vector (Inter-PN and Inter-SN Indexes). Whenever the standby's state of health is partially functional, duplicated call setup on the standby probably does not match that on the active. • **Not functional** — Expansion Archangel Links to all PNs are down on this PNC. No service is possible to any PNs via this PC.

Table continues…

Field	Description
Inter PN Index, Inter SN Index	The Inter-PN and Inter-SN Indexes screen the state-of-health vector, which is used to track and compare the states of health of both PNCs. The fields making up the indexes are 2-digit numbers separated by periods (.), with each field representing a different class of faults. The fault class fields are arranged in order of decreasing importance from left to right. In other words, each field in the index supersedes the following fields in determining which PNC is healthiest. The Inter-PN Index contains six fields (*aa.bb.cc.dd.ee.ff*), and the Inter-SN Index has two (*gg.hh*). The Inter-PN Index reports faults in connectivity between port networks and supersedes the Inter-SN Index, which reports faults in connectivity between switch nodes. (The Inter-SN Index is only meaningful for systems with a center stage switch having 2 switch nodes, each of which is duplicated). The meaning of each fault class field is given in Fault Class Field Descriptions table. A zero entry indicates that there are no such faults reported. Higher numbers indicate increasing number of faults. All zeros indicates a perfect state of health. Unless the PNCs are locked, the active PNC's state of health should always be equal to or greater than the standby's. (Otherwise, the system would perform a spontaneous interchange.) After a PNC-related alarm is cleared, the system performs a partial refresh of the standby PNC. The corresponding fault class field is not updated to reflect the improved state of health until the refresh is done. The state-of-health indexes will not agree with the current alarm status during this period.
Major Alarms, Minor Alarms, Warning Alarms	The number of major, minor, or warning alarms logged against DS1C-BD, SNI-BD, SNC-BD, EXP-INTF, FIBER-LK, DS1C-FAC, SNC-LINK, SN-CONF, SNC-REF, SYNCH, and SNI-PEER on the indicated PNC.
SN Locations	The locations of all switch nodes comprising the indicated PNC.

Fault Class Field Descriptions

Position	Fault Class	Priority	Description	MOs
Inter PN Index Fields (*aa.bb.cc.dd.ee.ff*)				
aa	FC_EAL	1	Number of PNs with EALs down	EXP-PN
bb	FC_INL	2	Number of PNs with LINL, RINL, or EI-SNI neighbor link faults	EXP-PN SN-CONF
cc	FC_BFDL	3	Number of PNs with Bearer Fault Detection Link (BFDL) faults	EXP-INTF SYS-LINK
dd	FC_HW	4	Number of PNs affected by hardware faults in a link having an EI as an endpoint (Endpoints can be determined with **`list fiber-link`**.)	EXP-INTF SN-CONF FIBER-LK

Table continues…

Position	Fault Class	Priority	Description	MOs
				SNI-BD DS1C-BD
ee	FC_PER	5	Number of PNs affected by SNI peer link faults for SNIs connected to EIs	SNI-PEER
ff	FC_DS1	6	Number of PNs affected by DS1C facility faults	DS1FAC
Inter SN Index Fields (*gg.hh*)				
gg	FC_SNIL	7	Number of inter-switch-node fibers affected by peer or neighbor link faults	SNI-PEER
hh	FC_SNIHW	8	Number of inter-switch-node fibers affected by hardware faults	SN-CONF SNI-BD FIBER-LK

pnc interchange

reset pnc interchange

Use **reset pnc interchange** to execute a PNC interchange on a critical-reliability system (duplicated PNC). The standby PNC becomes active and assumes control of active call processing, and the active goes to standby. If the standby PNC's health is equal to or greater than the active PNC's, no service disruption takes place; all stable calls and links are preserved. Some unstable calls may drop.

Note:

reset pnc interchange does not work like other reset commands. Instead of resetting or initializing hardware, a PNC interchange is executed. Before entering reset pnc interchange, use status pnc to check the states of health of the two PNCs.

Both demand and spontaneous PNC interchanges cannot take place when:

- The standby PNC is busied out.
- The PNCs are locked by means of the **set pnc lock** or **reset pnc interchange override-and-lock** commands.
- For 5 minutes after a spontaneous PNC interchange, or for 30 seconds after a demand interchange, an anti-thrashing mechanism prevents subsequent interchanges unless the override-and-lock option is used.
- When the standby PNC's state of health is lower than the active PNC's, the command aborts unless the override-and-lock option is used.

- If the standby PNC has not completed a global refresh since it was last initialized or released, the reset aborts unless the override-and-lock option is used.

Note the following caution regarding the use of the override-and-lock option.

See **status pnc** for details of how to obtain and interpret the states of health and other current information about the PNCs. For a more complete explanation of PNC duplication and interchanges, see PNC-DUP (PNC Duplication) of the *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*.

Syntax

```
reset pnc interchange  override-and-lock
```

override-and-lock	Override the anti-thrashing mechanism. Subsequent PNC interchanges are prevented, regardless of changes in the states health of the PNCs. Double call setup still takes place; each call is set up on both PNCs. To unlock the PNCs, use **set pnc unlock**.

Caution:

This option forces execution of the interchange regardless of the standby's state of health, possibly disrupting service.

If **reset pnc interchange** is unsuccessful due to the standby PNC's state of health (operation of anti-thrashing), the following message is displayed:

```
Interchange of pnc failed;
try again using the "override-and-lock" identifier
```

If **reset pnc interchange** is unsuccessful due to a busyout of the standby PNC, the following message is displayed:

```
Must release port network connectivity first
```

port

busyout port

Use **busyout port** to busyout a specified port on a circuit pack.

Syntax

```
busyout port   location
```

location	port address (PCSS) marked port: PPSSpp

Busyout port location on a specific SIP B-channel:

- drops any active call that exists on the B-channel
- reduces the trunk group's capacity by one
- the physical piece of hardware is removed from service

Example

```
busyout port 01c1101
busyout port 02c1501
```

clear port

Use **clear port** to remove marks from ports and free the ports for service. **clear port** works with **mark port**.

Syntax

```
clear port location
```

location	Port location: PCSSpp.

Example

```
clear port  01c1102
```

display port

Use **display port** to see a port's equipment type and identification number. The display ports command displays the IPv4 or IPv6 Ethernet link number for C-LAN boards.

Syntax

```
display port  location  [ schedule ]
```

location	Address of the port.
schedule	Specify a time to run the command.

Example

```
display port 1a0502
display port 01a05002
```

display port field descriptions

Field	Description
Port	Port address location
Equipment Type	Type of hardware that is physically connected to the specified port, or TTI port for a telephone in a TTI state.

Table continues…

Field	Description
	Softphone Restore Port — soft phone registration originated from this port. No new extensions can be assigned to this port location. Use **list registered-ip-stations** for more information on the IP soft phone extension assigned to this port.
Identification	Depending on the equipment type, identifies: • extension • trunk group number and member number • modem pool group number • IP address of an IP telephone that is in TTI state This field displays the IPv4 or IPv6 Ethernet link number for C-LAN boards.

mark port

Use **mark port** to make a port unusable by normal call processing. The port can be tested but calls are not attempted through the port. A marked port is saved as part of translation. Use **clear port** to restore the port to service.

Syntax

```
mark port location
```

location Location of the port to be marked.

Example

```
mark port 1c0208
mark port 2a1001
```

release port

Use **release port** to activate specified ports on circuit packs.

For more information see Busyout and Release Commands.

Syntax

```
release port location
```

location Physical location of the port, PCSS.

Release port location on a specific SIP B-channel:

- increases the trunk group's capacity by one
- the physical piece of hardware is added to service.

test port

Use **test port** to perform hardware diagnostic tests on an individual port circuit. In most cases, tests are performed on hardware connected to the port.

Syntax

```
test port location [ long | short ] [ repeat n  |  clear ]
```

location	Location of the port, PCSSpp.
long	Run the long test sequence.
short	Run the short test sequence.
repeat #	(Optional) The number of times to repeat the command. The default is 1.
clear	Repeats the test sequence until any active alarms against the maintenance object are cleared by the passing of tests, or until any test in the sequence fails.

Example

```
test port 01c1101  l
test port 02e1502 sh r 2
test port 02d1201 r 4
test port 01c1101 c
```

Warning:

Because **test port** location clear long clears all counters if tests pass, firmware counters may be cleared even when a problem exists. In some cases customer service might degrade because calls may be routed over defective equipment.

port-network

reset port-network

Use **reset port-network** to reset a specified port network to a specified level. This does not cause an interchange on a system with duplicated PNC. A reset will not work on a port network whose fiber link to the PN or CSS is down.

Caution:

A reset of level 2 is destructive, causing all calls and application links on the specified PN to drop. PN resets are described in 'EXP-PN (Expansion Port Network)' in *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*.

Syntax

```
reset port-network PN# level 1 | 2
```

PN# Port network number. Use **list cabinet** to find the PN number(s) associated with a given cabinet.

level *1* Use reset level 1 (warm restart) to restart a PN that is still fully or partially in service. All stable calls are preserved, and full service is restored within 35 seconds.

level *2* Use reset level 2 (COLD restart) to reset, remove, and reinsert all PN circuit packs, to recover a PN that has been taken out of service. Level 2 restarts should take less than 2 minutes. All calls and application links with an endpoint in the PN are dropped.

If two level 2 resets within an hour fail to return the PN to service, PN Emergency Transfer is invoked. PN Emergency Transfer is already in effect if the link to the PN has been down for more than 1 minute.

Example

```
reset port-network 10 level 2
```

status port-network

Use **status port-network** to see information about the status of a specified port network. The fields on the screen vary depending on the PNC configuration on the system.

In port networks where PKT-INTs are moved to the IPSIs, status port-network shows the location and state of the links, whether active or failed, and the total alarms, faults, and open bus links.

Syntax

```
status port-network
```

status port-network field descriptions

Field	Description
PN	The Port Network number associated with the Port Network for which status is being displayed.
Major Alarms	The number of major alarms logged against the Port Network that is being displayed.
Minor Alarms	The number of minor alarms logged against the Port Network that is being displayed.
Warning Alarms	The number of warning alarms logged against the Port Network that is being displayed.
Carrier Locs	The cabinet and carrier locations of each carrier in the Port Network.

Table continues…

Field	Description
PN Control Active/Standby	Active and standby (if control network is duplicated) control network status status for the specified port network. • **up** — the link between the TN2312 IPSI circuit pack and the server is up • **down** — the link between the TN2312 IPSI circuit pack and the server is down For direct connect, CSS, or fiber connected port networks, the PNC status of a port network is determined by the availability of the EAL (Expansion Archangel Link) and the INL (Indirect Neighbor Link) to the port network. • **up** — the EAL and INL are both available • **down** — the EAL and INL are both unavailable • **near-end** — the EAL is available but the INL is unavailable • **far-end** — the INL is available but the EAL is unavailable When the far-end EAL is unavailable, Tone-Clock, TDM-bus, and packet-bus information are blank. • **aa** — there is a problem with the archangel. The control is up, but the archangel is not functioning and is not available.
FIBER-LINK	This field displays the fiber-link number associated with all fiber links having an Expansion Interface circuit pack endpoint residing in the specified Port Network. The fiber connectivity side will also be displayed (that is, A-PNC or B-PNC).
Endpoints	The physical position of each Expansion Interface board that is an endpoint for a fiber link in the specified Port Network. A high-reliability system will display only one Expansion Interface pair, while a critical-reliability system will display two Expansion Interface pairs separated by a hyphen (-). If blanks are displayed, it means the endpoints could not be retrieved by software.
Mode	The mode is the current role of the link. A mode of **active** means the link is providing normal circuit and control functions for the Port Network. A mode of **standby** means the link is part of a duplicated system and is ready to perform its functions but is not active. If blanks are displayed it means that PNC is not duplicated, or the mode could not be retrieved from software.
TDM Bus	The TDM bus identifier associated with the Port Network is displayed. The TDM bus (a or b) specifies which half of the TDM bus is being displayed. When Control Links are down, this field is blank.
Service State	The operational state of the TDM bus. A TDM bus service state of “in” means the bus is in normal operation. A TDM bus service state of “out” means the bus has failed certain maintenance tests and has been taken out of service, or the maintenance object has been demand busied out.

Table continues…

Field	Description
	When Control Links are down, this field is blank.
Control Channel	**y/n** Shows whether the TDM bus has the control channel on it. Only one TDM bus of a TDM bus pair on each Port Network can have the control channel on it at a given time. Blank if the system does not contain a PN, and when Control Links are down.
Dedicated Tones	**y/n** Shows whether the TDM bus has the system tones on it. Only one TDM bus of a TDM bus pair can have system tones on it at a given time. Blank if the system does not contain a PN, and when Control Links are down.
TONE/CLOCK	The location of the IPSI or Tone-Clock circuit pack, containing the Tone-Clock circuit in the specified Port Network. The location is represented using the cabinet and carrier where the Tone-Clock resides (example, 1a, 1b, 2a, 2b, etc.). Blank — Control Links are down.
Service State	The operational state of the Tone-Clock circuit. **in** means the Tone-Clock has been installed and is in normal operation. **out** means that the Tone-Clock is out of service and has failed certain maintenance tests. Blank — Control Links are down.
System Clock	Shows which IPSI or Tone-Clock circuit pack supplies the system clock for that port network by displaying the mode of the Tone-Clock. • **active** — the Tone-Clock supplies the system clock. Only one Tone-Clock in each Port Network can be active at any given time. • **standby** — the Tone-Clock is part of a duplicated clock system and is ready to supply the system clock, but is not currently active • **down** — the Tone-Clock is not operational • **blank** — control links are down.
System Tones	Shows which IPSI or Tone-Clock circuit pack supplies the system tones for that port network by displaying the mode of the Tone-Clock. • **active** means that the Tone-Clock supplies the system tones. Only one Tone-Clock in each Port Network can be active at any given time. • **standby** means the Tone-Clock is part of a duplicated clock system and is ready to supply system tones, but is not currently active

Table continues…

Field	Description
	• **down** means the Tone-Clock is not operational. • **blank** when control links are down.
PKT	Packet Bus identifier, the same as the Port Network number.
Service State	This field represents the operational state of the packet bus. • A service state of **in** means the packet bus has been installed and is in normal operation. • A service state of **out** means either that the: - Packet bus is out of service and has failed certain maintenance tests - Maintenance object has been demand busied out • A service state of **reconfig** means that the Maintenance/Test circuit pack has swapped one or more signal leads because of lead faults detected during testing (high- and critical-reliability systems). • A service state of **open lds** means the Maintenance/Test circuit pack query was run, and open bus leads were found. • A **blank** in this field means the system does not have the Packet Bus feature optioned. When Control Links are down, service state information is unavailable.
Major Alarms	Whether major alarms are logged against the packet bus that is being displayed **y/n**. When Control Links are down, this field is blank.
Minor Alarms	Whether minor alarms are logged against the packet bus that is being displayed **y/n**. When Control Links are down, this field is blank.
Bus Faults	This field indicates the number of faulty bus leads, where a fault is defined as either shorted to another lead or stuck at some value. This field may take on any integer value between 0 and 24. The field contains a blank if the Maintenance/Test circuit pack is not present or has been taken out of service. When Control Links are down, this field is blank.
Open Bus Leads	This field indicates the number of bus leads that have an open circuit between the Maintenance/Test circuit pack and bus terminator. This information is determined by testing performed on the bus leads; bus leads test open as a result of physical damage to the backplane or the backplane's connectors, or because a bus terminator is missing. This field may contain integer values between 0 and 24. This field contains a blank if the Maintenance/Test circuit pack is not present or has been taken out of service. When Control Links are down, this field is blank.

power-shutdown

get power-shutdown

Use **get power-shutdown** to see the cause of the last shutdown of a power supply in an individual gateway or a stack. Use **get power-shutdown** on carriers or a stack (cabinet) equipped with a TN2312BP IPSI or later IPSI circuit pack. The carrier is the location of a G650 carrier within a G650 stack.

Use **display error** to see the time of the last shutdown.

Note:

When you reset a 655A power supply by unplugging it, keep it unplugged for 30 seconds to discharge it. Otherwise, it retains the information it stored before it was unplugged.

Syntax

```
get power-shutdown UUc
```

UUc The cabinet/carrier location of the IPSI board to be released.

get power-shutdown field descriptions

Field	Description
Slot	Power supply cabinet/carrier/slot
Cause	Cause of last shutdown

pri-endpoint

busyout pri-endpoint

Use **busyout pri-endpoint** to busyout all PRI endpoint ports (B-channels) associated with the specified PRI endpoint.

Syntax

```
busyout pri-endpoint extension #
```

extension # PRI endpoint extension number.

busyout pri-endpoint feature interactions

Active calls on busied out PRI endpoints are dropped.

Call attempts from far-end PRI terminal adapters are denied with a cause value of 17.

release pri-endpoint

Use **release pri-endpoint** to remove PRI endpoint ports (B-channels) associated with specified PRI endpoint from maintenance busy states. Periodic and scheduled tests resume on released ports. The switch attempts to negotiate with the far-end PRI terminal adapter activating PRI endpoint port (B-channel). Maintenance does background initialization testing on released ports.

Syntax

```
release pri-endpoint extension #
```

extension #	PRI endpoint extension number.

status pri-endpoint

Use **status pri-endpoint** to display the internal software state information for diagnosis and to help locate facilities with which a PRI endpoint is communicating. Status information for each of the B-channels which make up the PRI endpoint is displayed in addition to some overall PRI endpoint information.

Syntax

```
status pri-endpoint extension #
```

extension #	PRI endpoint extension number.

Note:

A PRI endpoint can initiate and receive a call on any one or more of the B-channels making up the PRI endpoint.

Example

```
status pri-endpoint 25012
status pri-endpoint 77868
```

status pri-endpoint field descriptions

Field	Description
Extension	PRI endpoint extension.
Width	Administered number of B-channels associated with the specified PRI endpoint.
Signaling Group ID	ID number of the signaling group that handles the signaling for the ports in the specified PRI endpoint.

Table continues…

Field	Description
Originating Auto Restoration	Administered option for the auto restore feature (restores calls originated from this PRI endpoint in the case of network failure): • **y** — restoration option enabled • **n** — restoration option disabled
B-Channels Active	The number of B-channels active on a call
B-Channels Idle	The number of B-channels in the in-service/idle state
Port	Port locations (cabinet-carrier-slot-circuit) for each of the B-channels making up the PRI endpoint.
Service State	Service state of the B-channels: • in-service/active • in-service/idle • out-of-service-NE • out-of-service-FE • maint-NE/active • maint-FE/active • maint-NE/idle • maint-FE/idle NE (Near End) and FE (Far End) refer to which **end** of the B-channel has placed the facility in the current state. NE refers to the switch and FE refers to the PRI terminal adapter (or any device that terminates the D-channel signaling on the facility).
Test In Progress	Whether or not there is any current maintenance testing on the port.
Connected Port	Connected port location (cabinet-carrier-slot-circuit) for each of the B-channels active on a call.

test pri-endpoint

Use **test pri-endpoint** to perform hardware diagnostic tests on all port circuits (B-channels) that are associated with the specified PRI endpoint.

Syntax

```
test pri-endpoint extension # [ short | long ][ repeat  # | clear ]
```

extension # PRI endpoint extension to be tested (must conform to dial-plan).

short Run the short test sequence.

long Run the long test sequence.

repeat #	(Optional) The number of times to repeat the command. The default is 1.
clear	Repeat the test sequence until any active alarms against the maintenance object are cleared by the passing of tests, or until any test in the sequence fails.

Example

```
test pri-endpoint 25012
test pri-endpoint 45002 sh
test pri-endpoint 45892 l
test pri-endpoint 24389 sh r 2
test pri-endpoint 34899 l r 6
```

processor-ip-interface

busyout processor-ip-interface

Use **busyout processor-ip-interface** to busyout the processor ethernet interface link. **busyout processor-ip-interface** brings down the processor channel applications, ip-services, and IP calls that were active on the link.

Syntax

```
busyout processor-ip-interface
```

release processor-ip-interface

Use **release processor-ip-interface** to release the processor ethernet interface link and to bring up the processor channel applications, ip-services, and IP calls that were administered active prior to busying out the link.

Syntax

```
release processor-ip-interface
```

For more information, see Busyout and Release Commands.

status processor-ip-interface

Use **status processor-ip-interface** to see the status of the processor-ip-interface.

Syntax

```
status processor-ip-interface
```

profile-base

display profile-base

Use **display profile-base** to see the Linux Group number that corresponds to Communication Manager user profile 0.

The screen name is User Profile Base.

Syntax

```
display profile-base
```

display profile-base field descriptions

Field	Description
Profile Base	Linux Group number that corresponds to Communication Manager user profile 0. Profile Base default number is 10000.

psa

status psa

Use **status tti** to see the TTI/PSA status screen and check if the TTI background maintenance task is active. If the TTI background maintenance task is active, the screen shows whether TTI ports are being generated or removed, the number of TTI-supported boards that have been processed, and the number of TTI-supported boards that have not yet been processed. The screen also shows the elapsed time since the background maintenance task started.

To activate the TTI background maintenance task, enter y in the TTI field on the Feature-Related System-Parameters screen.

Use **status psa** to also see the TTI/PSA status screen. It shows that the status of PSA is dependent on the state of TTI.

Syntax

```
status psa
```

status psa field descriptions

Field	Description
TTI Background Task State	• **generating TTI ports** • **removing TTI ports**

Table continues…

Field	Description
	• **suspended** • **not active** • **completed – all ports translated** — The last background maintenance task completed normally. • **completed – some ports not translated** — The last background maintenance task stopped when resources were exhausted, and some ports were not translated.
TTI State	**off** — TTI is disabled voice, data shows the type of TTI ports that are being generated or removed.
# of Boards Completed	Number of TTI-supported circuit packs that were processed by the background maintenance task. The ports on a **completed** circuit pack: • if unadministered, were translated as TTI ports • if administered, the administration was removed
# of Boards Left to Process	The number of TTI-supported circuit packs that were not processed by the background maintenance task.
Percent Complete	Ratio of the of number of circuit packs completed to the total number of circuit packs.
Elapsed Time Since Task Started	Elapsed time in *hours:minutes:seconds* since the TTI background task was started. This field is blank if the task is not active. If the task is completed or suspended, this field shows the elapsed time up to when the job finished or was suspended.

public-unknown-numbering

change public-unknown-numbering

Use **change public-unknown-numbering** to administer the desired digits for name and number display on display-equipped stations in an ISDN network.

Syntax

```
change public-unknown-numbering  n  [ ext-digits  x ][ trunk-group  # ]
```

n Number of digits (extension length, Ex-Len) in the extension being administered.

Enter 0 for attendant.

Comments on this document? infodev@avaya.com

ext-digits *x* First extension on the screen.

trunk-group # The trunk-group option displays valid results only when used in conjunction with the ext-digits option. Otherwise, an error message is returned.

See *Administering Avaya Aura®Communication Manager (03–300509)* for a screen example and field descriptions, and for more information on ISDN Call Identification Display and Numbering-Public/Unknown.

Example

```
change public-unknown-numbering 5change public-unknown-numbering 5 ext-digits 10010
```

display public-unknown-numbering

Use **display public-unknown-numbering** to see the administration for name and number display on display-equipped stations in an ISDN network.

Syntax

```
display public-unknown-numbering n [ ext-digits x ]
```

n Number of digits (extension length, Ex -Len) in the extension being administered.

Enter 0 for attendant.

ext-digits *x* First extension on the screen.

Example

```
display public-unknown-numbering 5
display public-unknown-numbering 5 ext-digits 10010
```

list public-unknown-numbering

Use **list public-unknown-numbering** to list all entries in the public-unknown-numbering table, used to specify desired digits for name and number display on display-equipped stations in an ISDN network.

Syntax

```
list public-unknown-numbering start n [ ext x | count n ]
```

start *n* Starting point for the extension digits you want to see.

ext *x* The first extension on the screen.

count *n* Number of output lines.

list public-unknown-numbering field descriptions

Field	Description
CPN Prefix	The number that is added to the beginning of the extension to form a Calling or Connected Number. • **blank** — the extension is sent unchanged. Use in countries where the public network is able to insert the appropriate CPN Prefix to form an external DID number. • If the CPN Prefix length matches the Total CPN Len, the extension number is not used to formulate the PN number. • If the CPN Prefix length plus the extension length exceeds the Total CPN Len, excess leading digits of the extension are deleted when formulating the CPN. • If the CPN Prefix length plus the extension length is less than the Total CPN Len, the entry is not permitted • If the Total CPN Len is 0, no calling party number information is provided to the called party and no connected party number information is provided to the calling party.
Ext Code	Can be up to 7 digits, but cannot be greater than the Ext Len field. • attd — attendant • 0 — Ext Len field must be 1 and the DDD number must be 10 digits • 0 to 9 or blank **Example:** When Ext Len is 4, Ext Code of 12 represents all extensions of the screen 12xx, excluding any explicitly listed longer codes. If code 123 is also listed, the Ext Code 12 represents all extensions of the screen 12xx except extensions of the screen 123x.
Ext Len	Number of digits for the extension, as entered on the command line (**`list public-unknown-numbering n`**).
Total CPN Len	Total number of digits to send. **0** — no calling party number information is provided to the called party and no connected party number information is provided to the calling party.
Trk Grp(s)	Number of the ISDN trunk group carrying the call, or the range of trunk groups that use the same CPN Prefix. **blank** — IEs are not dependent on which trunk group carries the call.

registered-ip-stations

list registered-ip-stations

Use **list registered-ip-stations** to see specific information about registered ip stations. Sort registered ip-station information by:

- gatekeeper address
- network region
- product ID
- station type
- TCP socket registration

Syntax

```
list registered-ip-stations [all] [v4] [v6] [ext x] [type x] [id x] [release x] [region x] [port x][gatekeeper x] [tcp y | n] [authenticated x] [count n]
```

all	Displays the v4 and v6 registered IP stations.
v4	Displays the v4 registered IP stations.
v6	Displays the v6 registered IP stations.
ext *x*	Extension number of the registered stations.
type *x*	Administered set type (*xxxxxx*).
id *x*	Product type (*x.yyy*) of the registered extension.
release *x*	Release number of the registered stations.
region *x*	Network region of the registered stations.
port *x*	Port number of the registered stations.
gatekeeper *x*	C-LAN's or processor's IP address (*xxx.xxx.xxx.xxx*).
tcp *y* | *n*	TCP signaling socket registration established.
authenticated *x*	Displays the V4 and V6 registered IP stations.
count *n*	Number of stations to list.

list registered-ip-stations field descriptions

Field	Description
For shared-control endpoints (an IP telephone and IP soft phone are in service on the same extension simultaneously), both endpoints register. The records for each endpoint are displayed vertically adjacent to each other.	
Station Ext or Orig Port	**First line:** Station extension number. **Second line:** Port number assigned to the extension that is now under the control of the specified endpoint, for example, a soft phone. For an IP endpoint, this is the circuit-switched port that was assigned to this extension number before the IP endpoint registered to the extension. For a shared-control extension where the Telephone is a DCP set, this is the port of the shared-control's DCP set. If a soft phone is not taking over a DCP set, no second line is displayed.
Set Type	Administered set type for the extension.
Net Rgn	Network region number assigned to the endpoint.
Prod ID	Product ID of the registered endpoint. For example, this can be the product ID of a soft phone that is registered to a hard phone extension, and the release information, provided from the endpoint during registration.
Prod Release	Release number of the endpoint, provided from the endpoint to the gatekeeper during registration.
TCP Skt	**y/n** Indicates whether or not the TCP signaling socket is established for the IP station.
Station IP Address	Location of the registered station, as the C-LAN or processor IP address or port location.
Gatekeeper IP Address	The IP address of the C-LAN, server, or other device that is performing the role of the H.323 gatekeeper for this endpoint.

remote-access

status remote-access

Use **`status remote-access`** to see information about remote access calls.

Syntax

```
status remote-access
```

status remote-access field descriptions

Field	Description
Remote Access Status	Whether the feature is enabled or not
Barrier Code	Remote access barrier code
Date Modified	Remote access modification date
Expiration Date	Barrier code expiration date
No. of Calls	Number of calls from barrier code
Calls Used	Number of times barrier code was used
Status	Enable/disable state of remote access
Date/Time Expired	Date/time barrier code expired
Cause	Reason for the expiration

remote-office

add remote-office

Use **add remote-office** to administer a new remote office on your system.

Syntax

```
add remote-office nn ]
```

nn The number assigned to the remote office.

add remote-office field descriptions

Field	Description
Node Name	Node Name or IP address assigned to the remote office
Network Region	Network Region number assigned to all stations supported on this remote office. This network region may be used to override the default region obtained form the C-LAN used for signaling to and from the stations.
Location	Location number of the remote office
Site Data	Text information specific to your company.

change remote-office

Use **change remote-office** to change the administration of a specific remote office on your system.

Syntax

```
change remote-office nn
```

nn The number assigned to the remote office.

display remote-office

Use **display remote-office** to see the information for a specific remote office administered on your system.

Syntax

```
display remote-office nn[ schedule ]
```

nn The number assigned to the remote office.

schedule Specify a time to run the command.

list remote-office

Use **list remote-office** to list all of the currently administered remote offices on the system. Information includes the remote-office number, node name, network region, location number, and IP address of the remote office.

Syntax

```
list remote-office [ schedule ]
```

schedule Specify a time to run the command.

list remote-office field descriptions

Field	Description
Node Name	Node Name assigned to the remote office
Net Region	Network Region number
Location	Location of the remote office
IP Address	IP Address of the remote office

remove remote-office

Use **remove remote-office** to remove a specific remote office from your system.

Syntax

```
remove remote-office nn
```

nn The number assigned to the remote office.

status remote-office

Use **status remote-office** to see information about a specified remote-office.

Syntax

```
status remote-office nn
```

nn The number assigned to the remote office.

status remote-office field descriptions

Field	Description
Node Name	Node Name assigned to the Remote Office
IP Address	IP Address of the node name assigned to the Remote Office
Network Region	Network Region number assigned to the Remote Office
Location	Location number for the Remote Office
Trunk Signaling Groups	Trunk Signaling Group assigned to the Remote Office
Stations Registered	Extensions of the stations on the Remote Office that are currently registered.

route-table

refresh route-table

Occasionally, tables that are used to route IP messages become corrupted and/or contain stale routes, delaying packet delivery. Use **refresh route-table** to remove learned routes from C-LAN circuit pack route tables, and replace administered routes that have been corrupted.

Syntax

```
refresh route-table [ all | location ]
```

all	Refreshes route tables in all C-LAN circuit packs.
location	Refreshes ip-route tables in a specific C-LAN circuit pack (CCcss).

Description

Occasionally, tables that are used to route IP messages become corrupted and/or contain stale routes, delaying packet delivery. Use **refresh route-table** to remove learned routes from C-LAN circuit pack route tables, and replace administered routes that have been corrupted.

refresh route-table field descriptions

Field	Description
C-LAN Board Location	The physical location of the circuit pack in CCcss format (cabinet, carrier, slot)
Number of Routes Removed	The number of routes that were deleted from the TN799DP (C-LAN) route tables
Number of Routes Added	The number of routes that were added from the TN799DP (C-LAN) route tables

security-violations

monitor security-violations

Use **monitor security-violations** to view information about failed attempts to access the system.

Syntax

```
monitor security-violations [authorization-code | remote-access | station-security-codes]
```

authorization-code	Monitors the number of failed attempts of accessing the system resources due to an invalid authorization code.
remote-access	Monitors the number of failed attempts of dialing into the system using remote access due to an invalid barrier code or authorization code.
station-security-codes	Monitors the number of failed attempts of accessing the system resources due to an invalid station security code.

Description

Use monitor security-violations to see the following information about failed attempts to access the system:

- the time of the violation

- trunk-group number
- member number
- extension

A total of 16 entries are maintained for each type of access. The monitor security-violations report is automatically updated every 30 seconds until the command is canceled by pressing CANCEL. Canceling does not log off the terminal.

Note:

`monitor security-violations` is not available in ASA in the GEDI mode.

monitor security-violations field descriptions

Field	Description
Authorization code violations	
Date	The date of the security violation in the MM/DD format.
Time	The time of the logged security violation in the HH:MM format.
Origin	The source of the call: internal or external.
Auth-Cd	The dialed authorization code.
TG No.	The trunk group involved in the security violation.
Mbr	The trunk-group member number involved in the security violation.
Bar-Cd	The dialed barrier code, if required.
Ext	The extension used to access the system.
CLI/ANI	The calling party number.
Remote access barrier code violations	
Date	The date of the security violation in the MM/DD format.
Time	The time of the logged security violation in the HH:MM format.
TG No.	The trunk group that carried the incoming remote access attempt.
Mbr	The trunk-group member number associated with the trunk from which the remote access attempt terminated.
Ext	The extension used to access the system.
Bar-Cd	The dialed barrier code, if required.
CLI/ANI	The calling party number.
Station security code violations	
Date	The date of the security violation in the MM/DD format.
Time	The time of the logged security violation in the HH:MM format.
TG No.	The trunk group involved in the security violation.
Mbr	The trunk-group member number involved in the security violation.
Port/Ext	The port or extension used to access the system.
FAC	The dialed feature access code.
Dialed digits	The dialed digits.

session

enable session

Use **enable session** to enable a telnet session on the TN2302 and TN2602 media-processor circuit packs.

Syntax

```
enable session
```

enable session field descriptions

Field	Description
Login	3 - 6 alphabetic characters
Password	7 - 11 characters containing at least one letter and one number.
Reenter Password	Reenter the password
Secure	y = enable SFTP n = enable FTP
Time to login	Number of minutes (0 - 255) to be logged in. The login will be dropped after that time.
Board Address	Location of the circuit pack

set-data

list set-data

Use **list set-data** to see telephone information administered from the Site Data and Station screens.

Syntax

```
action object [ schedule ]
```

schedule (Optional) Specify a start time for the command.

list set-data field descriptions

Field	Description
Ext	station extension number, administered on the Station screen

Table continues…

Field	Description
Name	name used in the system directory
Building, Floor, Room	physical location of the station
Cable	identifies the cable that connects the telephone jack to the system
Jack	identifies the jack where the telephone is plugged in
Color	color of telephone
Cord Len	length of the cord attached to the receiver
Speaker	y/n
Headset	y/n
Mounting	desk or wall
Set Type	type of telephone

shell

go shell

Use **go shell** to get SAT access to the server's Linux bash shell.

Syntax

```
go shell
```

Description

1. Type **go shell** at the SAT command prompt and press **ENTER**.

   The screen displays:

   Suppress alarm origination? (y/n) [y]

2. Enter y to suppress alarms if you are logged into a server via an analog modem that is also the server's only alarm-reporting interface.

   This prevents the other server logging an occurrence of SME Event ID #1.

3. Enter your terminal type, or press **ENTER** for the default terminal type.

   The Linux prompt is displayed. It is the login and the server name followed by >.

4. At the Linux prompt, enter a Linux command.

signaling-group

display signaling-group

Use **display signaling-group** to see the properties of a specific signaling group, designated by the qualifier.

Syntax

```
display signaling-group x
```

x number of signaling group to display

Description

Signaling groups are groups of B-Channels for which a given D-Channel (or D-Channel pair) carries the signaling information.

display signaling-group field descriptions

Field	Description
Grp No	The signaling group number
Group Type	The type of signal format (ISDN-PRI, , H.323, SIP)
Max NCA TSCs	Maximum number of Non-Call Associated (NCA) Temporary Signaling Connections (TSCs) - virtual connections established within a D-Channel in the facility so that users can transport non-call control user-user information.
Max CA TSCs	Maximum number of Call Associated (CA) TSCs.
Remote Office	The number of NCA TSCs that are administered.
Trunk Group for NCA TSC	The ISDN-PRI trunk group number whose incoming call-handling table handles incoming NCA-TSCs through this signaling group
Trunk Group for Channel Selection	If more than one trunk group is assigned to this signaling group, this trunk group is the one that can accept incoming calls
TSC Supplementary Service Protocol	This field is displayed when trunk Group Type is ISDN, and for signaling group types , H.323, and ISDN-PRI. a = AT&T Customer Supplementary Services when Country Code is 1A on the DS1 screen. a = Bellcore Supplementary Services when Country Code is 1B on the DS1 screen a = Nortel Proprietary Supplementary Services when Country Code is 1C on the DS1 screen. b = ISO Q SIT

Table continues…

Field	Description
	c = ETSI. Use to support ETSI-ISDN Completion of Calls (Auto Callback) functionality. d = ECMA QSIG e allows DCS with rerouting, when DCS with Rerouting is y, and Used for DCS on the trunk group screen is y. f = Feature Plus g = ANSI.
T303 Timer (sec)	The number of seconds the system waits for a response from the far end before invoking Look Ahead Routing. Displayed when the Group Type field is isdn-pri on the DS1 Circuit Pack screen or h.323 on the Signaling Group screen.
Near-end Node Name	The node name for the C-LAN IP interface on this switch, administered on the Node Names screen and the IP Interfaces screen.
Far-end Node Name	The node name for the far-end C-LAN IP interface used for trunks assigned to this signaling group, administered on the Node Names screen.
Near-end Listen Port	A port number assigned to both near-end and far-end systems for signaling. 1719 is used when LRQ is y.
Far-end Listen Port	The same port number assigned to the near-end listen port.
Far-end Network Region	The network region number that is assigned to the far-end of the trunk group. It is displayed only for H.323 signaling groups. A blank indicates the region of the near-end node
LRQ Required	n when the far-end PBX uses a Communication Manager server y when the far-end PBX uses a server that is not a Communication Manager server, and requires a location request to obtain a signaling address in its signaling protocol
RRQ Required	y when the signaling group serves a remote office (gateway) n when the signaling group serves a gatekeeper
Calls Share IP Signaling Connection	y = inter-Communication Manager server connections n = the local and/or remote PBX uses a non-Avaya server.
Bypass if IP Threshold Exceeded?	y = the system automatically removes from service trunks assigned to this signaling group, when IP transport performance falls below limits administered on the Maintenance-Related System-Parameters screen.
Direct IP-IP Audio Connection	y allows direct audio connections between IP endpoints, and saves on bandwidth resources and improves sound quality of VoIP transmissions.
IP Audio Hairpinning	y allows IP endpoints to be connected through the IP circuit pack on the switch in IP format, without going through the TDM bus.
Interworking Message	Determines what message the switch sends when an incoming ISDN trunk call interworks (is routed over a non-ISDN trunk group).

Table continues…

Field	Description
	PROGress causes the public network to cut through the B-channel and allow the caller to hear tones, such as ringback or busy tone, over the non-ISDN trunk. ALERTing causes the public network in many countries to play ringback tone to the caller. Select this value only if the DS1 is connected to the public network, and it is determined that callers hear silence (rather than ringback or busy tone) when a call incoming over the DS1 interworks to a non-ISDN trunk.

list signaling-group

Use **list signaling-group** to see a list of signaling groups, which are groups of B-Channels for which a given D-Channel (or D-Channel pair) will carry the signaling information.

Syntax

```
list signaling-group count x
```

count x The number of signaling groups to be displayed.

Example

```
list signaling-group count 6
```

list signaling-group field descriptions

Field	Description
Grp No	The signaling group number
Group Type	The type of signal format (ISDN-PRI, H.323)
FAS	Facility Associated Signaling (FAS), in which a D-Channel carries signaling information for only those B-Channels on the same facility as the D-Channel. This is identical to a DS1 interface. If the parameter is “n”, this is referred to as Non-Facility Associated Signaling (NFAS), in which a B-Channel can belong to any signaling group as long as the maximum number of DS1’s for a signaling group is not exceeded.
No. Trunk Brds	The number of trunk boards having members belonging to this signaling group
Primary D-Channel	The D-Channel administered to be the primary channel. If, during the backup procedure, both channels are in the same state, switches at opposite ends of the PRI select the primary D-Channel to be put into service.
Secondary D-Channel	This channel will only display if the signaling group is an NFAS signaling group. This D-Channel is administered to be the secondary D-Channel. If, during the backup procedure, both channels are in the same state, switches at opposite ends of the PRI select the primary D-Channel to be put into service.

Table continues…

Field	Description
Max NCA TSCs	Maximum number of Non-Call Associated (NCA) Temporary Signaling Connections (TSCs) — virtual connections established within a D-Channel in the facility so that users can transport non-call control user-user information.
Max CA TSCs	Maximum number of Call Associated (CA) TSCs.
No. Adm'd NCA TSCs	The number of NCA TSCs that are administered.

set signaling-group

Use **set signaling-group** to set the secondary D-channel in the specified signaling group to be the primary D-channel.

Syntax

```
set signaling-group group#
```

group# The number assigned to the signaling group.

Description

The primary D-channel becomes the secondary D-channel. A signaling group is a collection of B-channels signaled for by a designated single D-channel or set of D-channels over an ISDN-PRI link.

status signaling-group

Use **status signaling-group** to see the service state, type, and port location of the primary and secondary D-channels within an ISDN-PRI signaling group.

Syntax

```
status signaling-group group#
```

group# The administered number associated with each signaling group.

Description

A signaling group is a set of B-channels signaled for by a designated single D-channel, or combination of D-channels over an ISDN-BRI.

status signaling-group field descriptions

Field	Description
Group ID	An administered number that identifies the signaling group.
Type	See the ISDN-SGR (ISDN-PRI Signaling Group) section on the *Maintenance Alarms for Avaya Aura®Communication Manager,*

Table continues…

Field	Description
	Branch Gateways and Servers (03–300430) for more information about group types. • facility associated signaling: Every member is carried on a single DS1-associated facility. Facility-associated signaling groups support only simplex D-channel configurations. • non-facility associated signaling: Members can include trunks on several different associated DS1 facilities. • An explicit identifier specifies members of the DS1 trunk group across its ISDN-PRI link. A single D-channel on one facility provides signaling for every member. With D-channel backup, a second D-channel is assigned to assume control of signaling if the primary D-channel fails.
Group State	in-service: one of the D-channels signaling for the group is in service out-of-service: neither D-channel in the group is in service If there is no D-channel backup and the primary D-channel is out-of-service, the signaling group is in an out-of-service state.
Link	Link transporting the D-channel
Port	Address of the port transporting either the primary or secondary D-channel
Q-SIP Reference Signaling Group	Displayed only when the Group Type field is sip or h.323. If a signaling group is used as a QSIG over SIP signaling group, the Q-SIP Reference Signaling Group field displays the reference signaling group.
Level 3 State	State of the primary or secondary D-channels: • in-service: the D-channel is in the multiple-frame-established state at layer 2 carrying normal call-control signaling at layer 3. • standby: the D-channel is in the multiple-frame-established state at layer 2, and not carrying any layer 3 call-control messages on logical link 0,0. • wait: an attempt has been made by one side of the interface to establish layer 3 peer communications as part of the process of going to the “in-service” state, which is transitional in nature. Only when the ISDN SERVICE message is sent over the interface, and the far end of the interface responds with a SERVICE ACKnowledge message is the D-channel placed in the “in-service” state. • maintenance-busy: the D-channel is not in the multiple-frame-established state at layer 2. This state is entered automatically when an active D-channel is declared failed. A D-channel that has been placed in the “maintenance-busy” state may be placed in the “out-of-service” state without system technician intervention. • manual-out-of-service: system technician intervention has caused the D-channel to be placed in the TEI-assigned state at layer 2.

Table continues…

Field	Description
	System Technician intervention is required to retrieve a D-channel from this state. • out-of-service: the D-channel is in the TEI-assigned state at layer 2, but is periodically requested by layer 3 to attempt to establish the link. • no-link: no link is administered for the D-channel

test signaling-group

Use **test signaling-group** to validate the administration of a signaling group, and run a series of diagnostic tests on it.

Syntax

```
test signaling-group group# [ short | long ] [ repeat repeat# | clear ] [ schedule ]
```

group# The station extension (must conform to dial-plan)

short Run short test sequence. This is the default.

long Run long test sequence.

repeat # (Optional) The number of times to repeat the command. The default is 1.

clear Repeats the test sequence until any active alarms against the maintenance object are cleared by the passing of tests, or until any test in the sequence fails.

schedule (Optional) Specify a start time for the command.

Description

An ISDN-PRI signaling group is a set of B-channels whose signaling messages are carried together on a designated D-channel or set of D-channels. See **status signaling-group** for information on how to access the additional data after running **test signaling-group**.

Example

```
test signaling-group 1
test signaling-group 1 repeat 10
test signaling-group 2 short
test signaling-group 4 long
test signaling-group 4 long clear
```

skill-status

list skill-status

Use **list skill-status** to see administration and status data for skilled hunt groups.

Syntax

```
list skill-status [ starting-number  xx ] [ count num-groups  yy ][ schedule ]
```

starting-number *xx* The starting hunt group number.

count num-groups *yy* The number of hunt groups to be displayed.

schedule Specify a time to run the command.

list skill-status field descriptions

Field	Description
Group No.	The number of the hunt group/skill group being reported
Group Name	Communication Manager name associated with the hunt group/skill group as administered with **change hunt-group** (not the CMS name)
Group Type	Call distribution method for the hunt group/skill group
SLS	Service level supervisor
CSO	Call selection override
OCW	(Activate on) Oldest call waiting
DTA	Dynamic threshold adjustment
DPA	Dynamic percentage adjustment
DQP	Dynamic queue position
SO	Service objective
Extension Service Level	Extension number of the hunt group/skill group and the assigned service level targets (represents percentage of calls answered in a specific number of seconds)
Level 1 Threshold	First wait time threshold; when value is exceeded, calls queued to group of reserve agents.
Level 2 Threshold	Second wait time threshold; when exceeded, calls routed to contingency reserve agents
EWT	Estimated wait time for calls queuing to hunt group/skill group
OCW	Oldest call waiting time in queue for the hunt group/skill group

Table 8: Skilled hunt group details

Group Number	Group Name	Group Extension	Group Type
Service Level Supervisor	Call Selection Override	Activate on Oldest Call Waiting	Dynamic Threshold Adjustment
Dynamic Percent Adjustment	Dynamic Queue Position	Service Objective	Weighted Service Level (status)
Service Level Target (percentage and time)	Level 1 Threshold	Adjusted Level 1 Threshold (status)	Level 2 Threshold
Adjusted Level 2 Threshold (status)	SLS State (status)	Expected Wait Time (status)	Time in Queue of Call at Head of Queue (status)

socket-usage

monitor socket-usage

Use **monitor socket-usage** to show how many IP endpoints are registered and how many of those registered IP endpoints have their TCP signaling channels established (connected). The monitor socket-usage screen is periodically updated until the user cancels out of the command.

Syntax

```
monitor socket-usage
```

status socket-usage

Use **status socket-usage** to show a snapshot of the individual socket usage for each C-LAN or Processor Ethernet information, and to list the system's:

- number of registered IP endpoints
- number of registered IP endpoints with TCP signaling sockets established
- number of sockets used
- number of sockets on the system

status socket-usage replaces **status clan-usage**.

Syntax

```
status socket-usage [ schedule ]
```

schedule Specify a time to run the command.

status socket-usage field descriptions

Field	Description
Total Registered IP Endpoints	The number of IP endpoints registered with the server.
Registered IP Endpoints with TCP Signaling Socket Established	The number of registered IP endpoints that have their TCP signaling channels established.
Total Socket Usage	The number of TCP signaling sockets currently in use by C-LANs and Processor Ethernet circuit packs.
Intf Type	Type of interface: • **C-LAN** — TN799 circuit pack • **procr** — Processor Ethernet circuit pack • **procr6** — Displays the socket count for the procr6 node name
Loc	The cabinet/carrier/slot location of the C-LAN or Processor Ethernet circuit pack
Board/Suffix	The circuit pack designation suffix
Socket Usage	First number is the number of sockets in use on the circuit pack when the command was entered. Second number is the value administered in the Number of C-LAN Sockets Before Warning field using the **add/change ip-interfaces** command. The socket number does not include sockets used by adjuncts.
Net Rgn	Network Region assigned to the circuit pack on the add ip-interfces screen.

sp-link

busyout sp-link

Use **busyout sp-link** to put the system printer link into a maintenance busy state and prevent access to the system printer.

The system printer link is a link from the switch to an external printer. This link is created by administering the system printer extension and setting up a call to the system printer.

Syntax

```
busyout sp-link
```

See **status link** for more details on links.

release sp-link

Use **release sp-link** to release the system printer link from a maintenance busy state and enable access to the system printer.

Syntax

```
release sp-link
```

See **busyout sp-link** for more information, and Busyout and Release Commands. See **status link** for more details on links.

status sp-link

Use **status sp-link** to see a summary of the operational state of the system printer link.

Syntax

```
status sp-link
```

See **status link** for more details on links.

status sp-link field descriptions

Field	Description
Link State	The operational state of the link: • **up** — call is currently set up to the system printer. • **down** — link is administered but a call is not currently set up to the printer. • **extension not administered** — extension is not administered on the features-related system parameters screen for the system printer.
Number of Retries	The number of times the switch tried to establish the link since a request to set it up was received. This field is displayed only when the link is down.
Maintenance Busy	Whether maintenance testing is being performed on the system printer link. Blank if the system printer link is not administered.

test sp-link

Use **test sp-link** to perform tests on the system printer link to determine if the link is up, down, or if an extension was not administered. The system printer link is a link from the switch to an external printer.

Syntax

```
test sp-link [ long | short ][ schedule ]
```

long	Run the long test sequence.
short	Run the short test sequence.
schedule	Specify a time to run the command.

See **status pms-link** for more information. See **status link** for more details on links.

ssh-keys

reset ssh-keys

Use **reset ssh-keys** to generate new SSH dynamic host keys on C-LAN and VAL circuit packs for craft/dadmin logins and higher. Before you reset the dynamic host keys with **reset ssh-keys board**, use **busyout board** to busyout the C-LAN and VAL circuit packs.

Syntax

```
reset ssh-keys location
```

location	Location of the board on which to reset the dynamic host keys.

Dynamic host keys

Dynamic keys are inherently more secure than static keys because:

- If static keys for one circuit pack are compromised, all circuit packs are compromised.
- The probability of compromise is reduced when each circuit pack has its own dynamic key.
- Users can change dynamic keys at any time.

Dynamic host keys include:

- IP address
- Host name
- Firmware

Public key exchange

TN circuit packs support dynamic host keys. Because clients have the server's public key information stored on them, when the server generates a new public/private key pair (which happens the first time the board initializes or when the user decides), the client prompts the user to accept the key when logging into the server. This is to make the client user aware that the server's public key is not what it used to be and this may, but not necessarily, imply a rogue server.

A technician encountering a situation where the server's public key is not what it used to be should determine if the server's keys were changed since the last servicing.

- If they were, the technician should continue login.

- If not, there is a security issue, and the technician should notify the appropriate personnel.

station

add station

Use **add station** to administer a new station.

Syntax

```
add station x | next
```

x Extension number of the new station.

next Assigns the next available extension number to the new station.

For field descriptions, see *Administering Avaya Aura®Communication Manager (03-300509)*.

busyout station

Use **busyout station** to busyout an installed or uninstalled station extension.

Syntax

```
busyout station x
```

x Extension number per dial plan.

Example

```
busyout station 12345
```

change station

Use **change station** to change an installed extension.

Syntax

```
change station x
```

x Extension number per dial plan.

For field descriptions, see *Administering Avaya Aura®Communication Manager (03–300509)*.

list station

Use **list station** to list the installed extensions.

Syntax

```
list station [ ext x ][ to-ext  x | port  x | type  x | movable  x | count  n ][
schedule ]
```

ext *x* First extension in the list.

to-ext *x* Last extension in the list.

port *x* Port number. Shows IP Telephone port when IP Softphone and IP Telephone are in shared control.

Note:

The Port field shows information for only IP Telephone when an IP telephone and IP Softphone are in service on the same extension simultaneously.

type *x* Type of station.

movable *x*
- list station movable always – shows extensions available for moves anytime
- list station movable done – shows extensions that had the Automatic Moves field set to once, and have moved
- list station movable error – shows extensions administered incorrectly and non-serialized extensions
- list station movable no – shows extensions not available to be moved
- list station movable once – shows extensions available to be moved once

count *n* Number of stations in the list.

schedule Specify a time to run the command.

release station

Use **release station** to remove specified administered voice terminal extensions from a maintenance busy state.

Syntax

```
release station x
```

x Extension number per dial-plan.

status station

Use **status station** to see the internal software state information for a specific station. Use the information for diagnosis and to help locate the facilities to which the station is communicating.

Syntax

```
status station x
```

x Extension number per dial plan.

status station field descriptions, page 1 — General Status and Hospitality Status

Field	Description
Active Coverage Option	Specifies the active coverage path.
Administered Type	Administered station type.
Call Parked	Whether the station has a call parked (**y/n**)
Connected Ports	Port locations of the facilities to which the telephone/softphone is connected: cabinet-carrier-slot-circuit **Note:** If a station is connected to a QSIG over SIP trunk, you can view the involved port of the SIP trunk. However, you cannot view the port of the QSIG trunk since the port is not involved in the media connection.
Connected Type	The type of telephone connected to this port.
Download Status	Status of soft key download.
EC500 Status	**enabled** — Extension to Cellular is enabled **disabled** — Extension to Cellular is disabled
Extension	Station or attendant extension.
Group Cntrl Restr	One or two of the following: • none • total • stat-stat • outward • terminate
Limit Incoming Calls	State of the Limit Number of Concurrent Call (LNNC).
Message Waiting	Whether there is a message waiting for the station. • AUDIX • PMS

Table continues…

Field	Description
	• blank if no messages are waiting
Network Region	The network region (NR) that determines whether Communication Manager triggers the IGAR or DPT feature: • For a DCP or analog station, this field displays the NR of the port network or media gateway to which the station is connected. • For a registered H.323 station, this field displays the NR to which the station is currently assigned. • For an unregistered H.323 station, this field displays the NR in which the station was registered most recently. • For a SIP station, this field displays the NR associated with the IP address that Communication Manager received in the most recent SIP INVITE or SIP response for that station.
Off-PBX Service State	• **inservice/idle** — there is no OPTIM call at the station • **inservice/active** — there is an OPTIM call at the station • **out-of-service** — the station is busied out.
Parameter Downlaod	Current status of downloading terminal parameter information. • **complete** — the information was successfully downloaded sometime in the past. • **pending** — the system is waiting to download the information. The download will complete through a background periodic test or demand test. • **not applicable** — this is not a programmable station.
Port	Port location of the endpoint: cabinet-carrier-slot-circuit.
Ring Cut Off Activated	Whether ring cut-off is activated (**y/n**).
SAC Activated	Whether Send All Calls is activated on this extension (**y/n**).
Service Link Extension	Extension for the softphone off-premise destination on a telecommuter configuration.
Service Link Port	Shows the port used to establish a connection to the softphone off-premise destination on a telecommuter configuration.
Service State	State of the telephone endpoint: • **in-service/on-hook** (with no OPTIM calls, if applicable) • **in-service/off-hook** • **in-service/disconnected** (no OPTIM calls, if applicable) • **in-service/idle** (the station is AWOH or hardware is otherwise not present, with no OPTIM calls if applicable) • **in-service/active** (with OPTIM, has OPTIM calls and is not physically off-hook) • **in-service/in-tsa** (Terminal Self Administration)

Table continues…

Field	Description
	• **out of service** (the station is busied-out)
Shd TCP Signaling Status	Indicates whether a TCP signaling channel is established for the endpoint on a shared control connection. Displayed only for IP Telephones and Softphones. • **connected** — Endpoint is registered and TCP signaling link is established • **connecting** — Endpoint is registered and TCP signaling link is in the process of being connected • **not connected** — Endpoint is unregistered • **on-demand** — Endpoint is registered and TCP signaling link is not established. For IP endpoints with **on-demand** status, **`test station`** triggers TCP socket establishment. For all IP endpoints except soft IP endpoints such as IP Softphone and IP Agent, **`status station`** triggers TCP socket establishment.
Softphone Port	The port for the softphone controlling an IP telephone.
TCP Signal Status	Indicates whether a TCP signaling channel is established for the endpoint. Displayed only for IP Telephones and Softphones. • **connected** — Endpoint is registered and TCP signaling link is established • **connecting** — Endpoint is registered and TCP signaling l0000000ink is in the process of being connected • **not connected** — Endpoint is unregistered • **on-demand** — Endpoint is registered and TCP signaling link is not established. For IP endpoints with **on-demand** status, **`test station`** triggers TCP socket establishment. For all IP endpoints except soft IP endpoints such as IP Softphone and IP Agent, **`status station`** triggers TCP socket establishment.
User Cntrl Restr	One or two of the following • none • total • stat-stat • outward • terminate
Hospitality Status	
Awaken At	Time that Automatic Wakeup Call is scheduled. The time is based on the location of the station.
User DND	**activated/not activated** Status of Do Not Disturb

Table continues…

Field	Description
Group DND	**activated/not activated** Status of Do Not Disturb
Room Status	Whether a room is occupied or not • non-guest room • vacant • occupied

status station field descriptions, page 2 — Connected Station Information and Unicode

Field	Description
General Status	
Connected Station Information	
Part ID Number	Part ID Number (comcode) of the telephone. If this field shows Unavailable, the software was unable to determine the Part ID Number.
Serial Number	Serial number of the telephone. • **Unavailable** — the software is unable to determine the Serial Number. • **Errored** — the serial number received is not in the correct format.
Station Lock Active	Indicates whether the station has been locked using Station Lock.
TOD Station Lock	Indicates whether the station is within a Time of Day lock interval.
Unicode Display Information	
Native Name Scripts	N/A, or on a Unicode-enabled station, the script used for the native name of the station: 0x plus the hex value of the script tag, and up to 7 language acronyms.
Display Message Scripts	N/A, or on a Unicode-enabled station, the script used for the display language of the station: 0x plus the hex value of the script tag, and up to 7 language acronyms.
Station Supported Scripts	N/A, or on a Unicode-enabled station, the script supported by the telephone: 0x plus the hex value of the script tag based on the scripts supported by Unicode capable endpoints, and up to 7 language acronyms.
Languages	Communication Manager displays the language that you have downloaded on a 9404 or 9408 telephones. The default value of this field is blank.
Language File Version	Communication Manager displays the version of the language that you have downloaded on a 9404 or 9408 telephones. The default value of this field is blank.

Table continues…

Field	Description
CF Destination Ext	Call forwarding destination extension, if any. • blank when Extension to Cellular is enabled • is displayed for mapped extensions when Extension to Cellular is disabled
Enhanced Call Forwarding Destinations	Up to six Enhanced Call Forwarding destination numbers for Unconditional, Busy, or No Rely ECF types, and the internal or external destination for each.
Team Button Monitoring Stations	Shows all monitoring extensions that supervise the monitored station

status station field descriptions — 3way IP Conference Call, pages 1–3

Field descriptions are the same as **`status station`**, pages 1 and 2 field descriptions.

status station field descriptions — Call Control Signaling, page 5

Field	Description
Call Control Signaling — Call Control Signaling fields display the information for both endpoints when an IP telephone and IP soft phone are in service on the same extension simultaneously (shared-control).	
Switch-End IP Signaling Loc	The C-LAN board location serving the switch end of the IP signaling link. The port number is always 17 for the **ethernet** port of the C-LAN. This field is blank for an unregistered H.323 station.
H.245 Port	The C-LAN port serving the H.245 signaling link. The port number is 17 for the **ethernet** port. This field is blank for an unregistered H.323 station, a VPhone, or when H.245 tunneling in Q.931 is used.
Switch-end: IP Address and Port	Switch-end Q.931 (H.323 station) or CCMS (IP SoftPhone) IP signaling address and IP port. IP Port has a decimal value 0-65535. This field is blank for an unregistered H.323 station.
V4 Set-End: IP address and Port	Set-end IPv4 IP signaling address and IP port. IP port is a decimal value 0-65535.
V6 Set-End: IP address and Port	Set-end IPv6 IP signaling address and IP port. IP port is a decimal value 0-65535.
Node Name (for Call Control)	Label administered for an IP address.
Region (for Call Control)	A number given to a set of IP addresses to indicate they have a common set of characteristics.
H.245 Near	Switch-end H.245 IP signaling address and TCP/IP port. IP Port is 0-65535. This field is blank for IP SoftPhone endpoints, endpoints using Q.931 tunneling of H.245, and unregistered or inactive H.323 stations.
H.245 Set	Set-end H.245 IP signaling address and IP Port. IP Port is 0-65535. This field is blank for IP SoftPhone endpoints, endpoints using Q.931 tunneling of H.245, and unregistered or inactive H.323 stations.

status station field descriptions — Audio Channel, page 6

Audio Channel fields display the information for only the IP Telephone when an IP telephone and IP soft phone are in service on the same extension simultaneously. Product Information fields show the information for both endpoints for soft phone and Telephone Shared Control.

Field	Description
xxxxxxx Audio	The type of audio active for the station. xxxxxxxx is one of these values: G.711-MU, G711-A, G.729A, G.723.1-6.3, G.723.1-5.3, PCM, 711-MU, 711-A, 729, 729A, 729B, 729-AB, or 723.1-5.3/6.3. • **PCM** - the station is a telecommuter IP softphone configuration with call-back audio • **blank** - no audio path is present
Port/Shared Port	The physical port used to provide audio path for the endpoint. The port represents a MedPro port for H.323 stations, or for stations using a H.323 endpoint for audio. An idle IP SoftPhone or H.323 station with an as-needed service link shows no audio port. Blank — stations with no established audio path, or for telecommuter stations.
Other-end IP Addr and Port	Other-end IP audio address and IP port. Port is a decimal value 0–65535. This field is blank for an idle station with no audio link, or for a telecommuter IP SoftPhone with circuit-switched audio link.
Set-end IP Addr and Port	Set-end IP audio address and IP port. Port is a decimal value 0–65535. This field is blank for an idle station with no audio link, or for a telecommuter IP SoftPhone with circuit-switched audio link.
Node Name	Label administered for an IP address.
Network Region	A number given to a set of IP addresses to indicate they have a common set of characteristics.
Audio Connection Type	Audio codec selected. • ip-tdm • ip hairpin • ip direct • ip-idle • blank — audio is carried directly to service link port

Table continues…

Field	Description
MAC Address	The Media Access Control (MAC) address received from the telephone when the telephone registers. This field is displayed in the second column of the screen when the Shared Port field is populated. • not available: the telephone registers but is unable to send a MAC address • blank: the telephone is not registered.

status station field descriptions — IP Endpoint Data, page 7

Field	Description
Product ID and Release	Identifier submitted by the endpoint during registration, and the release number of the endpoint that is provided to the gatekeeper upon registration. This field is displayed only for Avaya or Lucent products. This field is displayed in the second column of the screen when the Shared Port field is populated. Value is one of the 30 allowed product IDs administered on the system-parameters customer-options screen, including: • IP_Tel - IP Telephone • IP_Soft - IP Softphone • IP_eCons - An IP soft console • IP_Agent - An IP soft agent telephone • IP_ROMax - A remote office telephone
H.245 Tunneled in Q.931	**y** — H.245 is contained within Q.931, and H.245 fields are not displayed. Does not apply to IP SoftPhone endpoints. This field is displayed in the second column of the screen when the Shared Port field is populated.
Registration Status	Identifies the registration and authentication status of the IP endpoint. An unregistered IP SoftPhone cannot be identified as an IP endpoint. This field is displayed in the second column of the screen when the Shared Port field is populated. • **unregistered (H.323 station only)** — the endpoint is unregistered • **registered-not-authenticated (H.323 station only)** — the endpoint is registered, but has not been authenticated (the station is disallowed from making or receiving calls) • **authenticated-not-registered (H.323 station only)** — the endpoint has been authorized (by the associated IP SoftPhone), but is not yet registered • **registered-authenticated** — the endpoint is registered and authenticated (for example, an IP station that is able to make calls)

Table continues…

Field	Description
	• **pending-unregistration** — the endpoint is unregistered, but critical internal data structures have not yet been updated
MAC Address	The Media Access Control (MAC) address received from the telephone when the telephone registers. This field is displayed in the second column of the screen when the Shared Port field is populated. • not available - the telephone registers but is unable to send a MAC address • blank - the telephone is not registered.
Authentication Type	**Note:** This field complies with the Unified Capabilities Requirements (UCR) 2008 Change 3 requirements and is approved by Joint Interoperability Test Command (JITC). This field is available only for the USA Department of Defense (DoD) and approved Federal government customers. When you register the stations with security profile H323TLS, status station shows **Authentication Type** as TLS.
Native NAT Address	Specifies the network address translation (NAT) IP address of the endpoint when a network device provides the network address translation function for the endpoint. The network device provides the NAT address of the endpoint at the time of registration. The field is blank if the NAT address is not known. This field is displayed in the second column of the screen when the Shared Port field is populated.
ALG-NAT WAN IP Address	This field is populated only when a special application turned on.
Media Encryption	**aes** indicates Advanced Encryption Standard encryption, the standard used by U.S. government to protect sensitive (unclassified) information. Reduces circuit-switched to IP call capacity by 25%. **aea** indicates Avaya Encryption Algorithm. Not as secure as AES. **none** indicates an unencrypted media stream.

status station field descriptions — ACD Status, page 8

Field	Description
Grp	Hunt Group number
Mod	ACD Work Mode
On ACD Call	Whether the agent is on an ACD call (**y/n**)
Occupancy	Occupancy of the agent logged in at the specified station

status station field descriptions — Network Status and Summary

Network Status fields show information for only the IP Telephone when an IP telephone and IP Softphone are in service on the same extension simultaneously.

Field	Description
Average Jitter Last Ten Seconds # - more than 255 ms	The average jitter in received packets from the last ten one-second intervals. **#** — maximum (100%) packet loss per second during the one-second interval.
Packet Loss per Second Last Ten Seconds * - 100% loss	The 10 most recent one-second samples of the lost packet information for the requested endpoint. ***** — maximum (100%) packet loss per second during the one-second interval. * is displayed when silence suppression is y on the ip-codec-set screen, or when packet loss = 100%.
Out of Order Count	A count of the number of out-of-order packets detected during the current connection.
SSRC Change for Call	The number of SSRC changes occurring during the current connection.
Last Rx Sequence No.	Last received data packet sequence number.
Last Tx Sequence No.	Last transmitted data packet sequence number.
Echo Return Loss	Loss of the echo signal, relative to the transmitted signal, due to the PSTN network including the hybrid.
Bulk Delay	Delay offset of the echo relative to the original signal.
ERL Enhancement	Loss introduced by the echo canceller. This is the measure of the effectiveness of the echo canceller.
Summary	
Worst Case this Call	Jitter: the worst-case, 1-second jitter (ms) experienced during the current connection. Packet Loss: the worst-case, 1-second packet loss experienced during the current connection.
Average this Call	Jitter: the average jitter for the current connection (the running average of all the 1-second intervals during the connection. Packet Loss: the average packet loss number for the current connection (running average of all the 1-second intervals experienced during the connection.
Current Buffer Size	The current jitter buffer size.

status station field descriptions — Connected Ports

Connected Ports fields show information for only the IP telephone when an IP telephone and IP Softphone are in service on the same extension simultaneously.

Field	Description
src port	The port address of the statused station.
MP	The physical port location of the media processing circuit pack.

Table continues…

Field	Description
	The audio stream passes through a media processing circuit pack (either a Medpro or a VoIP module on a gateway) when direct IP-IP audio connections are disabled or the connection cannot be direct for other reasons (for example, the call requires a codec conversion).
HP	Hairpinning. **y** is displayed when the audio stream is handled entirely on the media processing circuit pack. The audio connection does not require more extensive processing (for example, some codec conversion), and does not use TDM bus resources.
ip-start	The IP address of one end of a direct connection.
ip-end	The IP address of the other end of a direct connection.
audio	Type of audio codec active for the connection. G.711-MU, G711-A, G.729A, G.723.1-6.3, G.723.1-5.3, PCM, 711-MU, 711-A, 729, 729A, 729B, 729-AB, or 723.1-5.3/6.3.
encryption	Type of media encryption as entered on the ip-codec-set screen. **aes** — Advanced Encryption Standard encryption, standard used by U.S. government to protect sensitive (unclassified) information. Reduces circuit-switched to IP call capacity by 25%. **aea** — Avaya Encryption Algorithm. Not as secure as AES. **none** — An unencrypted media stream.
ss	**on/off** Indicates whether silence suppression is active on this audio stream.
pkt	Size of the packet carrying the audio.
dst port	The port address of one of the other parties to which the statused station has a connection on this call.

status station field descriptions — SRC Port to Dest Port Talkpath

Field	Description
src port	port number

status station field descriptions — Voice Statistics

Field	Description
TN Code	The media processor board code used for the call.
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Codec	The codec used for the call.
Encryption	The type of media encryption used on the call (for example, AES, AEA, SRTP 1, and so on.

Table continues…

Field	Description
DSP Number	The number of the DSP on the media processor board used for the call.
Endpoint ID	The endpoint ID assigned for the call.
UDP Port	The UDP port used by the media processor board for the call.
Called Number	The number of the endpoint which received the call (far end).
Dst Net Reg	The network region where the destination media processor is located.
Far-End IP Addr	IP address of the device on the far end of the call (called party).
Echo Canc	Indicates whether the echo cancellation is on/off for the call.
Echo Tail (ms)	The tail length of the echo canceller used for the call. **0** — implies that a different echo canceller was used than the one on the media processor.
Silence Suppression	Indicates whether Voice Activation Detection (VAD) is used for the call.
Comfort Noise Gen	Indicates whether CNG is being used for the call.
Data Call/Type	Indicates whether the call is a data call. If **y** (yes), include type of data call (for example, FAX, Modem, Clear Channel, TTY, Fax-PT (pass-thru), Mod-PT, TTY-PT). For example, Data Call/Type: y/T.38 FAX
Threshold Exceptions	A total number of thresholds that are exceeded for the call when the data was requested.
Packet Size (ms)	The size for each steam of data for the associated call, measured in milliseconds.
% Packet Loss	The amount of packet loss occurred for the call when the data was requested.
Peak Packet Loss (%)	The peak packet loss recorded for the call.
Jitter Buffer Size (ms)	The size of the jitter buffer used for the call, measured in milliseconds.
Jitter Buffer Overruns	A number of jitter buffer overruns occurred for the call. Overruns occur when too many packets arrive into the jitter buffer very quickly, causing the jitter buffer to fill up. When it happens, the jitter buffer is unable to handle additional traffic/packets. If the number of overruns exceeds 99, the value in this field is **99+**.
Jitter Buffer Underruns	A number of jitter buffer underruns occurred for the call. When the arrival time of packets goes beyond the size of the jitter butter, the jitter buffer underrun occurs which results in silence until there are additional packets in the jitter buffer to process. If the number of underruns exceeds 99, the value in this field is **99+**.
Average Jitter (ms)	The average amount of jitter recorded for the call over a 10-second reporting interval, measured in milliseconds.

Table continues…

Field	Description
Peak Jitter (ms)	The peak amount of jitter recorded for the call, measured in milliseconds.
Avg RT Delay (ms)	The average round trip delay of packets, measured in milliseconds.
Peak RT Delay (ms)	The peak round trip delay recorded for the call, measured in milliseconds.

test station

Use **test station** to perform hardware diagnostic tests on an individual port circuit assigned to that extension. The technician must specify the extension and a translation is automatically done to the physical port location.

Syntax

```
test station x  [ short | long ][ repeat  # | clear ]
```

x Extension number per dial plan.

short Execute the short nondestructive test sequence.

long Execute the long test sequence.

repeat # Number of times to repeat the test, between 1 and 100.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

Example

```
test station 81709 l
test station 85136 s r 2
test station 85036 l r 25
test station 84297 r 4
test station 81709 c
```

survivable-processor

list survivable-processor

Use **list survivable-processor** on the primary controller to see the status of Survivable Remote Server or Survivable Core Server administered on the Survivable Processors screen (**add survivable-processor**) or the system-parameters port-networks screen. Verify that the Survivable Remote Server or Survivable Core Server(s) register, and that translations are updated.

Syntax

```
list survivable-processor
```

list survivable-processor field descriptions

Field	Description
Name/IP Address	Name of the Survivable Remote Server or Survivable Core Server as administered on the Survivable Processors screen (**add survivable-processor**) or the System Parameters Port Networks screen. IP address of the node name as it is displayed in the IP Node Name screen and on the Survivable Processor Ethernet screen.
Type	Survivable Remote Server, Survivable Core Server Survivable processor type as listed on the Survivable Processor Ethernet screen (**add survivable-processor node-name**).
ID	Server ID number (cluster ID) of the Survivable Core Server or Survivable Remote Server.
Reg LSP Act	
Service State	**in-service/idle** — the Survivable Remote Server is registered **out-of-service**
Translations Updated	Time and date of the translation update to the Survivable Remote Server or Survivable Core Server.
Net Rgn	Network region in which the PE interface of the Survivable Remote Server or Survivable Core Server resides, as listed on the Survivable Processor Ethernet screen.

For more examples of the Survivable Processor screen, see 'Survivable Processor' in *Avaya Aura®Communication Manager Screen Reference (03-602878)*.

suspend-alm-orig

disable suspend-alm-orig

Use **disable suspend-alm-orig** to stop entries from the active Suspend Alarm Origination table. This command disables all board entries that match a specific physical board location.

Note:

disable suspend-alm-orig does not disable port entries.

Syntax

```
disable suspend-alm-orig location
```

location	Physical location of the board.

Example

```
disable suspend-alm-orig 1C03
disable suspend-alm-orig 1E07
```

enable suspend-alm-orig

Use **enable suspend-alm-orig** to suspend alarm origination for alarms generated by the specified board (location) or port (location) for a the specified amount of time (hrs).

enable suspend-alm-orig does not support circuit packs without a board location. Enter **enable suspend-alm-orig** multiple times to suspend alarms on different boards or ports. If a physical location is specified for which there is already a suspension in effect, the most recent suspension request replaces the previous request.

Use **enable suspend-alm-orig** to improve control over situations such as:

- Quieting a hyperactive port board during installation or troubleshooting.
- Improving control over customer requests. For example, use **enable suspend-alm-orig** to temporarily suspend off-board DS1 alarms for customers who periodically disconnect DS1 trunks for testing or other business purposes.
- Improving control over external (non-Avaya) problems. For example, use **enable suspend-alm-orig** to suspend off-board DS1 alarms before a customer resolves facility problems, such as working with the vendor of a T1 trunk that has developed an off-board condition.
- Improving control over internal (Avaya) problems that cannot be immediately resolved. For example, use **enable suspend-alm-orig** to suspend alarm origination for a bad circuit pack detected late Friday night if personnel cannot be dispatched until Monday.

To see a list of active alarm origination suspensions, use **list suspend-alm-orig**. To disable a suspension, use **disable suspend-alm-orig**.

Syntax

```
enable suspend-alm-orig location [ off-board-only ]  expires-in-hrs  hrs
```

location	Physical location of the hardware.
off-board-only	(Optional) If not specified, both on-and off-board alarms suspended.
expires-in-hrs *hrs*	Number of hours (1–72).

Example

```
enable suspend-alm-orig 1B03 expires-in-hrs  3
enable suspend-alm-orig 1B0701 expires-in-hrs 72
enable suspend-alm-orig 1B07 off-board-only expires-in-hrs 24
```

list suspend-alm-orig

Use **list suspend-alm-orig** to see active entries in the Suspend Alarm Origination table. Even though this command only lists active entries, an entry that expires during the list process is still displayed in the output. If the Suspend Alarm Origination table is empty, the output contain only the title and field headings.

Syntax

```
list suspend-alm-orig
```

switch-node

status switch-node

Use **status switch-node** to see the operational status and attributes of the user specified switch node. The operational status of the active and standby Switch Node Clock (SNC) circuit packs for the switch node displays along with any alarms logged against the specified switch node.

Syntax

```
status switch-node SN#
```

SN# Normally switch node 1 resides in the PN cabinet, and switch node 2, if present, resides in the nearest PN cabinet.

status switch-node field descriptions

Field	Description
Switch Node	The switch node number, 1 or 2. If the PNC is duplicated, the A and B PNCs are reported separately.
Location	The physical location of the switch node carrier: • A high-reliability system shows one switch node location. • A critical-reliability shows the active and standby switch node locations.
Mode	Current role of the switch node carrier. • **active** — SN is providing normal circuit and control functions for PNC • **standby** — SN is ready to become active, but is currently not active • **blanks** — PNC is not duplicated

Table continues…

Field	Description
Major Alarms	Number of major alarms logged against the switch node carrier
Minor Alarms	Number of minor alarms logged against the switch node carrier.
Warning Alarms	Number of warning alarms logged against the switch node carrier.
Active SNC Location	The physical location of the standby switch node Clock circuit pack **no board** if an SNC is administered but not inserted
Standby SNC Location	The physical location of the standby switch node Clock circuit pack **no board** if an SNC is administered but not inserted Blanks if there is no standby switch node Clock for a given switch node

switch-node-clock

set switch-node-clock

Use **set switch-node-clock** to set the active switch node clock (SNC) circuit pack in a given switch node carrier.

set switch-node-clock is valid only for a simplex PNC with a Center State Switch (CSS).

Syntax

```
set switch-node-clock location [ override ]
```

location Switch node clock location (cabinet/carrier/slot).

override Set the active switch node clock regardless of the health of the standby SNC circuit pack.

synchronization

change synchronization

Use **change synchronization** to change the synchronization source for the system. After running change synchronization, clocks may momentarily lose synchronization.

Use **change synchronization** to administer primary and secondary references for the Stratum 4 option, or -Switch, indicating that the synchronization references are input directly to the switch.

Syntax

```
change synchronization [ media-gateway  n | css | port-network  n ]
```

media-gateway *n*	Change the gateway number.
css	Change CSS-connected PNs.
port-network *n*	Change the PN number entered.

change synchronization feature interaction

DS1 interface, BRI trunk, or UDS1 board selected as either a primary or secondary sync source cannot be removed on the DS1 circuit pack administration screen or the regular circuit pack administration screen.

change synchronization field descriptions

Field	Description
Stratum	Enter 3 for stratum-3 clocking or 4 for stratum 4 clocking.
Primary	First choice system synchronization source. Blank means no synchronization. Enter 5-character board location on any system. Sync source must be in the cabinet being administered.
Secondary	Five-character board location for second choice system synchronization source. Blank means no synchronization. Sync source must be in the cabinet being administered.
Location	Circuit pack location of all administered DS1 circuit packs (port network, carrier and board slot).
Type	Type of circuit pack.
Name	User-defined name for the DS1 circuit pack.
Slip	**y/n** Slip alarm enabled on DS1 circuit pack.
Port-Network	Display-only. Port network that supplies synchronization through the tone clock circuit pack (valid for stratum 3 synchronization).

disable synchronization

Use **disable synchronization** to disable the automatic clock-switching capability of the Synchronization Maintenance subsystem. The synchronization subsystem (TDM bus clock, DS1 trunk board, and maintenance and administration software) provides error-free digital communication between the switch and other PBXs, COs, or customer equipment.

disable synchronization does not apply to -connected port networks.

Syntax

```
disable synchronization [ all  |  css  |  port-network  n  |  media-gateway n ]
```


Comments on this document? infodev@avaya.com

all	Disable all PNs.
css	Disable CSS-connected PNs.
port-network #	Disable the PN number entered.
media-gateway #	Disable the media-gateway number entered.

display synchronization

Use **display synchronization** to see a synchronization plan. On a duplicated server, specify the port network number.

Use **display synchronization** to display the synchronization screen with the administered synchronization stratum and reference sources.

Syntax

```
display synchronization [ css | port-network  n| media-gateway  n][ schedule ]
```

css	Display CSS-connected PNs.
port-network *n*	Display the PN number entered.
media-gateway *n*	Display the gateway number entered.
schedule	Specify a time to run the command.

display synchronization feature interaction

A DS1 interface or a UDS1 board that is selected as a primary or secondary synchronization source cannot be removed on the DS1 circuit pack administration screen or the regular circuit pack administration screen.

display synchronization field descriptions

Field	Description
Stratum	Specifies the synchronization stratum used.
Primary	Designates the first choice system synchronization source. Blank — no synchronization.
Secondary	Designates the second choice system synchronization source.
Location	The circuit pack location (cabinet-carrier-slot) of all circuit packs administered to serve as synchronization references.
Name	The user-defined name of the circuit pack. If blank, no name was administered.
Slip	**y** If the circuit pack has slip detection enabled.

enable synchronization

enable synchronization does not apply to -connected port networks.

Use **enable synchronization** to return control of the selection of the synchronization source to the Synchronization Maintenance subsystem after being previously turned off by **disable synchronization**.

The synchronization subsystem consists of the TDM bus clock, DS1 trunk board, maintenance and administration software, and provides error free digital communication between the switch and other PBXs, COs, or customer-premise equipment (CPE). See SYNC (Port Network Synchronization) in the *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*.

Note:

When adding fiber-connect PNs to a configuration, the PNs must be added before enabling synchronization. If synchronization is enabled, use **disable synchronization** to disable synchronization before adding fiber-connect PNs.

Syntax

```
enable synchronization [ all | css | port-network n ]
```

all	Enable all PNs.
css	Enable CSS-connected PNs.
port-network *n*	Enable the PN number entered.

list synchronization

Use **list synchronization** to see the stratum clock and primary and secondary synchronization sources administered for all the cabinets.

Use **list synchronization media-gateway** to see all administered gateway reference boards and the existing reference sources.

Use **list synchronization port-network** to see all administered port network reference boards and the existing reference sources.

Syntax

```
list synchronization [ media-gateway | port-network ][ schedule ]
```

port-network	List the port network reference boards.
media-gateway	List the gateway reference boards.

schedule Specify a time to run the command.

set synchronization

Use **set synchronization** to set a specific synchronization-capable circuit pack as the reference source for system synchronization signals. Synchronization-capable circuit packs include:

- DS1 Trunks
- BRI Trunks
- IPSIs
- Tone-Clocks

Use **set synchronization** only after automatic synchronization has been disabled with **disable synchronization**.

Any administered circuit pack that is synchronization-capable may be specified with set synchronization. The circuit pack remains the synchronization reference until **set synchronization** specifies another circuit pack, or **enable synchronization** is entered.

After **enable synchronization**, the administered primary or secondary synchronization source becomes the synchronization reference. If no primary or secondary source is administered, an IPSI's Tone-Clock circuit, or a Tone-Clock circuit pack provides the port network's timing source.

set synchronization is not supported when -PNC is enabled.

Syntax

```
set synchronization location
```

location Specifies the physical position of the synchronization-capable circuit pack that supplies a reference for synchronization.

status synchronization

Use **status synchronization** to see the current synchronization reference. Synchronization can be established for:

- Fiber-PNCs, established through the server-connected PN, in a direct, CSS, or network.
- IP-PNCs, established by individual PN. The synchronization source can be the same source as the or CSS PNs in a Fiber-PNC network.

Syntax

```
status synchronization [ css | port-network n| all ]
```

css Status of CSS-connected PNs.

port-network *n*	Status of the PN number entered.
all	Status for all PNs.

status synchronization field descriptions

Field	Description
Location	Cabinet location of synchronization: • port network number • CSS
Stratum Level	The stratum level of the current system synchronization reference. If Stratum 3 is displayed, and no DS1s are connected to the Stratum-3 clock or no DS1 connection existed to the Stratum-3 clock for over 24 hours, then the Stratum-3 clock is in free run mode.
Source Maintenance Name	Maintenance object name of the circuit pack that is providing the current system synchronization reference. **IPSI or TONE-BD** — the switch is operating in free run mode. **-SWITCH** — Switching Capability, Excessive Reference Switching, and Physical Location fields are not displayed.
Source Physical Location	The carrier of the PN. Blank when Source Maintenance Name is **-SWITCH**.
Switching Capability	Indicates whether the online reference can be switched or not. Blank when Source Maintenance Name is **-SWITCH**.
Excessive Reference Switching	**y/n** Excessive reference switching is taking place (sync error 1793 is at threshold) Blank when Source Maintenance Name is **-SWITCH**.

test synchronization

Use **`test synchronization`** to check the timing synchronization source and update circuit packs with the correct synchronization parameters. The synchronization-capable circuit packs are sent down-link messages to place them in the correct synchronization configuration given the current on-line synchronization reference. The synchronization-capable circuit packs include:

- DS1s
- IPSIs
- EIs
- Tone-Clocks

The synchronization subsystem provides error-free digital communication between the switch and other PBXs, COs, or customer premises equipment. The subsystem is made up of the TDM bus clock, DS1 trunk circuit packs, and maintenance and administration software.

Syntax

```
test synchronization [ css | port-network  n | all ]
```

css	Check CSS-connected PNs.
port-network *n*	Check the PN number entered.
all	Check all PNs.

test synchronization field descriptions

Field	Description
Location	Cabinet location of synchronization: • port network number • CSS
Maintenance Name	**-SYNC** — port networks **Sync** — CSS port networks or IP-PNCs
Alt Name	Blank
Test No.	The test number, 417, associated with the synchronization test
Error Code	The maintenance error code if the test fails

sys-link

list sys-link

Use **list sys-link** to see every system link. Each link's location, type and dlci number, state, current path status, faulted path status, and last recorded fault (if any) are displayed. See SYS-LINK (System Links) in *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)* for details.

See **status link** for more details on links.

Syntax

```
list sys-link [ schedule ]
```

schedule	Specify a time to run the command.

list sys-link field descriptions

Field	Description
Location	The physical location of the far endpoint associated with the system link (cabinet-carrier-slot-circuit).
Type/dlci	The type of system-link and the dlci of the link (if there is one). System links include the following (see SYNC (Port Network Synchronization) in the *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*: • BFDL - Bearer Fault Detection Link • EAL - Expansion Archangel Link • INL - Indirect Neighbor Link (center stage switch) • MBL - Maintenance Board Link • MPCL - Medpro Control Link • PACL - Port-Network Connectivity Control Link • PRI - ISDN-PRI Signaling Link • RSCL - Remote Socket Control Link (C-LAN/VAL) • RSL - Remote Socket Link • TACL - Trunk Control Link
State	Whether the system link is **up** or **down**.
Current Path	This field specifies the status of the current path. This field displays **none** if the link is down or **present** if the current path is functional.
Faulted Path	This field shows whether the link has experienced a fault and been switched to another path. • **Present** indicates that the link has been faulted at least once. • **None** is displayed if the link has not gone down. • **Default** is displayed if the default faulted path is being used.
Last Fault Recorded	The date and time that the most recent fault on the link took place.

status sys-link

Use **`status sys-link`** to see status data for a specified system link. The report includes the type and operational state of the link, the associated processor dlci, if any, active alarms and path status, and a list of all hardware components making up the link's path. If, in addition to the current path, a faulted path exists, the components making up the faulted path are displayed on page 2 of the report.

For port networks with IPSI, **`status sys-link`** also provides status for a BFD link. The information shown is similar to other link types.

See **`status link`** for more details on links.

Syntax

```
status sys-link port-location [ dlci # ]
```

port-location Location of the port associated with the link.

dlci # dlci number associated with an RSL link.

status sys-link field descriptions

Field	Description
Location	Location of the port associated with the system link (cabinet-carrier-slot-circuit).
Type/dlci	Type of system link and dlci number (RSL link). See Type/dlci under **list sys-link** for the link types.
Alarms	The highest level of alarm currently logged against the components making up the link.
Current Path	The operational status of the current path: • **none** — The link is down. • **present**— The current path displayed below is valid.
State	Whether the system link is **up** or **down**.
Time Up	The date and time that the link came up
Faulted Path	The status of the faulted path, if any: • **present** — The path of the link has been faulted at least once. • **none** — There is no record of the link having gone down. • **default** — The default faulted path is being used.
Last Fault	The date and time at which the most recent fault occurred.
Current Hardware Path	The location, maintenance name, and alarm information for each hardware component making up the current path of the link. The path begins at the Packet Interface on the IPSI and terminates at the circuit path that terminates the other end of the link.
Faulted Hardware Path	If the link encounters a fault, the system will reroute it if possible over an alternate route. If this has taken place, the faulted path is displayed on page 2 of the report. The location, maintenance name, and alarm information for each hardware component making up the most recent faulted path is shown.

test sys-link

Use **test sys-link** to validate the existence of the specified link and runs diagnostic tests on the hardware path that comprises the system link. Use current or faulted to run tests on every hardware object that comprises the specified link. If current or faulted is not specified, only the end-to-end sys-link connection is tested.

The hardware path that comprises a system link consists of up to 21 hardware components that affect the behavior of the link. The number of components of a given system link hardware path depends on the system configuration and type of system link. The following links are examples of system links: EAL (Expansion Archangel Link), INL (Indirect Neighbor Link), and PRI (PRI signaling link).

See **status link** for more details on links.

Syntax

```
test sys-link location  [ dlci  # ][ current  |  faulted ] [ short  |  long ][ repeat #
|  clear ] [ schedule ]
```

location Port location associated with the system link.

dlci # dlci number.

current Current hardware path tested.

faulted Tests the hardware path of the system link as it was constituted when a fault last caused the link to go down.

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test, between 1 and 100.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

Example

```
test sys-link 2e0201 current
test sys-link 2e0201 faulted r 10
```

system

monitor system

Use **monitor system** to see a summary of the overall condition of the system, real-time status for time slots and buses, call rates, intervals, and so on. Press **CANCEL** to clear the command.

Syntax

```
monitor system view1 | view2 |conn [ conn pnn | conn pnn #
```

view1	Show attendant status, the maintenance status, the last hour's measurement of trunk groups, hunt groups, and the attendant group, and the time of day.
view2	Show the view1 screen except the last hour's hunt group measurements
conn	Show the connection monitor output for key information
conn pnn#	shows data for specific PNNs (1–3).

Use **monitor system view1** and **monitor system view2** to see the condition, or health, of the system.

- view1 shows attendant, maintenance, and traffic status. Attendant and maintenance status are updated every minute and traffic status is updated on an hourly basis. Pressing **CANCEL** forces a logout of the current login ID.
- view2 shows the view1 screen except the hunt group measurements

Use **monitor system** connection to see the status of connections, compiled by the connection manager. This on-line status report is automatically updated every minute or by pressing the **UPDATE** key. Pressing **CANCEL** forces a logout of the current login ID. Use **monitor system** conn pnn to specify PNNs for the report.

Examples

```
monitor system view1
monitor system view2
monitor system conn
monitor system conn pnn 1 5 7
```

monitor system view1 and view2 field descriptions

Field	Description
# of alarms for other resources	The number of existing minor and major alarms on every maintainable object in the system except trunks and stations.
First OSS number has been informed	Has every alarm been reported and acknowledged by the first OSS telephone number? If "Alarm Origination" is not enabled or there are no active alarms, this is n.
Measurement Hour	The starting time of the period for which the measurement was taken. For example, if the measurement hour is shown as 18, the traffic status data is for the time period from 6 PM to 7 PM. The measurement is taken on an hourly basis).
Grp no	The trunk-group or hunt-group number.
Grp dir	Group direction: incoming, outgoing, or two way.
Calls qued	Total calls that arrived and were placed in the queue for trunk groups.
Calls aban	Total calls that were abandoned by the caller.
%Out blkg	The ratio of outgoing calls that are not carried, due to overload conditions, on a trunk group to the outgoing calls offered.

Table continues…

Field	Description
% Time ATB	The percentage of time within the polling interval that every trunk in the trunk group was unavailable for use.
Time of day	The current time of day acquired from the system.

monitor system conn field descriptions

Field	Description
Max_callrate	The maximum call rate hit during the time since the last hour has passed. For example, if monitor system conn is executed at 20 minutes past 12:00, this shows the maximum call rate obtained during the past 20 minutes.
Next_hour	0 or 1, depending upon if the measurements being taken are for this hour or the next. It is related to the previous field in that the maximum call rate is reflected for this hour. When this flag is set, statistics begin to accumulate for the next hour. Shortly thereafter, the maximum call rate becomes zero and new accumulations begin.
tot_ts_req	Number of time slots in use during the time period elapsed since the top of the last hour. Data is collected every 100 seconds. When the timer fires and the data collection occurs, a check is made as to how many time slots are currently in use. One number is displayed for each PNN requested.
ts_denied	Number of time slots requests that were denied during the time period elapsed since the top of the last hour. Data is collected every 100 seconds. One number is displayed for each PNN requested.
tot_fts_req	Number of fiber time slots that have been requested. One number is displayed for each PNN requested.
ts_count	The number of time slots in use during the last 100-second poling period. One number is displayed for each PNN requested.
ts_total	Number of time slots requested since the top of the last hour.
fts_count	Number of fiber time slots in use during the last 100-second polling period. One number is displayed for each PNN requested.
fts_total	Number of fiber time slots requested since the top of the last hour.
Requests- TN748 TTRs	Number of currently active touch-tone receivers requested on the TN748 circuit pack.
Requests- TN748 CPTRs	Number of currently active call progress tone receivers requested on theTN748 circuit pack.
Requests- TN744 CPTRs	Number of currently active call progress tone receivers requested on the TN744 circuit pack.
Requests- TN744 TTRs	Number of currently active touch-tone receivers requested on the TN744 circuit pack.
Requests- TN744 MFC	Number of currently active multifrequency receivers requested on the TN744 circuit pack.

reset system

Use **reset system** to reload Communication Manager software. All system resets are disruptive and terminate the SAT login.

Caution:

All system resets are service affecting, with higher levels being increasingly destructive. Some resets may take up to one-half hour to complete. Certain conditions may result in a higher reset level than the one requested. Unless you are experienced with resetting a system, follow normal escalation procedures.

Syntax

```
reset system level#
```

level# (1–5) Restart Level

Description

If you set the value of the Display Warning Prior to System Reset? field to `y` on the **system-parameters maintenance** screen and then use the reset system command, a warning message is displayed.

```
WARNING: All system resets are service affecting, with higher levels
being increasingly destructive.
```

Press the SUBMIT or ENTER function key to continue or CANCEL to abort the command.

Note:

Connections are preserved on H.248 branch gateways on reset system 2 and reset system 4 conditions. To reset gateways from the SAT, use **reset media-gateway**.

reset system resets the system in the following manner:

- A mini-coredump is generated for non-interchange related restarts and placed in the directory:`/var/log/defty/dumps`.
- A change in translation administration is in progress.

System software generally does not escalate a demand system reset to a higher level. There are certain conditions that result in a higher level reset than that requested. These include:

- A PNC interchange is already in progress.
- the restart is performed

Approximate Recovery Time for System Resets (min:sec)

System reset times differ between different configurations

Level	Recovery	2,400 lines	5,000 lines	15,000 lines
1	Warm Restart	:10	:10	:10

Table continues…

Level	Recovery	2,400 lines	5,000 lines	15,000 lines
2	Cold-2	1:00	2:00	4:00
4	Reload	4:00	6:30	11:00

reset system feature interactions

reset system invokes system initialization like low-level maintenance. Software never escalates requested reset levels; technicians determine the levels.

Reset system cannot be canceled. The screen shows the results of various initialization tests. If reset system is successful, the user is logged off. Several conditions may prevent a requested reset.

Reset Level 1

Reset Level 1 (warm restart) duration, causes, and effects

Duration	Up to 10 seconds, typically 4 seconds
Causes	**reset system 1** command from Communication Manager (SAT/ASA) command line Spontaneous server interchange (those caused by hardware faults) Software faults that are not service affecting Demand server interchange Software escalation
Effects	Stable calls are preserved; queued ACD calls, H.323 calls, and H.320 (multimedia) calls stay up. System links such as ISDN-PRI D-channel signaling links, CMS, AUDIX, DCS links over C-LAN are preserved. The CMS, DCS, and AUDIX links could lose buffered messages. Error and alarm logs are preserved, but every alarm is resolved except busyouts. Stable features are preserved. Transient calls (not yet connected) and some user stimuli are dropped. New calls are not processed during the reset. Encrypted system links may be dropped and reestablished. Every administrative session except those over the TN799 C-LAN are dropped. If the reset resulted from a spontaneous server interchange, memory shadowing is turned off, and the standby server will not be available for service until memory is refreshed (several minutes). Application links such as those to AUDIX and CDR are dropped and re-established in under 2½ minutes. Translation data is preserved in memory. If **save translation** is in progress, an SAT-requested warm restart would be aborted. A software-requested warm restart would result in an unsuccessful **save translation** and possibly corrupt translations.

Reset Level 2

Reset Level 2 (cold restart) duration, causes, and effects

Duration	Up to 3.75 minutes
Causes	**reset system 2** command from Communication Manager (SAT/ASA) command line Escalation from SAT's **reset level 1** An attempted SAT's **reset level 1** during a PNC interchange Spontaneous interchange into an unrefreshed standby server
Effects	Every system and application link is dropped. Gateways are not reset. Every call is dropped. Every administrative session is dropped. Every system link is dropped and re-established. Every application link is dropped and re-established. Non-translation feature data, such as Automatic Wakeup calls, are lost and must be re-entered. Translation data is preserved in memory. If **save translation** is in progress, a SAT-requested cold-2 restart would be aborted. A software-requested cold-2 restart would result in an unsuccessful **save translation** and possibly corrupt translations. Every login, including remote access and system port logins, is dropped. Initialization firmware runs diagnostics and displays results on the screen. Server memory shadowing is turned off, leaving the standby server unavailable for service for up to several minutes. Every hardware component is reset except: • Active TN2312 IPSI in any PN. • Active EI in a non-IPSI connected PN. • SNIs. • SNCs. • DS1 clocks. For a critical-reliability system (duplicated PNC), a global refresh of the standby PNC is performed after the reset. Every busied-out MO is released and can be rebusied. Circuit packs are reinitialized. (Translations are verified by comparison to physical boards' locations.) Error and alarm logs are preserved, and every Communication Manager alarm is resolved.

Reset Level 4

Reset Level 4 (reload) duration, causes, and effects

Duration	Typically 11 to 14 minutes
Causes	**reset system 4** command from Communication Manager (SAT/ASA) command line Escalation from SAT's **reset level 2** Power up Recovery attempt from server-down mode
Effects	System software (boot image) is reloaded and every process is re-initialized. Communication Manager administration (translations) are reloaded from the hard disk. Before reboot, the system attempts to save the alarm and error logs. After reboot, error and alarm logs are restored. Some error and alarm information may be lost if the last save before the reboot save does not succeed. Other effects are the same as those in **reset level 2**, except that more extensive diagnostics are performed. A core dump is automatically enabled for this reset level and is saved to the /var/log/defty/dumps/ directory. The reboot is delayed until the core dump is finished.

system-parameters duplication

change system-parameters duplication

Use **change system-parameters duplication** to enable or disable PNC and/or IPSI duplication.

If only IPSI duplication is administrable, it is because PNC duplication is disabled on the change system-parameters customer-options screen. IPSI duplication can be enabled without PNC duplication, but if PNC duplication is enabled, IPSI duplication must also be enabled.

Enabling IPSI duplication requires that all IPSI-connected port networks with direct-connect, CSS, or fiber connections have both primary and secondary IPSI boards. Disabling IPSI duplication requires that all primary IPSI boards be active.

Syntax

```
change system-parameters duplication
```

change system-parameters duplication field descriptions

Field	Description
Enable Operation of PNC Duplication	**y/n**
Enable Operation of IPSI Duplication	**y/n** Defaults to **n** if a gateway exists. If **y**, all fiber-connected PNs must have duplicated IPSIs

display system-parameters duplication

Use **display system-parameters duplication** to see if IPSI (processing element) and PNC (port network connectivity) duplication is enabled. The following must be duplicated:

- Each switch node record and every switch node with its duplicate. Cabinets must be administered.
- Every fiber link containing either an EI circuit pack as an endpoint, or a DS1-C. Fiber links must be administered, including circuit pack administration and then duplication administration.

Every unduplicated SNI (switch node interface) to an SNI fiber link is automatically duplicated.

Note:

Release every PNC-A and -B board from the **busyout** state before PNC duplication, and be sure PNC Duplication is y on the Duplication Related System Parameters screen before you administer duplication. You must obtain a license file to enable this option.

Syntax

```
display system-parameters duplication
```

display system-parameters duplication field descriptions

Field	Description
Enable Operation of PNC Duplication	**y/n** PNC duplication enabled. Displayed when PNC Duplication is y on System-Parameters Customer-Options screen.
Enable Operation of IPSI Duplication	**y/n** IPSI duplication enabled.

system-parameters ip-options

change system-parameters ip-options

Use **change system-parameters ip-options** to modify the IP-OPTIONS SYSTEM PARAMETERS screen. The RTCP Monitor Server Address fields support the IPv6 addresses.

Syntax

```
change system-parameters ip-options
```

See *Avaya Aura®Communication Manager Screen Reference (03–602878)* for more details on the change system-parameters ip-options fields description.

display system-parameters ip-options

Use **display system-parameters ip-options** to display the IP-OPTIONS SYSTEM PARAMETERS screen. The description of the display system-parameters ip-options screen is the same as the change system-parameters ip-options screen. However, the fields in the display system-parameters ip-options sceen are display-only.

Syntax

```
display system-parameters ip-options
```

See **change system-parameters ip-options** for more details.

system-parameters ipserver-interface

change system-parameters ipserver-interface

Use **change system-parameters ipserver-interface** to:

- display the subnet address of the two servers on a duplicated system
- administer the switch identifier
- turn on/off IPSI control of port networks
- turn on/off IPSI preference switching
- set the socket sanity timeout interval
- administer and manage the IPSI QoS parameters

Note:

Run **change system parameters ipserver-interface** before running **add ipserver-interface**.

Syntax

```
change system-parameters ipserver-interface
```

change system-parameters ipserver-interface field descriptions

Field	Description
Server Information	
Primary Control Subnet Address	The control subnetwork addresses typically match the first three groups of digits in the IP address of the server. An asterisk (*) to the right of the Control Subnet Address fields means that Communication Manager does not have the subnetwork information and the subnetwork address displayed is incorrect.
Secondary Control Subnet Address	Select the **configure server** command on the Maintenance Web Interface to see the IP address of the server. The Primary and Secondary Control Subnet Address fields support the IPv6 addresses.
Options	
Switch Identifier	[**A-J**], [**a-j**] The ID letter of the switch Default is **A**.
IPSI Control of Port Networks	**enabled** **disabled**
Preference switching to A-side IPSI	The automatic preference to the A-side IPSI (duplicated IPSIs). • **enable** — If a fault causes an interchange away from IPSI-A to IPSI-B, the system will automatically return to IPSI-A when the fault heals. Changing this field to **disable** stops the automatic return.
IPSI Socket Sanity Timeout	Number of seconds between **3–15** for IPSI connections to recover from a network outage before closing the IPSI signaling connections that result in data loss and port network warm restarts. Default is **3**. When the field is set to a value higher than 3 seconds, the IPSI gateway is less prone to warm restarts and is more resilient to short network outages. Even when set at 15 seconds, IPSI Socket Sanity Timeout accommodates only short control network outages of up to approximately 7 seconds. Resynchronization of the TCP connections between the media server and the IPSI once the network recovers requires additional time. Actual network outages of longer than 7 seconds may still result in IPSI socket sanity timeouts.
QoS Parameters	

Table continues…

Field	Description
802.1p	The value for this field is between **0–7**. The default value is **6**. The value is queued and downloaded to the IPSI board, if you set the value of the Use System QoS values? field to yes on the corresponding change ipserver-interface screen. After you reset the board, the value is downloaded to the IPSI board. If you change the value, the system displays the ipserver(s) must be busied out to effect change message. When you accept the change, PCD stores the updated value. The updated value is displayed on the Systems Parameters IP Server Interface screen, and on the change ipserver-interface screen.
DiffServ	The value for this field is between **0–63**. The default value is **46**. The value is queued and downloaded to the IPSI board, if you set the value of the Use System QoS values? field to yes on the corresponding change ipserver-interface screen. After you reset the board, the value is downloaded to the IPSI board. If you change the value, the system displays the ipserver(s) must be busied out to effect change message. When you accept the change, PCD stores the updated value. The updated value is displayed on the System Parameters IP Server Interface screen, and on the change ipserver-interface screen.

display system-parameters ipserver-interface

Use **display system-parameters ipserver-interface** to display the information for the primary and secondary servers.

Syntax

```
display system-parameters ipserver-interface [ schedule ]
```

schedule Specify a time to run the command.

For field descriptions, see **change system-parameters ipserver-interface**.

system-parameters maintenance

change system-parameters maintenance

Use the **change system-parameters maintenance** command to specify and display scheduled maintenance operations and maintenance support functions. It also activates and

deactivates INADS alarm origination during repairs. Fields on this screen may differ depending on the configuration of the system (duplicated or not).

Syntax

```
change system-parameters maintenance
```

change system-parameters maintenance field descriptions — page 1

Field	Description
Operations Support Parameters	
CPE Alarm Activation Level	Indicates the minimum level (Major, Minor or Warning) to activate Customer-Provided Equipment (CPE) alarm. If the level is none, the CPE does not activate for any alarm. When the switch goes into Emergency Transfer, the CPE alarm activates regardless of the CPE Alarm Activation Level setting.
Scheduled Maintenance	
Start Time	Hour and minute (24-hour notation) when daily scheduled maintenance starts.
Stop Time	The hour and minute when scheduled daily maintenance ceases. If any daily maintenance operations are not completed by this time, the system notes its stopped sequence location and includes those operations during the next scheduled daily maintenance.
Save Translation	Indicates days that translation data in memory automatically saves to the hard disk during scheduled maintenance. The operation saves to disk, then completes a backup to tape. Translation data saves to both servers. If you set the field value as `n` , the system does not save the translations automatically.
Update LSP and ESS Servers When Saving Translations	The values of this field are: • `y` — update the LSP and ESS servers when saving translations • `n` — do not update the LSP and ESS servers when saving translations Enable filesync to Survivable Remote Server and Survivable Core Servers during scheduled maintenance save translations.
Command Time-out (minutes)	Displays the time in which the command times out. The values of this field are in the range 10–360. Enter the number of inactive minutes after which an active SAT screen reverts to a Linux screen or the user is logged off of the system. Default is 120.
Control Channel Interchange	Each port network has a pair of TDM busses (A and B). Each has a set of time slots dedicated to the control channel. One bus at a time carries the control channel in each PN. The values of this field include: • Daily • Days of the week

Table continues…

Field	Description
	• No
System Clocks/IPSI Interchange	The days that interchanges occur. The values of this field include: • Daily • Days of the week • No To prevent interchanges, set the field value to `No`. For high-reliability configurations, there are duplicate IPSIs on IPSI-controlled port networks. For critical-reliability configurations, there are both duplicate Tone-Clock circuit packs on non-IPSI controlled port networks and duplicate IPSIs on IPSI-controlled port networks. When this is turned on, a system clock or IPSI interchange is automatically initiated on each port network possessing duplicated Tone-Clock circuit packs or IPSIs. Each port network interchanges in the standby system clock or IPSI for 20 seconds. During this time the newly-active circuit pack is tested and system health is monitored. Then an interchange is made back to the originally-active circuit pack. This field indicates the days that interchanges occur: daily, days of the week, or no. No prevents interchanges. Does not apply to duplex-reliability configurations since the IPSIs are not duplicated in the port networks.
System Resets	
Display Warning Prior to System Reset?	The values of this field include: • y — displays a warning prior to a system reset • n — does not display any warning prior to a system reset

change system-parameters maintenance field descriptions — page 2

Field	Description
Minimum Maintenance Thresholds (Before Notification)	
TTRs	When the number of touch-tone receivers (TTRs) in service falls below the range 4 to 200, a warning alarm is raised against TTR-LEV. These are also known as dual-tone multifrequency receivers (DTMRs). There are four TTRs on each TN748, TN718, TN420, or TN756; TN2182 and TN744 (suffix C or later) each have eight TTRs. To alarm the first occurrence of a TTR being taken out of service, set this field to the total number of TTRs in the switch.
CPTRs	When the number of call progress tone receivers in service falls below this number (2 to 100), a warning alarm is raised against TTR-LEV. These are also known as general purpose Tone Detectors (GPTDs). There are two CPTRs on each TN748, TN718, TN420, or TN756; TN2182 and TN744 (suffix C or later) each have eight CPTRs. To

Table continues…

Field	Description
	alarm the first occurrence of a CPTR being taken out of service, set this field to the total number of CPTRs in the switch.
Call Classifier Ports	When the number of call classifier ports (CLSFY-PTs) in service falls below this number, a warning alarm is raised against TTR-LEV. Valid entries are 1 to 200. There are eight ports on each TN744 or TN2182 circuit pack. To alarm the first occurrence of a CLSFY-PT being taken out of service, set this field to the total number of CLSFY-PTs. If there are no TN744 or TN2182 circuit packs in the system, leave this field blank.
MMIs	The minimum number of MMI ports needed for the Multimedia Call Handling (MMCH) feature to run efficiently. The MMCH feature must be enabled on the system-parameters customer-options screen before the **MMIs** field can be changed to a number greater than zero. If the number of in-service Multimedia Interface (MMI) ports falls below the minimum port capacity (valid entries between 0–128), a MMI-LEV error is logged. Each MMI circuit pack contains a maximum of 32 ports. To alarm the first occurrence of an MMI being taken out of service, set this field to the total number of MMI ports. If this outage continues for 15 minutes, a major alarm is raised.
VCs	The minimum number of VC ports needed for the Multimedia Call Handling (MMCH) feature. The MMCH feature must be enabled on the system-parameters customer-options screen before the **VCs** field can be changed to a number greater than 0. Each VC circuit pack contains 16 physical ports: eight ports are reserved for VC-DSPPT ports, and the remaining eight ports are designated as VC-SUMPT ports. The eight DSP ports are made up of four encoder and four decoder resources that encode and decode audio formats. Thus, one VC circuit pack is required for every eight ports of MMCH port capacity. If the number of in-service VC ports falls below the MMCH port capacity (valid entries between 0 and 128), a VEC-LEV error is logged. To alarm the first occurrence of a VC port being taken out of service, set this field to the total number of VC ports. If this outage continues for 15 minutes a major alarm is raised.
Terminating Trunk Transmission Test (Extension)	
Test Type 100	Specifies extensions assigned to receive tie-trunk calls from other switches that have test line origination capability. The system responds by sending a sequence of test tones. Test Type 100 tests far-end to near-end loss and C-message by sending: • 5.5 seconds of 1004 Hz tone at 0 dB • Quiet until disconnect; disconnect is forced after the administered timer interval
Timer	When Test Type 100 is administered, you can change the default testing length for the test call in the Timer field.

Table continues…

Field	Description
	The field value range is 65–999 seconds. The default value is 65 seconds. **Note:** When an extension is added for Test Type 100 that is meant for Central Office trunks configured on media module board in an H.248 media gateway, you must increase the timer to 300 seconds for complete test coverage.
Test Type 102	Test Type 102 tests far-end to near-end loss by sending: • 9 seconds of 1004 Hz tone at 0 dB • 1 second of quiet • This cycle is repeated until disconnect; disconnect is forced after 24 hours.
Test Type 105	Test Type 105 tests 2-way loss, gain slope, and C-message and C-notch noise by sending: • 9 seconds of 1004-Hz tone at -16 dB • 1 second of quiet • 9 seconds of 404-Hz tone at -16 dB • 1 second of quiet • 9 seconds of 2804-Hz tone at -16 dB • 30 seconds of quiet • ½ second of 2225-Hz test progress tone • approximately 5 seconds of quiet • forced disconnect
ISDN Maintenance	
ISDN-PRI Test Call Extension	Indicates the extension used by far-end ISDN nodes to place calls to the system, for testing ISDN-PRI trunks between the far end and the system.
ISDN-BRI Service SPID	Shows if the link associates with the Service SPID. If the link is associated with the Service SPID. This number is the test SPID (0–99999) (under BRI-SET MO). Otherwise, this field is blank. Service SPID is a feature used by the system technician to check building wiring between the switch and the BRI endpoint.
DS1 and MF Maintenance	
DS0 Loop-Around Test Call Extension	The extension used to set up a DS0 loop-around connection for testing non-PRI DS1 trunks. Use DS0 Loop-Around Test Call to test DS0 channels associated with non-PRI trunks. Activate the loop-around by dialing the test extension. Establish multiple DS0 loop-around connections by placing multiple calls to the loop-around extension.

Table continues…

Field	Description
	For more information, see the DS0 Loop-Around test section in *Maintenance Procedures for Avaya Aura®Communication Manager, Branch Gateways and Servers* (03–300432).
MF Test Call Extension	Enter the multifrequency test call extension. To allow COs in different locations to use different DID numbers to reach the MF test call extension, administer one number as the MF test call extension. Administer additional DID numbers as x-port stations, and call forward from the x-port stations to the MF test call extension.

change system-parameters maintenance field descriptions — page 3

Field	Description
Maintenance Save Translation Corruption Audit	
Enable Translation Audit	The values of this field include: • y — enables translation audit • n — disables translation audit Set to y to have a translation audit performed prior to every scheduled save translation operation. A translation audit detects corruption in the translation data. y applies when Save Translation on the first page of this screen is y.
Display Warning When Detected	The values of this field include: • y • n Display a warning on the SAT at login if translation corruption is detected by a translation audit. Write the event to the command history log. The default field value is n. Set to y when translation corruption is actively being diagnosed. Displayed when Enable Translation Audit is set to y.
Alarm When Detected	The values of this field include: • y • n Issue an alarm if translation corruption is detected by a translation audit. The default field value is n. Set to y when translation corruption is actively being diagnosed. Displayed when Enable Translation Audit is set to y.
Block Save Translation When Detected	The values of this field include: • y

Table continues…

Field	Description
	• n Block the **save translation** command if corruption is detected. The default field value is n. Set to y when translation corruption is actively being diagnosed. Displayed when Enable Translation Audit is set to y.

display system-parameters maintenance

Use **display system-parameters maintenance** to display translation data for maintenance-related system parameters.

Syntax

```
display system-parameters maintenance [ schedule ]
```

schedule Specify a time to run the command.

A series of maintenance tests and operations runs automatically every day according to the schedule and settings specified in the following fields.

See **change system-parameters maintenance** for field descriptions.

system-parameters port-networks

change system-parameters port-networks

Use **change system-parameters port-networks** to assign port networks to communities and to specify the recovery rules for port networks to return to the main server.

For more details about the change system-parameters port-networks screens and field details, see the 'System Parameters – Port Networks' section in *Avaya Aura®Communication Manager Screen Reference (03–602878)*.

tdm

busyout tdm

Use **busyout tdm** to busyout a specified tdm bus.

Syntax

```
busyout tdm port-network PN# bus
```

port-network *PN#*	TDM bus Port Network number.
bus	Default control/tone bus. (Each 512 timeslot TDM bus configures as 2 duplicate 256 time slot buses. This division allows duplication of control channels and dedicated tone time slots.)

busyout tdm feature interaction

Move dedicated tone time slots to another bus (the other half of the duplicated bus) before you busyout a particular bus.

release tdm

Use **release tdm** to remove specified tdm buses from a maintenance busy state.

For more information, see Busyout and Release Commands.

Syntax

```
release tdm port-network PN# bus
```

port-network *PN#*	Port network number of the TDM bus.
bus	**a** or **b**. Specifies desired half of the TDM bus. Each 512 time slot TDM bus is configured as two duplicate 256 time slot buses. This division allows for duplication of control channels and dedicated tone time slots. The default control bus (carrying the control channel) is the **a** bus, while the default tone bus (carrying dedicated tones) is the **b** bus (1–3).

set tdm

Use **set tdm** to specify which of the paired TDM buses (A or B) on a port network carries the control channel and dedicated tone time slots. Each port network has a 512 time-slot TDM bus

configured as two separate 256 time-slot buses. This division allows for duplication of control channels and time slots dedicated for use by system tones. On power-up, the control channel is carried on the **a** bus, and the tone time slots are carried on the **b** bus. Execution of **set tdm port-network** puts both the control channel and the tone time slots on the specified bus.

Under extremely heavy traffic load, tone time slots on the bus that is not currently carrying the tones may be used for call processing. Use of **override** under these conditions causes calls to be dropped.

See 'TDM-BUS (TDM Bus)' in the *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)* for details.

Syntax

```
set tdm port-network PN# bus [ override ]
```

port-network *PN#*	TDM bus Port Network number. Use **list cabinet** to see port network numbers for a given cabinet.
bus	One of the paired TDM buses, **a** or **b**.
override	Sets a bus which is out of service, or a bus whose dedicated tone time slots are in use by call processing. **Caution:** Use of override option disrupts service.

set tdm feature interactions

New calls go to time slots reserved for tones on the bus that have not other time slots when:

- Time slots on a specified bus are in use
- Dedicated tone time slots are on the other half of the bus

A **set** command to buses that have calls on dedicated tone time slots drops these calls.

Example

```
set tdm  port-network 2 bus a
```

test tdm

Use **test tdm** to run hardware diagnostic tests on the time slots of the specified TDM bus. Both halves (**a** and **b**) of the TDM bus are tested. This command tests all the time slots on a bus associated with a PPN or an EPN.

Syntax

```
test tdm port-network PN# [ long  |  short ][ repeat # | clear ][schedule]
```

port-network *PN#*	Number of the port network to have its TDM bus tested. Both halves (**a** and **b**) of the TDM bus are tested.

long	Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
short	Execute a series of nondestructive diagnostic tests.
repeat #	(Optional) The number of times to repeat the command. The default is 1.
clear	Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.
schedule	Specify a time to run the command.

terminal

erase terminal

Use **erase terminal** to erase local data items from 2410 Release 2 and 2420 Release 4 DCP telephones. A system administrator can use erase terminal to reassign a telephone without having a technician erase the data manually. Erase terminal fails if the extension is busy on a call or on a local task.

erase terminal deletes:

- call logs
- speed dial lists
- button labels
- user option settings
- language

Syntax

```
erase terminal x [ log | customizations | all ]
```

x	Extension number of the telephone.
log	Erase the call log.
customizations	Erase customizations: call log, button labels, speed dial list, user option settings.
all	Erase all data: call log, button labels, speed dial list, user option settings, language.

test-number

disable test-number

Use **disable test-number** to prohibit selected maintenance tests.

Use **enable test-number** to run a disabled test.

Syntax

```
disable test-number number
```

number Maintenance test number.

enable test-number

Use **enable test-number** to re-enable a specified test that was previously turned off with disable test. While disabled, a test cannot be run by background or demand maintenance. Before enabling a test, ascertain why it was disabled, and inform INADS that it has been turned back on.

Use **display disabled-tests** to list all disabled tests.

Syntax

```
enable test-number number
```

number Number of the test to be re-enabled.

Descriptions of each test are displayed under the relevant MO in *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*.

Example

```
enable test-number 102
```

test-schedule

display test-schedule

Use **display test-schedule** to see the test schedule for an S trunk.

Automatic Transmission Measurement System (S) provides advanced maintenance procedures for monitoring system trunk facilities. This system performs transmission tests on system trunks to determine whether trunks are performing satisfactorily.

Syntax

```
display test-schedule
```

display test-schedule field descriptions

Field	Description
Schedule	The current schedule number.
Schedule Time	The hour and minute that the test begins (24-hour time, with 00:00 being midnight). This time must be greater than the current time.
Schedule Date	Month (1 to 12), day (1 to 31), and year on which testing begins (default is the system date). This date must be equal to or greater than the current date.
Schedule Test Days	**y** next to the days of the week indicates which days of the week this test runs.
Interval	The length of this schedule in weeks. If **0**, the schedule runs on the specified days only once.
OTL Throttle	The number of trunk members (1–4) tested concurrently during a schedule. If this field is set to **1**, the OTL (originating test line) tests each trunk sequentially. If set from **2–4**, the specified number of trunks are tested in parallel.
Test Type	One of the following types of test to be performed on the trunk group/ members in this schedule: • **full** — runs the most comprehensive test and collects every associated measurement for each TTL type. • **supv** — performs a supervision test and only confirms the presence of the test set at the far end. No measurements are taken for this test. • **no-st** — runs the full test, but skips any self-test sequences. This saves about 20 seconds on the type 105 test and does not have any effect on type 100 or 102 tests. • **no-rl** — runs the full test, but skips any return-loss sequences. This saves about 20 seconds on the type 105 test and does not have any effect on type 100 or 102 tests. • **no-st/rl** — runs the full test, but skips every self-test and return-loss sequence. This saves about 40 seconds on the type 105 test and does not have any effect on type 100 or 102 tests.
Duration	The maximum number of hours (1 to 24) a schedule can remain active. Schedules continue to run until every trunk group/member for that particular schedule is tested or until the scheduled duration elapses. If the duration elapses before every trunk group/member can be tested, the schedule stops.
Trk Trp	The trunk-group numbers to be tested when this schedule runs. There is no limit to the number of times that a trunk group can be displayed

Table continues…

Field	Description
	on any particular schedule, or to the number of different schedules in which a trunk group can be displayed. Default is blank.
Bgn Mbr	The beginning member number of the trunk group to be tested; default is 1.
End Mbr	The ending member number of the trunk group to be tested. This value must be greater than or equal to the value of the beginning member field.

testcalls

list testcalls

Use **list testcalls** to generate an Automatic Transmission Measurement System (S) report. S allows the voice and data trunk facilities to be measured for satisfactory transmission performance. The performance of the trunks is evaluated according to measurements produced by a series of analog tests (**test analog-testcall**) and are compared against user-defined threshold values. The purpose of the report is to provide measurement data to help determine the quality of trunk lines. The measurement report contains data on trunk signal loss, noise, singing return loss, and echo return loss.

The measurements are produced by a set of analog trunk tests (**test analog-testcall**). The tests are initiated by a maintenance demand test or by a set of scheduled tests. The largest portion of these measurements are generated through scheduled testing during system quiet hours (hours where the traffic volume is low). Each trunk test performed by the system stores the results in a database. The trunk measurements in this database reflect the state of each trunk at the time of its last test.

The test analog-testcall test aborts when attempting a test call on these trunk groups:

- ISDN-PRI: The S Summary Report (**list testcalls** command) shows a **0** in the in the Busied Out Trunks field when **test analog-testcall** is run on an ISDN-PRI trunk.
- SIP
- DID
- Any incoming trunk group (transmission tests can only be run on outgoing trunks).

Syntax

```
list testcalls [ detail | summary ][ grp # ][ to-grp # ][ mem # ][ to-mem # ][ port-location | result-identifier | not-result-identifier | count n ]
```

detail Detailed measurement report displayed.

summary Summary measurement report displayed.

grp # Measurements for a specific trunk group displayed. When used with the to-grp option, this option is the starting trunk group in a range of user-specified trunk groups.

to-grp # Measurements for all trunk groups from 1 to the specified to-grp trunk group are displayed. When used with the grp option, this option is the ending trunk group in a range of user-specified trunk groups.

mem # Measurements for a specific trunk group member displayed. When used with the to-mem option, this option is the starting trunk group member in a range of user-specified trunk group members.

to-mem # Measurements for all trunk group members from 1 to the specified to-mem trunk group member displayed. With mem, this option is the ending trunk group member in a range of user-specified trunk group members.

port-location Measurements for a specific trunk circuit (port) displayed.

result-identifier Filter out the measurement results that do not match the user-specified result. Only measurement results that match the specified result are displayed. Examples of results are pass, marg, fail.

not-result-identifier Filter out the measurement results that do match the user-specified result. Only measurement results that do not match the user specified result are displayed. Examples of results are pass, marg, fail.

count *n* Specify the number of records displayed.

list testcalls detail report field descriptions

Field	Description
Group	Trunk group number selected.
Type	Trunk group type.
Vendor	Vendor of this trunk group.
TTL Type	Kind of test line for this trunk group.
Threshold Values	The list of marginal and unacceptable threshold values defined on the trunk group form. The following fields display on the lower section of the form. Many of the column headings contain the abbreviations **FE** for far end and **NE** for near end. These abbreviations define which end took the measurements.
Trk Mem	The trunk member within the trunk group.
Test Date	The month and day this trunk was tested.
Test Time	The time of day this trunk was tested.

Table continues…

Field	Description
Tst Rslt	This field describes the results of the trunk transmission test.
1004Hz-loss Min	Far-to-near and near-to-far measurements of 1004-Hz loss from low-level tone.
1004Hz-loss Max	Far-to-near and near-to-far measurements of 1004-Hz loss at 0 dBm.
Loss dev at 404Hz	Transmission tests at low frequency. These tests measure a maximum positive and negative deviation of +9 and -9 dB from the 1004-Hz loss measurements.
Loss dev at 2804Hz	Transmission tests at high frequency. These tests measure a maximum positive and negative deviation of +9 and -9 dB from the 1004-Hz loss measurements.
C-msg Noise	Maximum noise interference (in dBrnC: decibels above reference noise, which is B(EQ)10 sup -12E(EQ) watts) terminating on a voice terminal within the voice-band frequency range (500 to 2500 Hz) between 15 and 55 dBrnC.
C-ntch Noise	Maximum signal-dependent noise interference on a line between 34 and 74 dBrnC.
SRL-LO	Singing return loss from 0 to 40 dB between the sum of the circuit (repeater) gains and the sum of the circuit losses. SRL-LO occurs most often in the frequency range of 200 to 500 Hz.
SRL-HI	Singing return loss from 0 to 40 dB between the sum of the circuit (repeater) gains on a circuit and the sum of the circuit losses. SRL-HI occurs most often in the frequency range of 2500 to 3200 Hz.
ERL	Echo return loss from 0 to 40 dB between the level of signal strength transmitted and the level of signal strength reflected. ERL occurs most often in the frequency range of 500 to 2500 Hz.

list testcalls summary report field descriptions

Field	Description
Trk Grp Num	The trunk group number which is being summarized. Only outgoing or two-way analog trunks will be listed.
Num Of Trks	Total number of members per trunk group.
Last Test Date	Date of the oldest measurement in the trunk group.
Last Test Time	Time of the oldest measurement in the trunk group.
Trunks Passed Transm Test	Number of trunks that have passed the trunk transmission tests.
Trunks Failed Marginal Threshld	Number of trunks that failed a marginal threshold, but not an unacceptable threshold according to the threshold values defined on the trunk group form.
Trunks Failed Unaccept Threshld	Unacceptable threshold administered on the Trunk group form.
Trks In-Use	Number of trunks that were in-use at the time of testing.
Trks Not Test	Number of trunks that were not tested due to error conditions.

Table continues…

Field	Description
Busied Out Trunks	Number of trunks that were busied out at the time. This could be due to hardware problems, incorrect threshold values, etc.

tftp-server

change tftp-server

Use **change tftp-server** to copy a firmware image from the FTP file server into Communication Manager memory. The Local Node Name and TFTP Server Node Name fields support the v6 node names.

Syntax

```
change tftp-server
```

display tftp-server

Use **display tftp-server** to see the status of the TFTP Server, and to verify the status of a firmware image file download.

Syntax

```
display tftp-server
```

See **disable suspend-alm-orig**.

time

display time

Use **display time** to display the system date and time.

Syntax

```
display time [ schedule ]
```

schedule Specify a time to run the command.

display time field descriptions

Field	Description
Day of the Week	The day of the week that the system has stored.
Day of the Month	The numerical day of the month.
Month	The month of the year stored by the system.
Year	The current year stored by the system.
Hour	The hour of the current day.
Minute	The number of minutes into the hour.
Second	The number of seconds into the minute stored by the system.

set time

Use **set time** to show and edit the current day, date, month, year and time kept by the system clock. The second field is set to zero when the time on the clock is altered.

Note:

When the system clock is upgraded from an earlier release, the daylight savings time rule on the set time screen defaults to 0 (no rule). When you change the daylight savings time rule, the system clock automatically adjusts during the next transition of the rule.

Syntax

```
set time
```

set time field descriptions

These are the fields on the set time input screen. The current time, or default time is displayed in the fields.

Field	Description
Day of the Week	Valid entries are Monday through Sunday.
Day of the Month	1–31 are valid entries. A check for leap year is also made.
Month	January through December.
Year	The year must be saved as translation data and passed to the kernel whenever kernel memory is corrupted (system reboot or cold I restart), or the data is changed.
Hour	0–23 are valid entries.
Minute	0–59 are valid entries.
Second	This field is reset automatically and cannot be altered.
Type	**Daylight-savings** — daylight savings time **Standard** — standard time
Daylight Savings Rule	The daylight savings time rule number (0 to 15). Rule 0 is no daylight savings time, and rule 1 defaults to U.S. daylight savings time rule.

tone-clock

set tone-clock

On port networks not controlled by an IPSI, use **set tone-clock** to force a Tone-Clock interchange.

On port networks with duplicated Tone-Clocks, use **set tone-clock** to select which of the two Tone-Clock circuit packs is to be active.

On port networks with an IPSI for a Tone-Clock, **set tone-clock** is blocked.

In PNs, the A-carrier Tone-Clock is the preferred Tone-Clock. It is always active unless a failure, maintenance testing, or **set tone-clock** caused an interchange to the B-carrier Tone-Clock. If you use **set tone-clock** during a maintenance session, set the PN Tone-Clock back to the A carrier when you are finished, assuming it is healthy.

Tone-clock interchanges executed by scheduled daily maintenance cause the standby to become active for 20 seconds and then interchange back to whichever Tone-Clock was originally active.

Syntax

```
set tone-clock location [ override ]
```

location Tone/Clock location (cabinet/carrier).

override Executes the set command regardless of the health of the Tone/Clock circuit pack.

Caution:

Use of this option is destructive to an entire port network for PNs.

Example

```
set tone-clock 01c override
set tone-clock a
```

test tone-clock

Use **test tone-clock** to perform hardware diagnostic tests on the three maintenance objects on a specified IPSI, or Tone-Clock circuit pack: TONE-BD, TONE-PT, TDM-CLK.

See the MO information for TONE-BD (Tone-Clock Circuit Pack), TONE-PT (Tone Generator), and TDM-CLK (TDM Bus Clock) in *Maintenance Alarms for Avaya Aura®Communication Manager, Branch Gateways and Servers (03–300430)*.

Syntax

```
test tone-clock location  [ short  |  long ] [ repeat #  |  clear ] [ schedule ]
```

location	Tone/clock location (cabinet/carrier).
short	Execute a series of nondestructive diagnostic tests.
long	Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
repeat #	Number of times to repeat the test, between 1 and 100.
clear	Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.
schedule	Specify a time to run the command.

trace

list trace media-gateway

Use **list trace media-gateway** to trace gateway registration messages and denial events. The **list trace media-gateway** command traces the following registration messages:

- ServiceChangeRequest
- ServiceChangeReply
- NotificationRequest (only Keep Alives)
- NotificationReply (only Keep Alives)

Syntax

```
list trace media-gateway ip-address ip-address | identifier n
```

ip-address *ip-address*	The IPv4 or IPv6 address of the media gateway.
identifier *n*	The number assigned to the media-gateway.

Example

```
list trace media-gateway ip-address 10.10.10.1
list trace media-gateway identifier 23
```

list trace ras

Use **list trace ras** to see the RAS (registration, admission, status) messages that Communication Manager is processing between:

- servers in a Survivable Core Server configuration
- servers in a Survivable Remote Server/Survivable Core Server configuration
- gatekeepers and endpoints

This can be limited to a single station or expanded to the whole system. It shows registration, keepalive, and unregistration requests.

This information is helpful when an endpoint fails to register. For example, use list trace ras for a particular endpoint, then register the endpoint. If no commands are displayed on the output screen, the gatekeeper is not receiving the message from the endpoint. Check for a network problem.

Syntax

```
list trace ras [ ip-address x | ip-stations x | forced_urqs ]
```

ip-address *x* Shows RAS messages between the entity owning the IP address and the recipients of its messages. To monitor registration requests from the Survivable Core Server, use **list trace ras ip-address** to display registration requests from the Survivable Core Server and the associated response from the Main server. The **list trace ras ip-address** command supports the IPv6 addresses.

ip-stations *x* Shows RAS messages between the gatekeeper and endpoints using the extensions specified in the command.

forced_urqs Shows some RAS unregistration request (URQ) messages sent by the gatekeeper to force unregister endpoints. Not all gatekeeper-originated URQ messages are captured here. See the denial event log (display events, category — denial) for a complete record.

list trace station

Use **list trace station** to trace the time and activity on a specific station.

Syntax

```
list trace station ext gw-diag n
```

ext Station extension.

gw-diag *n* Displays a full set of diagnostic information for V.150.1 calls. n is the debug level. If you set n=0, the system displays the default output. If you set n=1, the system

displays a full set of diagnostic information for V.150.1 calls. n= 2 through 255 is reserved.

Use list trace station to check VPI.VCI data for a specific station. Add **/a** after the extension (**ext/a**) to request -specific trace data.

list trace tac

Use **list trace tac** to trace calls entering and leaving the server via a trunk group. To request additional trace data, follow tac# with a slash (/) and then one or more of the qualifiers.

Syntax

```
list trace tac tac# /[ q | d | a ] gw-diag n
```

tac#	Trunk access code number.
q	Requests trace data of QSIG operations, such as diversion, diversion with reroute and path replacement, performed on the specified trunk. QSIG trace data displayed includes reject and invoke information and return errors.
d	Requests trace data on calls made over a specified trunk group.
a	Requests -specific trace data for specified trunk.
gw-diag *n*	Displays a full set of diagnostic information for V.150.1 calls. *n* is the debug level. If you set n=0, the system displays the default output. If you set n=1, the system displays a full set of diagnostic information for V.150.1 calls. n= 2 through 255 is reserved.

Example

```
list trace tac 48
list trace tac *14 / q
list trace tac 284 / d q a
```

list trace vdn

Use **list trace vdn** to trace vdn (Vector Directory Number) operations. Show the next call that enters the VDN, through all vectors, until the call leaves vector processing. **list trace vdn** command resembles list trace vector, except that **list trace vdn** follows the call through multiple vectors.

See *Avaya Call Center Release 4.01 Call Vectoring and Expert Agent Selection (EAS) Guide* for more information.

Syntax

```
list trace vdn vdn#
```

vdn# Vector directory number.

list trace vector

Use **`list trace vector`** to trace vector operations. For a specific vector, see the next call that enters the vector, each vector step being executed, and data for steps associated with Best Service Routing until the call leaves the vector.

See *Avaya Call Center Release 4.01 Call Vectoring and Expert Agent Selection (EAS) Guide* for more information.

Syntax

```
list trace vector #
```

Vector number.

trace-route

trace-route ip-address

Use **`trace-route ip-address`** to trace the route of packets originated from TN IP circuit packs through the LAN. The output shows the IP address of each router or host (hop) that the packets encounter and the time elapsed between each hop. If a TN IP circuit pack has trouble communicating with a far-end device, trace-route can determine how far packets get toward the destination.

TN IP circuit packs include:

- TN799B (or later suffix) C-LAN board
- TN802B Medpro board
- TN2302 IP Medpro board
- TN2602 IP Medpro board

The output screen lists:

- Hops traversed from source to destination
- IP addresses of the hop points and the final destination
- Observed round-trip delay from the source to each hop point

If no reply is received from a potential hop point, **IP Address** contains stars (*), which indicates a timeout condition.

The primary use of trace-route is to determine quickly and unambiguously if the fault lies within Avaya-provided equipment, or if the fault is with the LAN or LAN administration to which the server switch is connected.

Syntax

```
trace route ip-address ip-address | node-name node-name [ board board-location | source source ][ clan-port clan-port ][ schedule ]
```

ip-address *ip-address*	IP address is in the form of*www.xxx.yyy.zzz*
node-name *node-name*	From the node-name screen.
board *board-location*	Cabinet-carrier-slot address of the active (not busied-out) IP circuit pack.
clan-port *clan-port*	Port 1–17 (the port must be translated).
source *source*	An endpoint's virtual port ID.
schedule	Specify a time to run the command.

Note:

The default DiffServ and 802.1p/Q parameters downloaded to an IP Media Processor board are used for **ping** and **trace-route** commands which are sourced from that IP Media Processor. The recipient of a ping replies with the same QoS value found in the received packet, and the measurements reported should reflect the behavior of the type of packets sent. IP Media Processor-sourced pings should reflect audio transport performance and C-LAN-sourced pings should reflect control information transport performance.

Example

```
trace-route node-name sr1clan1 source S00015
trace-route ip-address 123.4.56.789 board 1C14 clan-port 2
trace-route ip-address 2001:0db8:1111:1111:1111:1111:1111:1112
```

trace-route field descriptions

Field	Description
IP Address to trace	Specify a valid IPv4 or IPv6 address.
From Board/Port Location	Specify the source board location.
Source Port ID (IP ENDPOINT)	Specify the source port number of the IP endpoint that you want to ping or trace.
clan-port	Port on the C-LAN board from which **trace-route** is issued. **Note:** If no C-LAN port is specified for trace route on a ppp link, trace route defaults to the Ethernet port (port 17, SAT passed port 0). This field is displayed only if the board is a C-LAN board.

Table continues…

Field	Description
Hop	The node number (in sequence). The 0 node is the address from which trace route is issued.
	Time from the board to each intermediate destination and back in milliseconds. If an error occurs at a node, the entry is repeated with an error code immediately following the time. Error codes and their meanings are: • **!** — Unable to reach port • **!N** — Unable to reach network • **!H** — Unable to reach host • **!P** — Failure between endpoints • **!F** — Need fragmentation of data packet • **!S** — Source return failure • **!X** — Packet blocked by filter • **“** —- Timeout — no data available
IP Address	The 32-bit network address.

trace route error messages

Message	Description
Port not up	Port or link is down
Out of service	RSCL is down
Try later	No socket is available
Ethernet port not translated	Ethernet port is not administered

traffic

monitor traffic

Use **monitor traffic** to see the current load on specified trunk and hunt groups, the number of trunk group and hunt group calls waiting to be serviced, and the length of time that the oldest call in the group has been waiting.

Syntax

```
monitor traffic trunk-group [ starting-group # ]
monitor traffic hunt-group [ starting-group # ]
```

trunk-group Number of calls in the queue waiting to be serviced for each trunk group. The number of members in the group and the number of members active on calls

starting-group # are displayed for comparative analysis. Only administered trunk groups up to a maximum of 60 are displayed.

Use # to specify the starting trunk group. For example, enter 5 to see trunk groups from group 5 and up.

hunt-group starting-group # Shows trunk-group report information plus how long the oldest call in each group's queue has been waiting. Updated every minute. Unadministered hunt groups are blank.

monitor traffic field descriptions

Field	Description
#	Group number for the trunk group or hunt group.
S	The number of members administered for each trunk or hunt group.
A	The number of members in a group that are active on a call. This does not include busied out members.
Q	The length of the queue administered for a group.
W	The number of calls waiting in the group queue to be serviced.
LCIQ	The time, in seconds, the oldest call in the hunt group queue has been waiting to be serviced.

translation

save translation

Use **save translation** to commit the active server translations (volatile) in memory to a file (non-volatile). It either completes or fails. For Linux platforms, the translation file is copied to the standby server by a filesync process.

Note:

save translation can take up to 5 minutes to complete. Do not press **ENTER** key on the keyboard during this time, or result messages will be lost.

For Duplex server pair servers, the translation file is copied to the standby server by a filesync process. On Survivable Core Server, **save translation** changes only on the main server pair.

Syntax

```
save translation [ all | ess | lsp ]
```

all Save translations to all Survivable Core Server, Survivable Remote Server, and the main server pair.

ess From the Server, send changed translations to the active server and to the standby for Duplex server pair servers, and to the Survivable Core Server by a filesync process.

lsp From the Server, send changed translations to the active server and to the standby for Duplex server pair servers, and to the Survivable Remote Server by a filesync process.

All translation data is kept in volatile system memory or on the hard drive during normal operation. In the event of a power outage or certain system failures, data in memory is lost. **save translation** stores on disk the translation data currently in memory.

When a SAT user issues save translation on a duplicated system, translations are saved on both the active and standby servers. If an update of the standby server is already in progress, subsequent save translation commands fail with the message:

```
save translations has a command conflict.
```

save translation will not run and an error message is displayed when:

- translation data is being changed by an administration command
- translations are locked by use of the Communication Manager web interface Pre-Upgrade Step.

Run **save translation** as part of scheduled background maintenance or on demand. See **change system-parameters maintenance** for more information.

save translation field descriptions

Field	Description
Command Completion Status	Identifies the success or failure of the command.
Error Code	Identifier for any error that occurred during translation.

trunk

busyout trunk

Use **busyout trunk** to put an entire trunk group or a single trunk-group member in a maintenance busy state, whether it is installed or uninstalled. Entering only the group number busies out every member in the group.

Note:

You must not enter a group number and a slash (/) without a member number, because it busies-out the member with the lowest-numbered port location.

Syntax

```
busyout trunk group#  [ /member# ]
```

group#	Trunk group number.
member #	Number of particular trunk in a group.

monitor trunk

Use **monitor trunk** to see same information as **status trunk**. **monitor trunk** updates the data automatically every minute, or manually with the **UPDATE** key. The terminal login is not dropped when you press **CANCEL** to cancel **monitor trunk**.

Syntax

```
monitor trunk trunk-group# [ hunt-group# ]
```

trunk-group#	Trunk-group number.
hunt-group #	Hunt group number.

monitor trunk field descriptions

Field	Description
Trunk Group/Member	Trunk group and group member number. (1–99/1–99).
Port	The port location (cabinet-carrier-slot-circuit) for trunks.
Signaling Group ID	If the trunk is ISDN, this field contains the number of the ISDN Signaling Group. Otherwise, this field is blank.
Connected Ports	Port locations (cabinet-carrier-slot-circuit) connected to the trunk.
Service State	In-service/active, in-service/idle, out-of-service, out-of-service-NE (Near End), out-of-service-FE (Far End), maint-NE/active, maint-FE/active, maint-NE/idle, maint-FE/idle, pending-in-service, pending-maint, or disconnected. NE (Near End) and FE (Far End) refer to the end of the trunk that has placed the facility in its current state.
Maintenance Busy	Identifies maintenance testing that occurs on the trunk.
CA-TSC State	The state of temporary signaling connections. (connection set up to pass call information over PRI signaling links).

release trunk

Use **release trunk** to remove specified trunk groups or trunk group members from a maintenance busy state. Specifying the group number releases a single group member and the member number; specifying the trunk group number releases members in a trunk group.

Syntax

```
release trunk group# [ /member# ]
```

group #	Trunk group number
member #	Trunk group member number

status trunk

Use **status trunk** to see information about the current status of a single trunk or of all members of a trunk group. You can also use status trunk to locate facilities with which the trunk is communicating.

Note:

If you use status trunk for a trunk that uses a 1d interface, you receive different information with status trunk on the near end of the trunk from status trunk on the far end of the trunk.

- If you execute **status trunk** on the near end of the trunk, it correctly indicates whether or not the trunk is in a maintenance state.
- If you execute **status trunk** on the far end of the trunk, it never indicates that the trunk is in a maintenance state. This is because the near end is unable to inform the far end of its maintenance state status.

See **monitor trunk**, which shows the same information as status trunk and updates the screen automatically every minute or on demand.

Syntax

```
status trunk group# [ /member#]
```

group#	Status all members of the trunk group.
/member #	Status a specific member of a trunk group.

status trunk field descriptions — page 1

Field	Description
Trunk Group/Member	Group and member numbers of specified trunks.
Port	The location of the port associated with the trunk.
Signaling Group ID	For ISDN trunks, the number of the signaling group to which the trunk group belongs. For other trunk types, the field is blank.
Connected Ports	Locations of ports currently connected to the trunk. **Note:** If a QSIG over SIP trunk call is active on a SIP trunk, the Connected Ports field displays the involved port of the reference trunk. If a QSIG over SIP trunk call is active on a QSIG trunk, the Connected Ports field does not display any ports.

Table continues…

Field	Description
Q-SIP Reference Port	This field works only with the **status trunk** QSIG-group-number/member-number, where QSIG-group-number is the QSIG trunk group number and member-number is the QSIG trunk group member number. If a QSIG over SIP trunk call is active on a trunk, the system displays the Q-SIP Reference Port field, irrespective of the service state. If the QSIG port is inactive, the Q-SIP Reference port field remains bank. **Note:** If the trunk group is not Q-SIP enabled, the Q-SIP Reference Port field is not displayed.
Service State	One of the following states is displayed: in-service/active, in-service/idle, out-of-service, out-of-service-NE (Near End), out-of-service-FE (Far End), maint-NE/active, maint-FE/active, maint-NE/idle, maint-FE/idle, pending-in-service, pending-maint, or disconnected. NE (Near End) and FE (Far End) refer to which end of the trunk has placed the facility in its current state. Explanations of these service states for each type of trunk are displayed in the maintenance object descriptions in the *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers*.
Maintenance Busy	Whether maintenance testing is currently being performed upon the trunk.
CA-TSC State	The status of the call-associated temporary signaling connection, if any. A TSC is a temporary connection set up to pass call information over ISDN-PRI signaling links.
Audio Connection Type	Shows ip-tdm, ip hairpin, ip direct, or ip idle.
Audio Switch Port	Shows a virtual port number (that is, one starting with **T**). If a trunk is in ip-idle state, the Audio Switch Port field is blank.
Media Encryption	Enter **aes** for Advanced Encryption Standard encryption, standard used by U.S. government to protect sensitive (unclassified) information. Reduces circuit-switched to IP call capacity by 25%. Enter **aea** for Avaya Encryption Algorithm. Not as secure as AES. Enter **none** for an unencrypted media stream.

Use **status trunk** to generate a snapshot jitter and packet loss report for a particular trunk-group member.

In this instance, jitter is the variability in the amount of time (in milliseconds) that packets are received over the network. When jitter increases, the user experiences a noisy connection, delays, and a general loss of quality, making speech unintelligible.

If you issue **status trunk** for a non-IP station or the connection is hairpinned or shuffled, then the packet loss and jitter size information (page 2) is not displayed. Refer to *Administering Network Connectivity on Avaya Aura® Communication Manager* for more information.

status trunk field descriptions — page 2

Field	Description
Average Jitter Last Ten Seconds # - more than 255 ms	The average jitter in received packets from the last ten one-second intervals. **#** — more than 255 ms
Packet Loss per Second Last Ten Seconds * - 100% loss	The ten most recent one-second samples of the lost packet information for the requested endpoint. ***** — maximum (100%) packet loss per second during the one-second interval. * is displayed when silence suppression is `y` on the ip-codec-set screen, or when packet loss is 100%.
Out of Order Counter	A count of the number of out-of-order packets detected during the current connection.
SSRC Change for Call	The number of SSRC changes occurring during the current connection.
Last Rx Sequence No.	Last received data packet sequence number.
Last Tx Sequence No.	Last transmitted data packet sequence number.
Worst Case this Call	**Jitter** — the worst-case, 1-second jitter (ms) experienced during the current connection. **Packet Loss** — the worst-case, 1-second packet loss experienced during the current connection.
Average this Call	**Jitter** — the average jitter for the current connection (the running average of all the 1-second intervals during the connection. **Packet Loss** — the average packet loss number for the current connection (running average of all the 1-second intervals experienced during the connection.
Current Buffer Size	The current jitter buffer size.

test trunk

Use **`test trunk`** to perform hardware diagnostic tests on an entire trunk group or an individual trunk-group member, depending on the options entered.

Syntax

```
test trunk group#  [ /member# ] [ short  |  long ] [ repeat#  |  clear ][ schedule ]
```

group # Administered group number.

member # Administered number identifying a particular trunk within a trunk group.

short Execute a series of nondestructive diagnostic tests.

long	Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
repeat #	Number of times to repeat the test, between 1 and 100.
clear	Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.
schedule	Specify a time to run the command.

trunk-group

list trunk-group

For information about **list trunk-group**, see 'Trunk Groups' in *Administering Avaya Aura®Communication Manager (03–300509)*.

tsc-administered

status tsc-administered

Use **status tsc-administered** to see the operational status of temporary signaling connections (TSCs) administered for a specified signaling group.

Syntax

```
status tsc-administered  signaling-group # [ /tsc-index ]
```

signaling-group #	Administered signaling group number.
/tsc-index	TSC number in the signaling group.

Example

```
status tsc-administered 1  / 2
```

status tsc-administered field descriptions

Field	Description
TSC Index	The administered TSC index (1–759).
TSC State	**inactive** — the administered TSC is not functioning (D-channel out-of-service, disabled, etc.). **active** — the administered TSC is up and user information can be exchanged end-to-end. **pending-inactive** — the TSC is being released. **pending-active** — the TSC is about to come up.
Establish	This field pertains to the switch responsible for the origination of the administered TSC. **as-needed** — the TSC is established on an as needed basis. **permanent** — the TSC is permanently established.
Enabled	**y** — indicates that the administered TSCs have been enabled.
Congested	A congested state indicates that the network cannot handle the receipt of USER INFORMATION messages for the administered TSC. • **y** — the administered TSC is congested. • **n** — the administered TSC is not congested. • **clear** — the TSC was congested during its active period and the congestion has been cleared.

test tsc-administered

Use **test tsc-administered** to run diagnostic tests on any type of administered TSCs (Temporary Signaling Connections) on a signaling group. A switched services request to run the TSC heartbeat test is also performed.

Syntax

```
test tsc-administered signaling-group # [ /tsc-index ][ repeat  # ][ schedule ]
```

signaling-group #	Administered signaling group number.
/tsc-index	TSC number in the signaling group.
repeat #	Number of times to repeat the command, between 1 and 100.
schedule	Specify a time to run the command.

test tsc-administered feature interaction

Additional data available after running the test. See **status tsc-administered** for how to access additional data.

tti

status tti

Use **status tti** to see the TTI/PSA status screen and see if the TTI background maintenance task is active. If the TTI background maintenance task is active, the screen shows whether TTI ports are being generated or removed, the number of TTI-supported boards that have processed, and the number of TTI-supported boards that have not yet been processed. The screen also shows the elapsed time since the background maintenance task started.

To activate the TTI background maintenance task, enter y in the TTI field on the Feature-Related System-Parameters screen.

Use **status psa** to also see the TTI/PSA status screen. It shows that the status of PSA is dependent on the state of TTI.

Syntax

```
status tti
```

status tti field descriptions

Field	Description
TTI Background Task State	• **generating TTI ports** • **removing TTI ports** • **suspended** • **not active** • **completed - all ports translated** — The last background maintenance task completed normally • **completed - some ports not translated** — The last background maintenance task stopped when resources were exhausted, and some ports were not translated.
TTI State	**off** — TTI is disabled **voice, data** — the type of TTI ports that are being generated or removed
# of Boards Completed	Number of TTI-supported circuit packs that were processed by the background maintenance task. The ports on a **completed** circuit pack: • if unadministered, were translated as TTI ports • if administered, the administration was removed
# of Boards Left to Process	The number of TTI-supported circuit packs that were not processed by the background maintenance task.

Table continues…

Field	Description
Percent Complete	A ratio of the of number of circuit packs completed to the total number of circuit packs.
Elapsed Time Since Task Started	Elapsed time in hours:minutes:seconds since the TTI background task was started. This field is blank if the task is not active. If the task is completed or suspended, this field shows the elapsed time up to when the job finished or was suspended.

tti-ip-stations

list tti-ip-stations

Use **list tti-ip-stations** to see information on the stations administered as in TTI service.

Stations in TTI service do not show up on the list multimedia ip-unregistered screen.

Syntax

```
list tti-ip-stations
```

user-profile

change user-profile

Use **change user-profile** to change the access permissions of an existing SAT profile. Changes do not affect active SAT sessions, but become effective on new sessions.

The screen name is User Profile. Use **change user-profile-by-category**.

Syntax

```
change user-profile n
```

n Profile number (20–69).

See **add user-profile** for field descriptions.

display user-profile

Use **display user-profile** to display the permissions of an existing SAT profile.

The screen name is User Profile. Also use **display user-profile-by-category**.

Syntax

```
display user-profile n
```

n Profile number (20–69)

display user-profile field descriptions, page 1

Field	Description
User Profile Name	The user-defined profile name, up to 40 characters.
Shell Access	**y/n** **y** — users assigned this profile are able to execute **go shell** from the SAT. This does not affect the user's default login shell in Linux.
Facility Test Call Notification	**y/n** **y** — users assigned this profile receive notification at logoff if Facility Test if Notification is still administered. For security, set to **y** for all profiles.
Acknowledgement Required	**y/n** **y** — users assigned this profile must acknowledge that they want to logoff while Facility Test if Notification is still administered.
This profile is disabled	**y/n** **n** — the profile is active **y** — the profile is disabled If changed to **y**, an existing active login using this profile is unaffected, but any new attempted session using this profile fails. • A login via CLAN receives `access denied`. • A login via Linux receives an error return code with the message `access denied` displayed via stderr.
Grant un-owned Permissions	**y/n** **y** — If this profile has write access to the user-profile form, users with this profile can grant any permission allowed for profile 18 (customer super user) to other profiles even when this profile does not itself have those permissions. **n** — users may not grant permissions they themselves do not have.
Extended Profile	**y/n**, default is **n**

Table continues…

Field	Description
	y — extended profile is enabled. If **y**, the profile has additional access restrictions to the station and vector forms.
Name	Category name. Each category is associated with a unique set of SAT screens. A given object (SAT screen) displays in one category.
Cat	Category.
Enbl	**y/n** **y** — enable the category for this user-profile. Category displays **y** when any object in a category has permissions other than **- -**. **n** — disable the category for this user-profile. Category displays **n** only when all objects in the category have permissions **- -**. • If the field is changed from **n** to **y**, permissions for all objects assigned to the category are set to **w--**. • If the field is changed from **y** to **n**, permissions for all objects assigned to the category are set to **--**. This field also reflects the settings on pages 2 - x of this screen.

display user-profile field descriptions, page 2 – x

Field	Description
Set Permissions for Category _ to –	Set permissions for only the objects assigned to this specific category. 1. Enter a letter to specify the category to set. 2. Enter the permission. • Set permission entries as read/write for administration and yes/no for maintenance. • A blank character indicates no-change. For example, if the permissions field is set to blank **-**, all affected objects are set to deny maintenance access but the current access for administration for each object in this category remains unchanged. See the field description for Perm for more details.
Set All Permissions to	Set permissions for all objects in all categories.
Cat (category)	Display only. Letter that corresponds to the category, used for sorting alphabetically by category, as opposed to alphabetically by SAT form command object.
Perm (permissions)	Enter a two-character value, including blank. Set permission entries as deny, read/write for administration and deny, yes/no for maintenance. • The first character specifies access for administration. - **- (dash)** — deny. No access.

Table continues…

Field	Description
	- **r** — view only. - **w** — add, change, remove in addition to view. • The second character specifies access for maintenance. - **- (dash)** — deny. No access to maintenance commands. - **m** — access to maintenance commands. Setting this field to **m** requires at least read access for administration. - For example, • **r-** — a user with this profile can use the commands read, display, export, status, and list for the object assigned the **r-** permission, and no others. • **wm** — grants full access for all commands to the object assigned this permission A blank character indicates no-change. For example, if the permissions field is set to blank **-(dash)**, all affected objects are set to deny maintenance access but the current access for administration for each object in this category remains unchanged. All permission fields on the User Profile pPage 2 – x accept the full range of values (**r**, **w**, **d**) or (**w**, **m**) Independent of whether all values apply to the field or not. Settings on these pages are reflected on the Enbl field on page 1 of this screen.
Name	Name of the SAT screen by command object. Display only.

duplicate user-profile

Use **duplicate user-profile** to duplicate an existing SAT profile. **duplicate user-profile x** copies the permissions from profile **x** to a new profile.

Syntax

```
duplicate user-profile x
```

x Number of an existing SAT profile greater than 17.

export user-profile

Use **export user-profile** to export SAT profile files for editing in a program such as Microsoft Excel.

When **export user-profile** is entered, SAT profiles in Communication Manager numbered 20–69 are written to `/var/home/ftp/pub/cmprofiles.txt`. If the file already exists, it is deleted and replaced.

Syntax

```
export user-profile
```

export user-profile file field descriptions

Field	Description
Fields from User Profile screen, page 1	
first line	Current release
second line	Number of profiles being exported
next lines - x	Profile number and name of the profile, for as many profiles as exist
next line	Profile number and a list of existing SAT profile numbers in ascending order starting with the first existing number after profile 19.
Fields from User Profile screen, pages 2 - x	
remaining lines	Two columns: • category and feature names as they display on the user-profile forms • object permissions for each profile number

export user-profile error messages

Error Message	Description
/var/home/ftp/pub/cmprofiles.txt create error (the actual file name from the ecs.conf variable cm_profile_export_file)	The file cannot be created.
/var/home/ftp/pub/cmprofiles.txt write error (the actual file name from the ecs.conf variable cm_profile_export_file)	The file cannot be written.

import user-profile

Use **import user-profile** to import SAT profiles numbered 20-69 from the `/var/home/ftp/pub/cmprofiles.txt` file to Communication Manager. You can edit SAT profile information in Microsoft Excel and import the information back into Communication Manager.

- If a profile in the file does not exist in Communication Manager, it is created.
- If a profile in the file already exists in Communication Manager, the profile in Communication Manager is overwritten.
- If profiles exist in Communication Manager that do not exist in the file, they remain in Communication Manager unmodified.

Use **status logins** to see SAT profile assignments.

Syntax

```
import user-profile
```

import user-profile error messages

Error message	Description	Result
Note: In the following text, the file `/var/home/ftp/pub/cmprofiles.txt` shall be replaced by the actual file name from the `ecs.conf` variable `cm_profile_export_file`.		
/var/home/ftp/pub/cmprofiles.txt does not exist and the import aborted.	The file does not exist.	The import is aborted.
var/home/ftp/pub/cmprofiles.txt not readable	The file is not readable.	The import is aborted.
release mis-match	The first line of the file does not contain a release number that exactly matches the release number of Communication Manager.	The user is prompted as to whether or not to continue. Additional checks will prevent corruption and cannot be overridden.
invalid profile identifier in file var/home/ftp/pub/cmprofiles.txt	The file contains a profile number lower than 20.	The import is aborted.
invalid feature name at line xxx in var/home/ftp/pub/cmprofiles.txt *xxx* — the file line number where the first error is found.	The feature names do not exactly match in spelling, order and number the existing profile forms in Communication Manager.	The import is aborted.
invalid permissions at line xxx in var/home/ftp/pub/cmprofiles.txt	The feature permissions characters are not valid.	The import is aborted.

list user-profiles

Use **`list user-profiles`** to see existing SAT profile numbers and profile names in numerical order.

Use **`status logins`** to see SAT profile assignments.

Syntax

```
list user-profiles
```

list user-profile field descriptions

Field	Description
Profile	Profile number
Extended Profile	**y/n**

Table continues…

Field	Description
	y — the Extended Profile field is `y` on the User Profile (add user-profile) screen.
User Profile Name	Avaya-defined name for Profile numbers 0–19. Customer-defined name for Profile numbers 20–69.

remove user-profile

Use **remove user-profile** to remove an existing SAT profile and its extended profile, if one exists.

When **remove user-profile n** is executed, the selected profile is displayed. Submit the form to remove the profile.

When a profile is removed, SAT sessions using the profile are automatically logged out.

Syntax

```
remove user-profile n
```

n Profile numbers 20–69.

user-profile-by-category

add user-profile-by-category

Use **add user-profile-by-category** to add a new SAT profile and administer permissions, where n is the profile number 20-69.

Pages 2 - X contain a list of SAT forms in order by category and alphabetically within category, and the type of access granted to or denied this profile.

The screen name is User Profile.

Set permission entries as read/write for administration and yes/no for maintenance. Also use **add user-profile**.

Syntax

```
add user-profile-by-category
```

For field descriptions, see **add user-profile**.

change user-profile-by-category

Use **change user-profile-by-category** to change the access permissions of an existing SAT profile. Changes do not affect active SAT sessions, but become effective on new sessions.

Pages 2 - X contain a list of SAT forms in order by category and alphabetically within category, and the type of access granted to or denied this profile.

The screen name is User Profile. Also use **change user-profile**.

Syntax

```
change user-profile-by-category n
```

n Profile number (20–69).

See **add user-profile** for field descriptions.

display user-profile-by-category

Use **display user-profile-by-category** to display the permissions of an existing SAT profile.

Pages 2 - X contain a list of SAT forms in order by category and alphabetically within category, and the type of access granted to or denied this profile.

The screen name is User Profile. Also use **display user-profile**.

Syntax

```
display user-profile-by-category n
```

n Profile number 20–69.

See **add user-profile** for field descriptions.

val

reset val

Use **reset val** to perform a software reset of every administered port on the circuit pack. **reset val** performs the same functions as **reset board**, but overrides querying the board to determine whether an announcement autosave is in process. This allows resetting the circuit pack if it is in the insane state.

Syntax

```
reset val  location
```

location Reset every administered port on the circuit pack.

val-ip

status val-ip

Use **status val-ip** to generate an IP-related status report about the specified VAL circuit pack's LAN connection.

Syntax

```
status val-ip location
```

location Location of the circuit pack.

video-bridge

status video-bridge

Use **status video-bridge** to view the status of the video bridge.

Syntax

```
status video-bridge number
```

number Video bridge number.

status video-bridge field descriptions

Field	Description
Name	The name configured on the video-bridge screen
Bridge Status	• **in-service** — the bridge is available • **low-resources** — the bridge is heavily loaded, but available • **call-rejected** — the last conference attempt failed • **no-resources** — the bridge has not reported any resources

Table continues…

Field	Description
	• **trunks-busy** — the configured trunks for this bridge are all full or busied out. Check trunk status • **out-of-service** — check signaling group status **Note:** Typically, CM does not use the low-resources and call-rejected bridges. However, if the in-service bridge is unavailable, CM uses the low-resources or call-rejected bridge.
Ports Used	The number of call-legs administered on the video bridge form which CM uses.
Network Region	The network region used to assess the bandwidth requirements of the bridge.
PRIORITY CONFERENCE STATUS	The resources available for priority users (see Class Of Service settings)
Call Rate	The allowed bandwidth usage for the call-legs to a bridge. • Maximum — bandwidth up to the reported rate. • Exact — bandwidth of the reported rate.
Ports Available	The available ports reported by the bridge. **Note:** The available ports are bridge dependent and may not match with the CM configuration or the number of endpoints in the conferences, especially if the bridge is supporting multiple CMs.
Conferences Available	The available conferences are reported by the bridge. **Note:** The available conferences are bridge dependent and may not match with the CM configuration or the number of conferences underway, especially if the bridge is supporting multiple CMs.
Ports Rsvd per Conf	The number of ports on the bridge that a new conference takes up.
Conference Failure Rate	The number of conferences reverted to the audio-only mode. **Note:** Typically, conferences are reverted to the audio-only mode if one or more call-legs to the video bridge are dropped.
Participant Failure Rate	The number of participants who are unable to dial in to the bridge. **Note:** If a participant is unable to dial in to the bridge, the call-rejected status is displayed. This status continues to display till the participant is able to make a call successfully.

Chapter 3: Linux bash commands

Introduction

Linux platform commands are executed from the bash shell. These commands provide server information and help troubleshoot problems in the switch and other components.

Linux commands can be found in **/opt/ecs/bin** and **/opt/ecs/sbin**. The user must be logged into the switch as **root** to execute certain bash commands.

Use **-?** to see a description of command options. For example, `fasttop –?` displays the options that can be entered for the `fasttop` command.

acpfindvers

Use **`acpfindvers`** to display the release string, date, and time for an object located in **/opt/ws** and in which software base the object was built. More than one file can be specified on the command line.

Syntax

```
acpfindvers  [ -? ] [ -c ] file1 [file2] ...
```

-?	Display the command option descriptions.
-c	Display only the CDA vintage string for the file(s)
file1 [file2] ...	Display the information for the specified files..

Example

```
acpfindvers pcd
```

almcall

Use **`almcall`** to:

- set or display the telephone numbers to services
- enable or disable alarm abbreviation on those numbers
- set the interval between retries

Syntax

```
almcall [ -f first-number ] [ -a [y|n] ] [ -s second-number ] [ -b [y|n] ] [ -t timer ]
[ -i interval ] [ -? ]
```

-f *first-number*	Set the first dial-out number to **first-number**. The number can have up to 30 digits (0–9) and “,” for pause. Dashes are allowed but are ignored.
-a *[y | n]*	Set alarm abbreviation on (y) or off (n) for the first telephone number. The default is y.
-s *second-number*	Set the second dial-out number to **second-number**. The number can have up to 30 digits (0–9) and “,” for pause. Dashes are allowed but are ignored.
-b *[y | n]*	Set alarm abbreviation on (y) or off (n) for the second telephone number. The default is y.
-t *timer*	Set the alarm abbreviation timer to the **timer** value. Valid values are between 1 and 24 hours. The default value is 4.
-i *interval*	Set the interval between retries in minutes. The interval range is between 1 and 20 minutes. The default is 7 minutes. The value 0 is ignored.
-?	Display the command usage.

Description

almcall with no arguments displays the dial-out numbers, alarm abbreviation, timer, and interval information.

---

almclear

Use **almclear** to clear specific server alarms, a list of server alarms, or all server alarms within a range. An alarm is referenced by a positive integer called the Alarm ID, which can be found using the **almdisplay** command. **almclear** does not clearCommunication Manager alarms.

Syntax

```
almclear  [ -a ] [ -n [id | id1, ids1,...idn | idn1-idn]] [ -? ]
```

-a	Clear all outstanding server alarms.
-n *id*	Clear a single server alarm with Alarm ID *id*.
-n *id1, id2, ... idn*	Clear a set of server alarms with Alarm ID numbers *id1, id2, ... idn*. **almclear -n 1, 2, 3** is a valid command. **almclear -n 1 2 3** is not.
-n *id1–idn*	Clear a range of server alarms from ID number *id1* to ID number *idn*
-?	Display the usage statement.

almdisplay

Use **almdisplay** to display the list of outstanding messaging, Communication Manager, and server alarms.

Syntax

```
almdisplay  [ -v ] [ -? ]
```

-v Display the description contained in the original alarm string in addition to the outstanding alarms.

-? Display the usage statement.

Description

almdisplay with no options displays the outstanding alarms.

almdisplay field descriptions

Field	Description
ID	Lists the unique Alarm ID assigned to each alarm.
MO	Name of the Maintenance Object that was alarmed.
Source	Displays the abbreviated name of the source which generated the alarm.
On Bd	Display **y** if the problem is on-board, **n** if the problem is off-board.
EvtID	Displays the Event ID of the alarm. The Event ID identifies a particular event that occurred on a given source that generated the alarm.
Lvl	The severity level of the alarm: Warning (WRN), Minor (MIN), Major (MAJ).
Ack	Displays Y or N, indicating if the alarm has been acknowledged or not.
Date	The time stamp assigned when the alarm was created.

almenable

Use **almenable** to enable or disable dial-out and SNMP alarm origination.

Syntax

```
almenable [ -d [n] ] [ -s [y|n] ] [ -? ]
```

-d *n* Set the dial-out alarm origination to **neither** (default). Disable alarming dial-out. Alarm Origination does not occur, reports are not sent to either OSS number.

-s *y|n* Enable (y) or disable (n) alarming through SNMP. The default is y.

-? Display the usage statement.

almnotif

Use **almnotif** to set the alarming strategy for dial-out.

Syntax

```
almnotif  [ -r [y|n] ] [ -c [y|n] ] [ -? ]
```

-r *y|n* Enable (y) or disable (n) restart notification.

-c *y|n* Enable (y) or disable (n) clear alarm notification.

-? Display the usage statement.

Description

almnotif with no options display the administration for restart notification and clear alarm notification.

almsnmpconf

Use **almsnmpconf** to administer or display administered information for SNMP alarming to a services organization.

Syntax

```
almsnmpconf   [ -d IP ] [ -c community ] [ -b [y|n] ] [ -e [y|n] ] [ -add | -del | -mod ]
[ -? ]
```

-d *IP* Set the IP address *IP* to send SNMP traps.

-b *y|n* Enable (y) or disable (n) alarm abbreviation for SNMP.

-e *y|n* Enable (y) or disable (n) the trap destination.

-add Add a new trap destination. A valid IP address is required.

-del Remove the trap destination. A valid and existing IP address is required.

-mod Modify an existing trap destination. To modify an IP address, the trap destination must first be deleted, then re-added with the modifications.

-? Display the usage statement.

almsummary

Use **almsummary** to display a summary of outstanding Major and Minor alarms against Communication Manager, Messaging, and servers.

Syntax

```
almsummary  [ -? ]
```

-? Display the usage statement.

almsuppress

Use **almsuppress** to suppress/unsuppress alarm origination or to check the state of alarm suppression. Use this command to stop alarms during troubleshooting operations.

Syntax

```
almsuppress [ -s [y|n] ] [ -t minutes ] [ -? ]
```

-s *y|n* Suppress (y) or unsuppress (n) alarm origination for 30 minutes. The default is y.

-t *minutes* Number of minutes to suppress alarm origination, where *minutes* is in the range of 30–120. The default is 30 minutes.

-? Display the usage statement.

authtype

Use **authtype** to verify if a login is authenticated with a password or Access Security Gateway (ASG).

Syntax

```
authtype   [ -l ] [ -u login-name ] [ -h | -? ]
```

-l Return status of the ASG lock.

-u *login-name* The *login-name* to check.

-h | -? Display the usage statement.

autosat

Syntax

```
autosat
```

Use **autosat** to run a Communication Manager SAT (System Access Terminal) session.

cmpasswd

Use **cmpasswd** to create or change a login password.

Syntax

```
cmpasswd username
```

username	The login to create or change.
-?	Display the usage statement.

cmuseradd

Use the **cmuseradd** command to add an administrator account.

Syntax

```
cmuseradd <type>  [ -C profile ] [ -P key ] [ -p password ] [-S Limit] username
```

type	The type of account that you want to add: • super-user • nonsuper-user • cm-only • remote
-C *profile*	The profile for the account that you want to add. You must assign a profile to the account of type **cm-only**. However, do not assign a profile to the account of type **remote**.
-P *[key]*	An ASG-authenticated account. If you do not specify the key on the command line, the system generates the key. Do not use this parameter with *-p*.
-p *[password]*	A password-authenticated account. *password* is the encrypted password. Do not use this parameter with *-P*. The *-p* parameter requires an encrypted password. Therefore, you can use the **cmuseradd** command without the *-p* parameter, and then use **cmpasswd** to set the password.

-S *Limit* The limit for the number of concurrent SAT sessions. You can assign up to five concurrent sessions or retain the default value none. If you retain the default value, the restriction on the number of concurrent sessions does not apply to the login. However, the restriction applies to the system.

Examples

```
cmuseradd super-user username
cmuseradd cm-only -C 20 username
cmuseradd cm-only -C 20 -S 3 username
```

cmuserdel

Use the **cmuserdel** command to delete an administrator account. This command replaces the SAT command `remove login`.

Note:

If you delete an account, the system removes the restriction on the number of concurrent sessions for the account.

Syntax

```
cmuserdel username
```

username The account to delete.

cmusermod

Use the **cmusermod** command to modify an administrator account.

Syntax

```
cmusermod [ -C profile ] [ -P key ] [ -p password ] [ -S Limit] [-L] [-U] ]-G
<group0>,...,<groupN>] username
```

-C profile The profile for the account. You must assign a profile to the account of type **cm-only**. However, do not assign a profile to the account of type **remote**.

-P *[key]* An ASG-authenticated account. If you do not specify the key on the command line, the system generates the key. Do not use this parameter with *-p*.

-p *[password]* A password-authenticated account. *password* is the encrypted password. Do not use this parameter with *-P*. The *-p* parameter requires an encrypted password. Therefore, you can use the **cmuseradd** command without the *-p* parameter, and then use **cmpasswd** to set the password.

-L	Lock the account. You must not use this parameter with *-U*.
-U	Unlock the account. You must not use this parameter with *-L*.
-G *<group0>,...,<groupN>*	A secondary group list. The system accepts the group names on the `profN` screen as Communication Manager profile groups.
-S *[Limit]*	You can assign up to five concurrent sessions or retain the default value none. If you retain the default value, the restriction on the number of concurrent sessions does not apply to the login. However, the restriction applies to the system.

corevector

Syntax

```
corevector  [-l] [-s [-f]] [-c arg] [-?]
```

-l List the current settings.

-s [-f] Set [f = force] the core dump vector using the arguments noted for the *-c* option.

-c Clear the core dump vector using the following options:

- `all` - coredump files on all Communication Manager restarts.
- `warm` - coredump on warm restart request.
- `cold2` - coredump on cold2 restart request.
- `reload` - coredump on reload (reboot) restart request.
- `insane` - coredump on system insane condition.
- `single` - coredump on single process restart and killing of TERMINAL processes.
- `trap` - coredump of process that trapped.

-? Display the usage statement.

Description

`corevector` is used to request or clear coredump requests. The core dump files are generated prior to the execution of the restart requested. After the core files are taken, a reload of Communication Manager processes is executed. Specifying a single process restart will also create a core file for terminal processes, e.g., map.

When the core files are to be taken, the state of health is lowered to force a server interchange. The system then waits to allow the interchange to occur (all processes are stopped), checks to ensure the standby server is now active, and generates the core files. The core files are only taken on the ACTIVE server unless the -f (force) option is specified.

In a simplex server configuration, the *-f* option is necessary.

corevector accepts multiple arguments, for example, **corevector**-s warm cold2

custalmopt

Syntax

```
custalmopt   [ -d ] [ -m ] [ -a ] [ -h | -? ]
```

-d	Display the current settings.
-m	Report Major/Minor alarms only.
-a	Report all alarms.
-h | -?	Display the usage statement.

Description

custalmopt sets or displays the current customer alarm option report option. This command runs on the active server only, and Communication Manager must be running.

defsat

Syntax

```
defsat
```

Description

Use **defsat** to invoke a Communication Manager SAT session if the incoming TCP port is 5022 or 5023.

dhelp

Syntax

```
dhelp [ command ] [ -? ]
```

command	Name of the shell command or first character(s) of command.
-?	Display the command option descriptions.

Description

Enter **dhelp** to display the list of valid Linux commands.

Enter **dhelp** *command* to display the command options and descriptions for a particular command, such as **dhelp** *server*.

disp_dup_log

Syntax

```
disp_dup_log  [ --hour | -h ] [ --day | -d ] [ --help | -? ] [ #_of_entries ]
```

--hour | -h	Display the hourly duplication measurements.
--day | -d	Display the daily duplication measurements.
--help | -?	Display the usage statement.
#_of_entries	Number of entries to display.

Description

Display logs from the duplicate server.

displaydenialevents

Syntax

```
displaydenialevents [-?]
```

-?	Display the usage statement.

Description

Display the denial events in Communication Manager log files, including the event description.

dkill

Syntax

```
dkill   [-def] [-a] [-h] [ <proc1> [<proc2>...]]
```

-def	All Communication Manager (defty) processes.
-a	All processes.
-h	Display the usage statement.
<proc1> [<proc2>]	Kill only this process or list of processes.

Description

Use **dkill** to send a kill signal to processes in Communication Manager. This command is generally used with the **-a** option (all) when a system is caught in a state where the **stop all** command failed.

---

dsat

Syntax

```
dsat  [ -h | -? ] [path]
```

-h | -? Display the usage statement.

path Path to a directory containing a SAT executable.

Description

Use **dsat** to run a Communication Manager SAT session. Use **sat path** to use an alternate SAT executable, where *path* is the path to the directory containing the SAT executable.

---

environment

Syntax

```
environment  [ -v ] [ -? ]
```

-v Turn on verbose mode.

-? Display the usage statement.

Description

Use **environment** to display reports for environmental sensors such as temperature, fan speed, and voltage.

---

fasttop

Syntax

```
fasttop  [-D] [-L] [-M] [-h | -?] [-o filename] [-d delay] [-c #] [-n lines]
```

-D Query the HMM overload information.

-L Do not track threads.

-h | -? Display the usage statement.

-o filename	Put the output in the specified filename.
-d delay	Display the results every *delay* seconds. The default is 5.
-c #	Number of ticks between looking at /proc.
-n lines	Display the number of lines specified by *lines*.

Description

Use **fasttop**to see occupancy results for Communication Manager processes running on the server. The default screen refresh is 5 seconds.

To exit the command, enter `quit`.

---

filesync

Syntax

```
filesync  [-w] [-s | -f | -t | -i | -d | -e | -v] [-Q <TYPE> [NUM]] [-r <TYPE>] [-a
<TYPE> <ipaddr>] [-q | -H <TYPE>] [ filegroup ]
```

Description

Use **filesync** to request synchronization of files from active to standby server(s). You can:

- Specify all files or sets of files.
- Define the type of synchronization.
- Enable, disable, or temporarily inhibit file synchronization.
- Report synchronization status and history.

File synchronization sends translations to a duplicate server, a standby server, or a survivable remote server. File synchronization may take place because of survivable remote server registration or with the following commands:

- **filesync trans** (sends translations to the standby server or the survivable remote servers)
- **loaddisplang** (sends unicode files to the standby server and the survivable remote servers)
- **loadlicense** (sends the license file to the standby server).
- **loadpwd** (in this instance, sends the password files to the standby server and the survivable remote servers).
- **save_trans** (sends translations to the standby server).
- **save_trans lsp** (sends translations to the standby server and the survivable remote servers).
- **server -i** (sends all synchronized files to the standby server before the interchange).

filesync command options

Option	Option description
`-w` *filegroup*	Wait for results. Specify *filegroup*, or *all* for all groups.
`-s` *filegroup*	Run the file synchronization silently. The exit status is the only indication of success or failure. Specify *filegroup*, or *all* for all groups.
`-t` *filegroup*	Timestamp-based synchronization for the specified filegroup to the duplicate server. Verify the timestamps on all files in the specified sets, and synchronize the file/remote server when: • the file's timestamp is more recent than the last synchronization. • the last synchronization attempt for the set failed. *-t* is more efficient on the active server. It ensures that if the file is changed locally, it will be synchronized to the other server(s). **`filesync -t`** will not correct a corrupted file on the other server. Specify *filegroup*, or *all* for all groups.

`-i`	Inhibit file synchronization temporarily. This command will not exit if given this option, so it should be run in the background as follows:
	`filesync -i&`
	`fs=$!`
	`***other processing ***`
	`kill-HUP $fs`

`-d`	Disable file synchronization. No files will be synchronized to or from this server until an enable is given. The disable state persists across Communication Manager restarts and Linux reloads.
`-e`	Enable or re-enable file synchronization.
`-v`	Turn on verbose mode. Use with -Q queries.
`-q` *filegroup*	Query the status and receive a summary of the most recent synchronization, and synchronize the requested filegroup. Implies *-w*, wait for a response before returning. Specify *filegroup*, or *all* for all groups.
`-a <TYPE> <ipaddr>` *filegroup*	Send files to a server of <TYPE> **ESS** or **LSP** at the specified IP address. Specify *filegroup*, or *all* for all groups.
`-Q <TYPE> [NUM]`	Query the status of the translation synchronization number [NUM] to the specified servers of type <TYPE>. Display the status for save trans, filesync trans, or nightly maintenance. The default synchronization number is the most recent synchronization. Server <TYPE> may be `dup`, `ess`, `lsp`, or `all`.
`-H <TYPE>`	Show the history of the last 25 translation synchronizations to specified server types. Displays the history for save trans, filesync trans, or nightly maintenance. Server <TYPE> may be `dup`, `ess`, `lsp`, or `all`.
`-r <TYPE>`	Send files to the duplicate server and remote servers of a specified type. Server <TYPE> may be `dup`, `ess`, `lsp`, or `all`.

filesync exit codes

If an error occurs, an explanation of the error is sent to stdout. If the command is successfully sent and any response is received, a description of the status is displayed.

Exit Code	Explanation
0	Successful
2	Synchronization is in progress.
3	Synchronization is currently inhibited or disabled.
4	Pre-script execution returned non-zero status.
5	Post-script execution returned non-zero status.
6	Request was invalid (such as an invalid set name).
7	An error occurred during file synchronization.
8	A local error occurred.

ftpserv

Syntax

```
ftpserv  [-? | -h] [-l] [-o] [-a] [-q] -s ftp [on | off]
```

-l	Lists the services supported by this command.
-o	Display only the services name, not the description.
-a	Display the “active” state of the service.
-q	Query for the state of the service.
-s ftp [on | off]	Enable (on) or disable (off) ftp service.
-? | -h	Display the usage statement.

Description

Use **ftpserv** to configure ftp access and service. This command works when the user is logged in as root or with **sudo** (i.e., **sudo ftpserv**).

fwdlreason

Syntax

```
fwdlreason  [ -a ] [ -c code ] [ -? ]
```

-a	Display the list of all reason codes
-c *code*	Display the reason for a specific *code*.
-?	Display command option descriptions.

Description

Use **fwdlreason** to see reason codes for firmware download failures.

---

hardware_info

Syntax

```
hardware_info  [ -D <delimter> ] [ -W <keyword> ] [-l] [-v] [-w] [-h] [-?]
```

-D <delimiter>	User-defined delimiter for the -w option.
-W <keyword>	Get a particular value.
-l	List the valid keywords for the -W option.
-v	Turn on verbose mode and display all system hardware information.
-h | -?	Display the usage statement.

Description

The **hardware_info** command display the hardware configuration for a server or virtual machine.

Example

```
hardware_info -w [ -D <delimiter> ][ -v ]
hardware_info -W <keyword> [ -v ]
hardware_info -w [ -v ]
hardware_info -l
```

---

listhistory

Syntax

```
listhistory  [-l] [-f filename] [-?]
```

-l	Lists the names of the existing command history log files.
-f *filename*	Specifies which command history log file.
-?	Display the command usage.

Description

Use **listhistory** to list the Communication Manager shell commands which alter system administration or environment. **listhistory** displays the most recent command history log file.

loaddisplang

Syntax

```
loaddisplang   [-? | -h]
loaddisplang  [-q] [-c] [-C] [-s] [-S] [-d] [-f] [filename]
loaddisplang  -i[c|s] [d]] [filename]
```

-c Operate on all custom non-installed telephone message files.

-C Operate on all custom installed telephone message files.

-s Operate on all standard non-installed telephone message files.

-S Operate on all standard installed telephone message files.

-d Indicates the file in question is user-defined (omission implies default of unicode file).

-f Indicates the file in question is non-installed telephone message files.

-i Install a unicode or user-defined file. With no file specifiers, will install all valid unicode files in the ftp directory.

-q Perform a query of the language tag.

- With no file specifiers, will query among the installed set of unicode files.
- With the *-d* option, will query among the installed set of user-defined files.
- With the *-T* option with filename, will query on the filename for time and date it was installed.

In all of the above cases, precedence is given to the custom file.

-v Display the version.

-? Display the usage statement.

Description

Use **loaddisplang** to query (-q) or install (-i) Unicode/user-defined telephone message files. There is no uninstall option for this command. If the installed files are not satisfactory, the user is expected to either overwrite them by re-running **loaddisplang** or to manually delete the installed files across all servers on which they reside. On Linux platforms, the ftp directory is /var/home/ftp/pub. The installation directory is /etc/opt/defty/i18n/

loadpwd

Syntax

```
loadpwd   [-c directory] [-o file] [-l file] [-i] [-f] [-t] [-L lacfile] [-?]
```

-c directory	The path to the directory that contains the passwd.conf and group.conf files. These files have the same format as /etc/group and /etc/passwd. They describe the attributes the logins added by this command will have (uid, home directory, etc.).The default is /etc/asg.
-o file	Path to the output file. Default is /etc/asg/asgfile.
-l file	Path to the authentication file to be loaded. The default is the newest file in /var/home/ftp/pub.
-i	Ignore the config file if the login already exists. By default, logins in the authentication file that already exist on the system are changed so they match what is in the passwd. conf and group.conf files. This option overrides this behavior.
-f	Force the new authentication file to load even if product ID's don't match.
-t	Test if the authentication file is valid; do not install.
-L lacfile	Only valid with -t option . Use this file for the overwrite legality test instead of the installed lacfile.
-?	Display the usage statement.

Description

Use loadpwd to run a command-line version of the utility to load the Avaya authentication file (password file) onto the:

- host server
- standby server
- Survivable Remote server

---

locktrans

Syntax

```
locktrans
```

Description

Use **locktrans** to lock translations so that no save translations can be performed until you use the **unlocktrans** command.

Caution:

This command does not have any options. Entering **locktrans -?** causes the command to lock translations.

logclear

Syntax

```
logclear
```

Description

Use **logclear** to remove logmanager output files from the /var/log/ecs directory.

logecho

Syntax

```
logecho -p procname -s[c|h|m|l] -l level | -t type -|message logecho -x procname
logecho -?
```

-p procname	The process name the user wants to display in the log.
-s severity	Severity: c = critical, h = high, m = medium, l = low
-l level	The level mask. The level can be entered in decimal, octal (preceded by ’0’), or hex (preceded by ’0x).
-t type	The type mask. The type can be entered in decimal, octal (preceded by ’0’), or hex (preceded by ’0x).
-	Log each stdin line.
message	The message to log.
x	Do a gstTrace_exit for this process.
-?	Display command option descriptions.

Description

Use **logecho** to make an entry in the logmanager log. Only the first non-option argument is placed in the log as the message body. Shell quoting can be used to put messages which contain white space. If the argument value is "-", then the standard input is read, and each line becomes an entry in the log.

logfilter

Syntax

```
logfilter   [-o] [-a] [-d] [-s] [-l level] [-t type] processname | all
logfilter   [-h] [-?]
```

-o OR in the mask for which levels and types of messages will be logged. The mask can be entered in decimal, octal (preceded by ’0’), or hex (preceded by ’0x).

-a AND in the mask for which levels and types of messages will be logged. The mask can be entered in decimal, octal (preceded by ’0’), or hex (preceded by ’0x).

-d Reset the debugging level and type to the original default.

-s Display a summary of the debugging level and type.

-l level Sets the mask for which levels of messages will be logged. The mask can be entered in decimal, octal (preceded by ’0’), or hex (preceded by ’0x).

-t type Sets the mask for which types of messages will be logged. The mask can be entered in decimal, octal (preceded by ’0’), or hex (preceded by ’0x).

-? | -h Display the usage statement.

Description

Use **logfilter** to selectively turn on or off the logging-specific types of messages as well as specific levels of messages for a specific process or all processes. If either the level or type mask is not specified, then its value is left the same. If neither are specified, then the current value of each for each specified process is displayed.

---

loginreport

Syntax

```
loginreport   [ -afhrsvw ] [ -n # ] [ -l { login | all } ] [ -b {begin_time} ] [ -e
{end_time} ] [-?]
```

-a Report only active sessions. Only valid with the -s or -y options.

-b begin_time Include sessions starting after this time. *Double quotes are required.* This parameter is optional. If not provided, events from the beginning of the file(s) to the stop time are included. The format is **"mm/dd hh:mm"**

-e end_time Include activity in the report starting at or before this time.*Double quotes are required.* This parameter is optional. If not provided, all events from the begin time to the current time are included. The format is **"mm/dd hh:mm"**

-f Produce a report of failed logins.

-n N Limit the output to N lines.

-n N Limit the output to N lines.

-r Display the report with the most recent events listed first (reverse order).

-s	Produce a report of successful logins.
-v	Produce a detailed report of user activity.
-l login | all	Enter a specific user name or `all`. If a specific user name is entered, activity for that single user in included in the report. The default is all.
-w	Format the report for the web.
-? | -h	Display the usage statement.

Description

Use **loginreport** to search for a specific set of log events. This command is intended to display normal user activity and is a starting point only for debugging analysis. At least one report type [-sfv] must be specified.

---

logv logc logw

Syntax

```
logv [OPTIONS]...[LOGS...] [-t time]...[[-a]FILTERS]...[-?]
logc [OPTIONS]...[LOGS...] [-t time]...[[-a]FILTERS]... [-?]
logw [OPTIONS]...[LOGS] [[-a]FILTERS]...[-?]
```

-b	Remove blank lines.
-c	Display the contents of the log. Automatically set if called with **logc**.
-d	Augment timestamps with time delta between entries displayed.
-desp [N]	Output a separator line when the delta between entries is greater than N seconds. The default is one second.
-ls	List the names and sizes of the log files.
-r	Reverse the order to display the latest entry first.
-s	Strip off the timestamp and header of each line.
-st	Leave the timestamp and strip off the rest of the header on each line.
-sd	Format the timestamp as **yyyy/mm/dd HH:MM:SS** and strip off the rest of the header on each line.
-w	Watch the log (automatically set if called with **logw**).
-v	Display the version of the command.

-l	Search only the latest file in the log. The default is all files.
-lf file	Assume that file is a log file and read input from it. Multiple -lf arguments may be entered.
-ld dir	Look for log files in the directory dir instead of the default directory.
-clear	Clear the log files (only logmanager files).
-t pattern	Filter events for a particular day/time pattern with the format of **yyyy[mm[dd:[HH[MM[SS[mmm]]]]]]**
-t range	Filter events for a particular day/time pattern with the format of **yyyy[mm[dd:[HH[MM[SS[mmm]]]]]]-yyyy[mm[dd:[HH[MM[SS[mmm]]]]]]**
-t today	Display today's log.
-t yesterday	Display yesterday's log.
app-pat	Filter events for a specific application or process (i.e., capro). Multiple application patterns may be specified.
-a	Application patterns following the -a are applied to the output of those preceding the -a. Application patterns following the -a are known to be grep patterns.
-g	Assume application filters are grep patterns instead of application names.
-I	Assume application pattern filters are grep patterns and ignore the case of letters.
--view VIEWNAME	Display the log using the log types and grep patterns associated with the view VIEWNAME. The built-in views are: • **ipevt** - List IP events (interfaces up/down, telephone/ endpoint registration/ deregistration). • **bashhist** - Platform command history log. • **mst** - If enabled via a SAT command, entries to the Communication Manager's message sequence trace (MST) log can be echoed into the debug trace log as well. • **hwerr** - The events that go into the Communication Manager's hardware error and alarm logs. This needs special deciphering by an external tool. • **sat** - The System Administration and Maintenance activities performed on Communication Manager's System Access Terminal (SAT). • **swerr** - The events that go into the Communication Manager's software error log. This needs special deciphering by an external tool. • **kernel** - Linux kernel debug messages.

- **cron** - Linux scheduled task log.

-? Display command option descriptions.

Description

Use **logv** to merge and edit (vi) the various log files in the system.

Use **logc** to merge and output (cat) various log files to standard output.

Use **logw** to watch the requested log file for changes applying the specified filters. Multiple logs can be specified. The logs are merged and sorted by time. Multiple time patterns and time ranges can also be specified.

Log file name

The log file names are:

Log file name	Description
all	Display all possible logs.
lm	logmanager debug trace log (default).
lxboot	Linux boot message.
lxsys	Linux syslog.
lxsec	Linux access security log.
lxwtmp	Linux login/logout/reboot log.
lxxfer	Linux file transfer log.
wd	Watchdog logs.
cmds	Platform command history log.
httperr	HTTP/web server error log.
httpssl	HTTP/web secure sockets layer (SSL) request log.
httpaccess	HTTP/web access log.
cmresetart	Communication Manager restart log (last 16 restarts).
filesync	Communication Manager file synchronization log.
update	System updates/patches
ccsppm	PPM log
siptrace	SIP trace log
ccsmasw	Core Router trace log.

modserv

Syntax

```
modserv  [-T] [-v] [ -stat | -off | -once | -respawn | -? ]
```

-T Turn on verbose mode.

-stat	Return the access status: • 0 = access off • 1= access on for one call • 2= access on for multiple calls
-v	Display current status if -stat option is set.
-off	Turn modem access off.
-once	Turn modem access on for one call.
-respawn	Turn modem access on for multiple calls.
-?	Display command option descriptions.

Description

Use **modserv** to turn modem access on or off for one or more calls.

---

mv_lastlog

Syntax

```
mv_lastlog
```

Description

Use **mv_lastlog** to run the Communication Manager modified version of the Linux lastlog utility.

---

mv_status

Syntax

```
mv_status
```

Description

Use **mv_status** to generate a report on Communication Manager run status.

---

ping

Syntax

```
ping  <ipaddr> [numpackets]
```

Description

Gets the target host IP address from the user at the command line. The user may elect to send from 1 to 255 data packets to the specified host by indicating the number of packets at the command line. Verifies that a remote host is reachable by sending ICMP echo request packets and waiting for replies. If the number of packets to send is not indicated on the command line, this command will send five data packets to the target host.

---

pingall

Syntax

```
pingall [ [-s [ServerID]] [-i [cab#][carrier]] [-c count] [-v] [-?]
```

-a	Ping all network entities on the remote sides, including servers, routers, and IPSI circuit packs.
-s ServerID	Ping a specific customer LAN.
-i cab# [carrier]	Ping a specific IPSI.
-c count	The number of test messages for each network entity
-v	Turn on verbose mode.
-?	Display a description of command options

Description

Use **pingall** to verify basic connectivity. **pingall** will ping all IPSI circuit packs.

---

productid

Syntax

```
productid   [ -p ] [ -m ] [ productID ] [ -? ]
```

-p productID	Set this server's Communication Manager productid. The productID is a 10–digit number that starts with **1**.
-m productID	Set this server's Messaging productid. The productID is a 10–digit number that starts with **2**.
-?	Display the command option descriptions.

Description

Use **productid** to view or set the Product ID for Communication Manager and , Messaging.

If no arguments are entered, **productid** displays the server's product IDs.

raid_status

Use **raid_status** to display the server RAID (Redundant Array of Independent Disks) controller status on an S8510 server.

Syntax

```
raid_status -c
raid_status -h
raid_status [-s | -v]
raid_status [-s | -v] -p
raid_status [-s | -v] -n
```

-c	Check for a possible HDD failure and log the failure in syslog.
-h	Display the help message..
-v	Verbose output, display all RAID Controller Data.
-n	Display the number of disk drives.
-s	(Default). Display physical disk drive data, short version.
-p	Display physical disk drive data. Use with -v or -s.
-p -s	(Default). Display short physical disk drive data.
-p -v	Display verbose physical disk drive data.
-n -s	(Default). Display short drive data 1, 2, or -1 (not sure).
-n -v	Display verbose (slot number) number drive data
-?	Display the help statement.

Description

raid_status -n displays the number of HDD's detected. The return values are:

- **-1** - **raid_status -n** will return -1 when it is not clear if both hard drives are plugged in. If this occurs, enter **raid_status -n -v** or **raid_status -p** which displays if both hard drives are present or if one is marked as Failed.
- **Failed** - If a hard drive is shown as Failed, the amber LED on the associated failed hard drive will either be flashing on a regular basis or solidly on. A hard drive may also be marked as Failed if it was pulled live.
- **Interim Recovery Mode** - It is possible that a disk is bad or the server only has one HDD plugged into the server. To determine the server HDD state, enter **raid_status -p -v** or **raid_status -n -v**.

If **raid_status -c** is executed and a disk failure exists, the output will indicate the failed disk.

Specifying the following options together is INVALID:

- raid_status -v -s
- raid_status -p -n

Note:

An unplugged HDD appears as a failed HDD to the RAID controller.

restartcause

Syntax

```
restartcause
```

Description

Use **restartcause** to see a list of Communication Manager restarts, their causes, and whether or not each restart escalated into a higher initialization. Use **restartcause** to help determine when an interchange or reload took place. Restarts are listed in ascending order of time.

Also see **display initcauses.**

Field	Description
Cause	The reason for the restart. • **Initialized** — System initialization. Internal request = Software requested the restart, usually in response to a server interchange. Internal request restarts are not initiated in direct response to an error and are non-escalating. Software request = Typically, software detected an error and automatically requested a restart. • **Craft request** — A user logged in as craft requested the restart and selected the level through an administration session on the server. • **Interchange** — A State of Health change caused the arbiter process to initiate the restart. • **Interchange-Craft** — An administrative session (session -i command, on-demand interchange) caused the arbiter process to initiate the restart. • **Internal request** — Software requested the restart, usually in response to a server interchange. Internal request restarts are not initiated in direct response to an error and are non-escalating. • **Software request** — Typically, software detected an error and automatically requested a restart.
Action	The level of the restart. • **1 (Warm)** — Communication Manager is restarted. Active calls remain up. • **2 (Cold)** — Communication Manager is restarted, ranslations are preserved, and all calls are dropped.

Table continues…

	• **4 (Reload)** — Communication Manager software is completely reloaded. All calls are dropped, the translations are reloaded, and the hardware is re-initialized.
Escalated	**Escalated** indicates whether the current restart has been escalated (increased in level) from a previous level. Restarts can be automatically or manually escalated to a higher level. For example, if the software detected an error and could not resolve the error by doing a level 1 restart, it would automatically initiate a level 2 restart.
Mode	State of the server immediately after the interchange, at the time of the restart. Look for a change of mode to help determine when an interchange occurred. • **Active** — Mode of a simplex server and for a duplex server that is the active server. • **Standby** — Mode of a standby server in a duplex configuration. • **Busout** — Mode of a standby server that has been placed out-of-service with a **busyout** command.
Time	The date and time the restart occurred. The restarts are displayed in descending order.

Error messages

Error Message	Description
invalid argument: <argument>	More than one arguemnt was entered on the command line.
No initfile at ./initcause.log or /var/log/defty/initcause.log	The data file is either missing or unreadable (for example, there is no read permission).
restartcause: Error reading initcausefile, error — <error>	The command encountered a problem reading the data file. The file is either ./initcause.log or /var/log/defty/initcause.log.

rm_download_files

Syntax

```
rm_download_files [ file-to-delete ]
sudo rm_download_files [ file-to-delete ]
```

Description

Use **rm_download_files** to add remove files from the /var/home/ftp/pub directory.

rm_download_files *file-to-delete* attempts to delete the specified file from /var/home/ftp/pub. The file must be present in the directory (or a subdirectory) and must alos be a regular file. The file must also be owned by the ftp user to prevent others from deleting files saved by other logins.

The susers group logins must use sudo to have access to this command since the command requires root permission to run.

rtrenice

Syntax

```
rtrenice
```

Description

Use **rtrenice** to change the current login's priority. Useful, but dangerous on a high occupancy customer switch.

Example

```
rtrenice -r 99 $$  (as root)
```

sat

Syntax

```
sat  [-? | h] [path]
```

path Use an alternate SAT executable, where path is the path to the directory containing the SAT executable.

-? Display the help message.

-h Display the help message.

Description

Use **sat** to run a Communication Manager SAT (system access terminal) session. Also use **autosat** and **dsat**.

save_trans

Syntax

```
save_trans
```

Description

Use **save_trans** to save translations to the active and standby servers. Equivalent to **save translations** on the SAT. This command has no options.

server

Syntax

```
server [ -i | -if | -c | -b | -r | -q | -o | -? ]
```

-i Perform an interchange between the active and standby servers.

-if Perform an inerchange immediately with a forced health-override (potentially dangerous).

-c Continuously display status updates at 1–second intervals.

-b Busyout this server if it is in standby mode.

-r Release this server if it is busied-out.

-u Pre-update/upgrade step, if active.

-U Undo the pre-update/upgrade step, if active.

-? Display command options descriptions.

Description

Use **server** to display or change server status on a server and to see the status and health of each server, including information regarding:

- duplication
- connectivity status
- shadowing
- status of outstanding major and minor alarms
- how long the servers have been up since the last restart
- state of health (hardware health, process health, control network health)

Use **server** with no options to display the status of the active and standby servers.

---

setnic

Syntax

```
setnic  -h
setnic [-d] -B <interface>
setnic [-d] -m <10H|10F|100H|100F|1000H|1000F|AUTO> <interface>
setnic [-d] -q <interface>
```

-h Display the help message

-B Boot mode. Invoked from network scripts like ifup

-d Turn on debug mode

-m Set < interface > to specified speed/duplex

-q Query the configured and current speed/duplex setting for < interface >

-w Web option (only update speed settings in config file)

Description

Use **setnic** to configure Ethernet interface speed, duplex, and auto-negotiation settings on the NIC of a specific server running Communication Manager.

Caution:

If you use **setnic** to query/set the interface Speed/Duplex settings of an interface, that interface will be reset. Be careful about doing this on an active server.

---

start

Syntax

```
start  [ -a ] [ -c ] [ -s app ] [ -? ]
```

-a Start all applications.

-c Continually display application status until all applications are fully running.

-s app Start a specific application.

-? Display the command option descriptions and a list of valid applications.

Description

Use **start** to start server applications. A single application or several applications can be specified.

The most common use is **start** -ac.

---

statapp

Syntax

```
statapp [-c# [-D | -U]] [-d] [-l [#]] [-p] [-w] [-b][-s app1 [,app2,...]] [-v] [-?]
```

-c# Continuous update of output every # (1-9) seconds.

-D Exit continuous update when all processes are DOWN.

-U Exit continuous update when all processes are UP.

-d List only applications that are down but expected to be up.

-l List all possible names of applications and services.

-l#	List the status of all possible applications and services. Show applications at level # (0-9) and below. The default is 0.
-p	List the names and status of processes associated with applications.
-w	Also list applications with status WATCHED by watchdog.
-b	Brief output status - application name and UP/DOWN/OFF status
-s app	List the status of the named applications.
-v	Display the command version.
-?	Display the command options descriptions.

Description

Use **statapp** to see the status of the server applications.

---

statuslicense

Syntax

```
statuslicense [-a application] [-e] [-f [ # | field] ] [-v]  [-h | -?]
```

-a application	Display the license information for the specified application. application may be: • 'CommunicaMgr' — display the license information for Communication Manager. This is the default. • 'Messaging' — display the license information for Communication Manager Messaging.
-e	Display Allocation License Status and Expiraton Date if Enterprise Wide Licensing is enabled.
-f [# | field name]	Display whether the feature is on or off in the license for a feature field number orf feature keyword.
-v	Turn on verbose mode to display more information.
-h | -?	Display the command option descriptions and a list of valid applications.

Description

Use **statuslicense** to display license information.

stop

Syntax

```
stop  [ -a | -b | -c | -f | -h | -i | -n | -r | -S | -s app | -? ]
```

-a Stop all applications.

-b Tell CMO to stop monitoring this virtual computer. Only applicable for vm_blade.

-c Continually display system status until all applications are DOWN.

-f Override any warnings or errors encountered with the -a, -h, -r and -s options.

-h Stop all applications and execute a processor halt.

-i Immediately stop all applications without allowing them to clean up.

-n Do not prompt before executing this command.

-r Stop all applications and execute a processor reboot.

-S Wait until all applications are stopped. Normally, the stop command returns when the stop request has been received by the system.

-s app Stop a specific application. Use stop -? for a full list.

-? Display a description of command options.

Description

Use **stop** to stop applications. The most common use is **stop** -acfn.

sudo

Syntax

```
sudo
```

Description

Use **sudo**, from a login that is not root, to temporarily run some commands as root.

swversion

Syntax

```
swversion [ -r [root-dir] [-v | -l | -R | -a ]] [-?]
```

-r	Use root2 as the base path.
-r root_dir	Use the specified directory as the base path.
-v	Display the Communication Manager software version string only.
-l	Display the Communication Manager load string only.
-a	Display all fields with the addition of the Application Directory information.
-R	Display the Communication Manager release string only.
-?	Display the command option descriptions.

Description

Use **swversion** to display the current software version of Communication Manager running on the server, including patches and the last time translations were saved.

---

systat

Syntax

```
systat [ -b ] [-c# [ -D | -U ] ] [-d ] [ -l#] [-p ] [-w][-s app1 [,app2, ... ] ] [-v] [-?]
```

-b	Display only the list of application names and their status.
-c#	Continuous update of output every # (1-9) seconds.
-D	Exit continuous update when all processes are DOWN.
-U	Exit continuous update when all processes are UP.
-d	List only applications that are down but expected to be up.
-l	List all possible names of applications and services.
-l#	List the status of all possible applications and services. Show applications at level # (0-9) and below. The default is 0.
-p	List the names and status of processes associated with applications.
-w	Also list applications with status WATCHED by watchdog.
-s app	List the status of the named applications.
-v	Display the command version.
-?	Display the command options descriptions.

Description

Use **systat** to see an update of the processes that are running on Communication Manager.

---

testcustalm

Syntax

```
testcustalm
```

Description

Use **testcustalm** to generate a customer-alarming test SNMP trap. No arguments are required. This command tests the health of alarm processing between the system and the receiver.

---

testinads

Syntax

```
testinads
```

Description

Use **testinads** to test the connectivity between the system and INADS. **testinads** generates a test alarm, sends it to INADS, and waits for a response. No command options are required.

To run **testinads** directly on the remote maintenance board, enter `sudo /opt/alarming/bin/testinads`

---

testinadsport

Syntax

```
testinadsport  [ -p [1024-65535]] | [-?]
```

-p -p with no assigned value sets the internal tcp port to a default value of 21111.

-p with a valid value sets the internal tcp port to that value. The valid tcp port values are 1024-65535.

If you enter an invalid port value for -p, the system displays an error message. For example, if you enter an invalid port value such as 65536, the system displays the following error message: `Invalid port number 1024-65535.`

-? Display the tcp port value usage.

Description

Use **testinadsport** to view, add, or change the tcp port number in the ecs.conf file. **testinadsport** will display the current value of the internal tcp port that is used between the GMM and the testinads command.

testled

Syntax

```
testled [ -a | -d | -s | -? ]
```

-a Test the LEDs on the server and the duplication memory card.

-d Test the Trans LED on the duplication memory card.

-s Test the LEDs on the server.

-? Display command option descriptions.

Description

Use **testled** to test the LEDs in the server.

tlscertmanage

Syntax

```
tlscertmanage [ -l ] [ -r # ] [ -i file ][ -h ] [-q]
```

-l List all CA (Certificate Authority) certificates on the server.

-r # Remove a CA (specifiy # 1–8) along with its corresponding file and hash link from the /etc/opt/ecs/certs/CA directory.

Caution:

Applications that depend on certificates will not operate properly if the certificates are removed.

-i file Install a Certificate Authority into Communication Manager's trusted certificate repository on disk. This command:

1. Copies the certificate file from the allowed location in the /etc/opt/ecs/certs/CA directory.
2. Concatenates the data in the certificate file into the all-ca.crt file.
3. Creates a link to the newly-copied certificate filename with the certificate's hash.

The full path to the file must be specified, e.g. **tlscertmanage -i /var/home/ftp/pub/newCA.crt**

-q Quiet mode — limit logging and return codes.

-h | -? Display the descriptions of the command options.

Description

The **tlscertmanage** (transport layer security certificate management) command facilitates loading a third-party trusted certificate into the Communication Manager repository for use the next time Communication Manager restarts.

CA certificates are now installed from the file system rather than being embedded into the telephony application. When Communication Manager is upgraded from an earlier release, the original Avaya CA certificates are installed. The administrator may then choose to modify the list of trusted CA certificates used by the Communication Manager telephony application to support third-party identity certificates.

To change the Communication Manager telephony application's CA certificates:

1. Use **tlscertmanage** to modify the list using the options described above.
2. Restart the Communication Manager application (stop -afc, start -ac from the root-level command line).

To identify the latest CA certificates installed in the telephony application, review the Communication Manager log and locate the last section of messages containing the phrase "gip/tls: Loaded trusted CA cert". Each CA certificate installed into the application is recorded in the Communication Manager log, which is viewable using the command **vilog**.

If the application fails to install any or all specified CA certificates, the Communication Manager log will contain one or more of the following error messages (where x is the Communication Manager release number):

- CMx_proc_err: pro=7204, err=201, seq=22145,da1=<n>,da2=<max>. This indicates that the number of CA certificates specified exceeds the number supported by the telephony application. <n> is the overlimit value and <max> is the maximum number of certificates supported. To resolve, use **tlscertmanage** to edit the list, then restart the application.
- CMx_proc_err: pro=7204, err=201, seq=22146,da1=<n>,da2=0. This indicates that a failure occurred when attempting to install the n'th CA certificate into the application. <n> is the index of the CA certificate list item that failed to install. To resolve, use **tlscertmanage** to remove, then re-add the certificate. Once re-added, restart the application.
- CMx_proc_err: pro=7204, err=201, seq=22147,da1=0,da2=0. This indicates that the CA certificate list file, /etc/opt/ecs/certs/CA/all-ca.crt, cannot be opened. This may be due to a user privilege issue or a missing/corrupted file. Use **tlscertmanage** to reconstruct the CA certificate list, then restart the application.

tlscertmanage informs the administrator upon successfully displaying, adding, or removing CA certificate list entries, and notes that a restart of the application is required if the list has changed. It prompts for confirmation before deleting a CA entry and associated CA files from the file system. It returns a warning message if the CA certificate list is empty.

topsting

Syntax

```
topsting [ -e ] [ -C procname] [-p pid] [-d directory] filename
```

-e	Generate abbreviated core files for all processes.
-C procname	Generate abbreviated core files for a specific procname. This option can be repeated for multiple processes.
-P pid	Generate abbreviated core files for process id (PID). This option can be repeated for multiple processes.
-d directory	The directory where abbreviated core files are to be placed. The default is the current directory.
-p path	path contains a colon-separated list of directory paths used to locate the exec_file and any shared libraries. An example would be -p $MYPJ/_mipslx.O:$BASEPJ/_mipslx.O
filename	Name of the mini-core dump file.
-?	Display the command option descriptions.

Description

Use **topsting** to pull information from a specific mini-core dump, based on the mini-core dump filename. Mini-core dump files are located in /var/log/defty/dumps, and are created after traps or buffer exhaustion in the system.

uname

Syntax

```
uname [ -a ] [ --help ]
```

Description

Use **uname -a** display all system information, including the kernel and the node name.

Use **uname --help** to display the list of valid options.

unlocktrans

Syntax

```
unlocktrans
```

Description

Use **unlocktrans** to unlock the “locked” translations and allow successful translation saves.

unused_login_audit

Syntax

```
unused_login_audit
```

Description

Use **unused_login_audit** to lock logins after a period of non-use.

update_activate

Syntax

```
update_activate [ -h ]
```

-h Display the command options.

Description

Use **update_activate** to activate a previously unpacked update on the server. Updates cannot be activated when a kernel update is in a pending state.

update_deactivate

Syntax

```
update_deactivate [ -h ]
```

-h Display the command options.

Description

Use **update_deactivate** to deactivate a previously activated update on the server. Updates cannot be deactivated when a kernel update is in a pending state.

update_info

Syntax

```
update_info [ -h ]
```

-h Display the command options.

Description

Use **update_info** to see information about a specified software update that is already installed.

update_remove

Syntax

```
update_remove [-a | <update_id> ] [-h | -?]
```

Description

Permanently remove an unpacked (deactivated) update from the server.

Use **update_remove -a** to remove all unpacked updates.

Use **update_remove** *update_id* to remove a specific unpacked update.

Use **update_remove -h** or **update_remove -?** to display the command option descriptions.

Note:

Communication Manager must be stopped for **update_remove** to compelte successfully.

update_show

Syntax

```
update_show [-a] [-c] [-k ] [-u] [-d] [-L] [--everything] [--updateidonly] [-?|-h|--help]
```

-a	Display activated updates.
-c	Display pending kernel updates.
-k	Display all kernel updates.
-u	Display all unpacked updates.
-p	Display packed updates.
-L	Display load-specific updates only.
--everything	Display all updates.
--updateidonly	Display only the updated ID names.
-? | -h | --help	Display the command option descriptions.

Description

Use **update_show** to display information about a specified software or kernel update.

update_unpack

Syntax

```
update_unpack [-L or <update-name.tar.gz>]
```

Description

This command unpacks the specified packed update or lets you select from a list of packed updates. Updates can only be unpacked if they are packed.

Use **update_unpack -L** to list only load-specific updates.

Use **update_unpack** *update-name.tar.gz* to unpack a specific update.

userlock

Syntax

```
userlock [-t tries] [-o lockout] [enable] [disable] [settings] [[-u login] unlock] [[-u
login] status] [-?] | [-h]
```

-t tries	The number of sequential failed login attempts when the account becomes locked out. The default is 5.
-o lockout	The number of seconds to lock out an account. The default is 600 seconds.
enable	Enable the security software that locks out accounts.
disable	Disable the security software that locks out accounts. The current settings of `tries` and `lockout` are preserved upon the next `enable`.
settings	Display if the feature is enabled or not, the value for the number of unsuccessful login attempts, and for how long a login should be locked out.
unlock	Unlock all locked-out accounts, or just the specified login if `-u login` is used.
status	Display the lockout status of all accounts, or just the specified login if `-u login` is used.
-u login	Unlock or display status on this login only.
-?|-h	Display the help message.

Description

Use **userlock** to configure the security software used to lock out login accounts where too many unsuccessful login attempts have occurred. This command also unlocks accounts that have been locked out by the security software.

vilog

Syntax

```
vilog [ -q ]
```

-? Display the usage statement.

Description

Use **vilog** to run the vi editor and to open current Communication Manager log files.

webssl

Syntax

```
webssl [-o] [-d [-r]] [-r] [-h]
```

-o Display the root certificate.

-d Set the openssl certificate to the default.

-r Restart the web server daemon.

-h Display the command option descriptions.

Description

webssl provides the ability to generate server certificates using Avaya certificate authority (CA) certificate, display the CA certificate, and reset to the default server certificate. With no options, **webssl** creates the open ssl certificate using the hostname (if it contains the domain name) or its IP address.

wlog

Syntax

```
wlog  -?
```

-? Display the usage statement.

Description

Use **wlog** to run the vi editor and to open current Communication Manager log files.

xlnrecovery

Syntax

```
xlnrecovery [-d] [-i ] [-?]
```

-d Set the translation recovery strategy to deferred.

-I Set the translation recovery strategy to immediate.

-? Display the usage statement.

Description

xlnrecovery provides the ability to display or set the translation recovery strategy stored in the system configuration files. There are currently two supported translation recovery strategies: immediate and deferred. The recovery strategy is applied during a system restart when Communication Manager detects that the restart has interrupted a translation transaction and has left the translation corrupted.

The **immediate** recovery strategy escalates the current system restart to a higher restart level that forces translation to be read from the disk to eliminate the corruption. This is the default strategy.

The **deferred** strategy just sets the translation corruption flag and continues execution of the current restart level. Setting the corruption flag prevents the corrupted translation from being saved to the disk file. At some later time, a system restart can be executed to force translation to be read from the disk to eliminate the corruption. This strategy allows the user to select a convenient time for the system restart.

Chapter 4: IPSI commands

IPSI commands

This chapter describes the command functionality available for the TN2312 IPSI (IP Server Interface) circuit pack. The IPSI provides an IP interface to servers and provides PKTINT, Archangel and Tone/Clock functionality in a port network. You can access IPSI functionality locally via a laptop connected to the IPSI's Ethernet services port which connects to the IPSI via the Control Network.

The IPSI hosts the ipadmin firmware application which may be accessed from the laptop or the server. The ipadmin applicatio:

- permits IPSI IP operating parameters to be changed.
- grants remote access to the server from the laptop.
- allows the execution of IPSI and network diagnostics.

Command interpreter

The IP administration command interpreter features a command-line interface (CLI), menus, and command help. The command interpreter initializes in an unprivileged mode when a user connects to the IPSI via telnet. The user may telnet to another host, including the active server, and determine the IPSI firmware version.

The user may enter into the privileged mode prompt via the `ipsilogin` command. In a privileged mode, the user must enter a valid login ID and password when prompted. In privileged mode, the user may query or set IPSI operating parameters, execute network diagnostics, and observe the IP addresses of the servers.

IPSI Clock

The IPSI clock is a tick count-driven firmware data structure which is used to timestamp debugging messages. It is synchronized with the server's clock via SNTP (Simple Network Time Protocol), the preferred method, or may be set manually via ipadmin commands.

IPSI/Network diagnostics

Authenticated IPSI users may execute diagnostics commands, such as:

- ping
- show arp
- show control route
- traceroute
- show internet status

Commands to reset the IPSI or to disable its IP interface are also available to authenticated users.

Query/display Server IP Addresses

Server IP addresses are hidden from unprivileged users. The IPSI telnet client suppresses the remote host IP address in its traditional “Trying <IP addr > message and other messages that reveal the IP address of the server.

If the user authenticates, the server IP addresses which are provided by the IPSI SIM (Server Interface Module) firmware are displayed (if known) when the IPSI telnet command is issued without specifying an IP address.

Ethernet services port configuration commands

Ethernet Services Port Configuration commands configure the Ethernet services port IP operating parameters. These commands are only for use in special circumstances.

Caution:

Exercise caution when issuing the following commands. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

These commands are:

- set services interface
- set services gateway
- set port negotiation
- set port speed
- set port duplex
- set port flowcontrol

exit (or quit)

Exit ipadmin, end the telent session, or return to the shell.

Syntax

```
exit
```

help (or ?)

Syntax

```
help (or ?)
```

Description

Display a context-sensitive list of available commands at the current level if a command is not specified. If `help` is entered followed by a command, the usage statement for that command is displayed with a brief description. An ipadmin user may enter `help`, `help [ cmd [subcmd] ]` to display a list of available commands or to get more detailed help for a command. For example, entering `show help` will instruct the ipadmin command interpreter to display all valid commands that pertain to `show`. The help is context-sensitive; a user must authenticate to be able to gain access to the privileged commands.

ipsilogin

Syntax

```
ipsilogin
```

Description

Prompts for a login ID and password. If these are entered correctly, the user may access the IPSI administrative and diagnostic commands.

ipsisession

Syntax

```
ipsisession  [-d] [-k] [-c cab#carrier] [-p IP_address] [-?]
```

-d	Disable the telnet server. Default is enable the telnet server.
-k	Remove known hosts file and enable SSH on IPSI circuit packs that have changed dynamic host keys. (reset the ssh host public key).
-c *cab#carrier*	The target IPSI board with the specified cabinet number and carrier ID.

-p *IP_address* The IP address of the target IPSI board.

-? Display the help message.

Description

Use **ipsisession** to enable:

- Secure Shell (SSH) remote access protocols through login/password authentication on IPSI circuit packs that support SSH
- Telnet on IPSI circuit packs that do not support SSH

Use **ipsisession** -k to remove the known hosts file in Communication Manager and enable an SSH session on the circuit pack. For more information on dynamic host keys, see **reset ssh-keys** and **ssh-keygen**.

Once the session is established, the user is prompted to accept the new keys. Verify that:

- A new host key has been generated.
- The IP address or hostname of the IPSI has changed. Use **list history** at the SAT to see whether **reset ssh-keys** has been executed on the CLAN or VAL circuit packs.

If neither of these conditions has occurred, then it is likely that another server is posing as the IPSI (rogue server, aka man-in-the-middle attack).

ipsiversion

Syntax

```
ipsiversion  [-a | -c cab#[carrier]] [-?]
```

-a Shows all IPSIs in the system.

-c *cab#* [*carrier*] Shows information for a specific IPSI.

-? Displays the help message.

Description

Use **ipsiversion** to query each IPSI to determine its IP address, name, TN code, and hardware and firmware vintages.

loadipsi

Syntax

```
loadipsi   [-a board_code] [-c cab#[carrier]] [-d] [-e] [-f filename] [-l] [-s time] [-i
ip-addr -u user] [-r] [-w pwd] [-F] [-?]
```

-a board_code Download the file to all IPSI boards with the specified board code.

-c cab#[carrier]	• -c cab# - Download the file to all IPSIs in a specified cabinet. • -c cab#carrier - Download the file to all IPSIs in a specified cabinet and carrier.
-d	Display all scheduled loadipsi jobs in the system.
-e	Erase all scheduled loadipsi jobs in the system.
-f filename	The firmware image file.
-l	Download the application firmware or boot code file to all standby IPSIs.
-s time	Download the file at the specified start time. The format is **mmddyyyyhh:ii**, where m = month, d = day, y = year, h = hour, i = minute.
-i ip-addr	Download the firmware image from the specified server.
-u user	Use the specified user name to obtain the file from the remote server specified by the -i option.
-r	Download without checking the version.
-p pwd	Use the specified password for the user name specified by the -u option.
-F	Fork a background process to do the download.
-?	Display the usage statement.

Description

Use **loadipsi** to load IPSI application firmware or boot code to all or specific IPSI boards in the system. The firmware or boot code is then burned into flash memory.

Prior to a download, **loadipsi** checks the current firmware and boot code versions on all target IPSI boards against the version ready for download. If the version on the boards is equal to or greater than the version on the server, **loadipsi** will stop the process. The command option -r will override the version check and allow the download.

loadstbyipsis

Syntax

```
loadstbyipsis   [-r] [-?] -f filename
```

-r	Download the file without checking the current version on the target standby IPSI board(s).
-f filename	The path/name of the application firmware or boot code file to download.

-? Display the usage statement.

Description

loadstbyipsis loads all standby IPSI boards in the system with the IPSI firmware image. This command is especially useful to load firmware on all standby IPSIs in a duplicated IPSI system, then using the **resetstbyipsis** command to activate the firmware (non-service affecting). This command will do nothing if the system is not running or if there are no standby IPSIs administered.

---

logout

Syntax

```
logout
```

Description

Disconnect form the IPSI ipadmin appication.

---

reset

Syntax

```
reset
```

Description

Causes the IPSI to immediately reset.

---

resetipsi

Syntax

```
resetipsi [-a | -b | -c cab#[carrier] | -d | -r | -i interval | -s start_time |-t
stop_time | -F | - S suffix] [-?]
```

-a Reset all IPSI circuit packs.

-b Reset all standby IPSI circuit packs.

-c cab#[carrier] Reset a specific IPSI circuit pack.

-d Display all scheduled resets.

-r Remove all scheduled resets.

-i interval Interval in minutes between two resets. The default is 10 minutes, the maximum is 15 minutes.

-s start_time	Start time for the reset in the format **hhddyyyyhh:ii**
-t stop_time	Stop time for the reset in the format **hhddyyyyhh:ii**
-F	Fork a background process to run the reset(s).
-S suffix	Suffix of the IPSI boards to reset.
-?	Display the command option descriptions.

Description

Use **resetipsi** to reset one or more IPSI boards.

---

resetbyipsis

Syntax

```
resetbyipsis
```

Description

Use **resetsbyipsis** to reset all standby IPSI boards in the system. This command is especially useful to activate the firmware on all standby IPSIs in a duplicated IPSI system. This command will do nothing if the system is not running or if there are no standby IPSI boards administered.

This command only works on the active server.

Caution:

This command has no options. It is executed when the command is entered.

---

set control gateway

Syntax

```
set control gateway  <gateway>
```

Caution:

Exercise caution when issuing `set control gateway`, especially from a remote platform. If improper IP operating parameters are issued, the IPSI may need to be reset, or even removed and reinserted, to recover.

Description

Gets the control network default gateway value from the user at the command line. If the default gateway value format is valid, it is applied to the control network IP interface.

Note:

The default gateway is where datagrams are routed when there is no specific routing table entry available for the destination IP network or host. This control network interface setting will take effect upon exiting IPADMIN.

set control interface

Syntax

```
set control interface <ipaddr> <netmask>
```

Description

Gets the IP address and subnetmask from the user at the command line. If the address is in valid format, it is applied to the control network IP interface. “IP [blank]” will be written to the faceplate LED display; this indicates at a glance that the IPSI IP address has been set manually. If the command fails, an error message is written to standard output, the control network IP interface will be disabled, and “A00” is written to the faceplate LED display; this indicates at a glance that the IPSI IP interface has been disabled. These control network interface settings will take effect upon exiting IPADMIN.

Caution:

Exercise caution when issuing set control interface, especially from a remote platform. If improper IP operating parameters are issued, the IPSI may need to be reset, or even removed and reinserted, to recover.

set diffserv

Syntax

```
set diffserv < value >
```

Description

Sets and stores the diffserv value in flash memory.

set port duplex

Syntax

```
set port duplex < port number > {half | full}
```

Description

Configures the duplex mode of a 10/100Base-T port. You can configure the 10/100Base-T port. You can configure the duplex mode to either Half or Full duplex. If auto negotiation is enabled for such ports, the port's duplex mode is determined by auto negotiation, overriding any value specified with this command. If auto negotiation is disabled, the speed configured with this command will take effect.

Caution:

Exercise caution when issuing **set port duplex**. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

set port flowcontrol

Syntax

```
set port flowcontrol < port number > {receive | transmit} {on | off}
```

Description

Enables/disables IEEE 802.3 flow control for a full duplex port. If auto negotiation is enabled, the flow control configured by this command will be advertised as during auto negotiation. After auto negotiation, flow control remains enabled only if it is negotiated between the link partners. If auto negotiation is disabled, flow control will only be enabled if the port is set to full duplex operation. Currently only receive flow control is available.

Caution:

Exercise caution when issuing **set port flowcontrol**. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

set port negotiation

Syntax

```
set port flowcontrol < port number > {enable | disable}
```

Description

Enables or disables auto negotiation on a port. For 10/100Base-T ports auto negotiation determines the speed duplex mode. The set port flowcontrol command affects the advertisement of flow control during auto negotiation.

Caution:

Exercise caution when issuing **set port negotiation**. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

set port speed

Syntax

```
set port speed < port number > {10MB | 100MB}
```

Description

Configures the speed of a 10/100Base-T port. You can configure the speed to either 10 Mbps or 100 Mbps. If auto negotiation mode is enabled for such ports, the port's speed is determined by auto negotiation, overriding any value specified with this command. If auto negotiation is disabled, the speed configured with this command will take effect.

Caution:

Exercise caution when issuing **set port speed**. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

set services gateway

Syntax

```
set services gateway ip-address
```

Description

Gets the services port gateway value from the user at the command line. If the gateway value is valid, it is (at the time of this writing) written into FLASH memory, but is not applied to the services port IP interface; it is reserved for a possible future use.

Note:

The services port gateway is typically the same value as the IP address of the services laptop personal computer. This is not the same gateway described under the set gateway command description.

Caution:

Exercise caution when issuing **set services gateway**. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

set services interface

Syntax

```
set services interface ip-address net-mask
```

Description

Gets the services port IP interface address and subnet mask from the user at the command line. If the address format is valid, it is applied to the services port IP interface upon exiting IPADMIN. If the command fails, an error message is written to standard output.

Caution:

Exercise caution when issuing **set services interface**. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

set time slot occupancy notification

Syntax

```
set fault-thresholds timeslot [ none  | %upper-threshold | %lower-threshold ]
```

%upper-threshold	1–100. The default value of the range is 90.
%lower-threshold	0–99. The default value of the range is 85.

Description

Sets and clears the time slot occupancy rate at which an SNMP trap is generated.

set vlan priority

Syntax

```
set vlan priority level
```

Description

Sets vlan priority level to specified level and stores it in flash memory.

set vlan tag

Syntax

```
set vlan tag [ on | off ]
```

Description

Sets vlan tagging on/off and stores the specified vlan tagging switch, on/off, in flash memory.

show arp

Syntax

```
show arp
```

Description

Displays the current Internet-to-Ethernet address mapping in the ARP table.

show control interface

Syntax

```
show control interface
```

Description

Displays several IPSI control network interface status indicators, including the IP address, subnet mask, default gateway, and the manual IP addressing mode.

show control stats

Syntax

```
show control stats
```

Description

Displays IP operating statistics associated with IPSI control network interface. Displayed data includes the IP and MAC addresses, number of packets sent and received, number of input and output errors, and flags (loopback, promiscuous, ARP, and so on).

show firmware version

Syntax

```
show firmware version
```

Description

Displays the IPSI application firmware version and related information, including the build time and workspace name.

show host

Syntax

```
show host
```

Description

Prints a list of remote hosts, along with their Internet addresses and aliases.

show internet stats

Syntax

```
show internet stats
```

Description

Displays a list of all active Internet protocol sockets in a format similar to the Unix netstat command.

Caution:

Exercise caution when issuing **show internet stats**. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

show ip stats

Syntax

```
show ip stats
```

Description

Displays detailed statistics for the IP protocol.

show network stats

Syntax

```
show network stats
```

Description

Displays statistics for all three attached network interfaces. Unit number 1 is the control network interface, unit number 2 is the services port interface, and unit number 3 is the packet bus interface.

show port

Syntax

```
show port port-number
```

port-number	Port number.

Description

Displays link indication, speed, duplex, and auto negotiation of a specified port.

Caution:

Exercise caution when issuing **show port**. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

show qos

Syntax

```
show qos
```

Description

Displays current and future vlan and diffserv parameters stored in flash memory. The future vlan and diffserv parameters, if applicable, is stored after the next reset.

show route

Syntax

```
show route
```

Description

Displays the current routing information contained in the routing table for all three interfaces (control network, services port, and packet bus).

show route stats

Syntax

```
show route stats
```

Description

Displays routing statistics.

show servers

Syntax

```
show servers
```

Description

Displays the IP addresses of the active and standby servers.

show services interface

Syntax

```
show services interface
```

Description

Displays several IPSI services interface status indicators, including the IP address, subnet mask, and default gateway.

Caution:

Exercise caution when issuing **show services interface**. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

show services stats

Syntax

```
show services stats
```

Description

Displays IP operating statistics associated with IPSI services interface. Displayed data includes the IP and MAC addresses, number of packets sent and received, number of input and output errors, and flags (loopback, promiscuous, ARP, and so on).

Caution:

Exercise caution when issuing **show services stats**. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

show tcp stats

Syntax

```
show tcp stats
```

Description

Displays detailed statistics for the TCP protocol.

ssh-keygen

Syntax

```
ssh-keygen
```

Description

Use **ssh-keygen** (IPSI-CLI command) to generate new SSH dynamic host keys on the IPSI circuit pack. Before you reset the dynamic host keys with **reset ssh-keygen**, use **busyout board** at the SAT to busyout the IPSI circuit pack.

Dynamic host keys

Dynamic keys are inherently more secure than static keys because:

- If static keys for one circuit pack are compromised, all circuit packs are compromised.
- The probability of compromise is reduced when each circuit pack has its own dynamic key.
- Users can change dynamic keys at any time.

Dynamic host keys include:

- IP address
- Host name
- Firmware

Public key exchange

TN circuit packs support dynamic host keys. Because clients have the server's public key information stored on them, when the server generates a new public/private key pair (which happens the first time the board initializes or when the user decides), the client prompts the user to accept the key when logging into the server. This is to make the client user aware that the server's public key is not what it used to be and this may, but not necessarily, imply a rogue server.

A technician encountering a situation where the server's public key is not what it used to be should determine if the server's keys were changed since the last servicing.

- If they were, the technician should continue login.
- If not, there is a security issue, and the technician should notify the appropriate personnel.

telnet

Syntax

```
telnet ip-address
```

Description

Connects user to ipadmin, [IPSI]: prompt

Connects to the specified server via the telnet protocol on TCP port 23. User may access the server, or authenticate to run administrative and diagnostic commands. If the user authenticates, the prompt is changed to [IPADMIN].

If the user connects to the shell via telnet, he or she may start ipadmin from the shell prompt. In this case, the ipadmin exit (or quit) command will return the user to the shell prompt. The user must then enter logout to disconnect.

Any ipadmin user may telnet to the active server via the telnet command. He or she will have to contend with the server's security.

trace route

Syntax

```
trace route ip-address
```

Description

Uses ICMP messages to verify each segment along a path to a remote host.

Caution:

Exercise caution when issuing this command. If improper IP operating parameters are issued, the services interface may be rendered unusable with the standard services laptop personal computer configuration.

Appendix A

PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) in case of any software update. For example, a PCN must accompany a service pack or a patch that needs to be applied universally. Avaya issues product-support notice (PSN) when there is no patch, service pack, or release fix, but the business unit or services need to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a workaround for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.

   Note:

   If the Avaya Support website displays the login page, enter your SSO login credentials.
2. On the top of the page, click **DOCUMENTS**.
3. On the Documents page, in the **Enter Your Product Here** field, enter the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. Select the appropriate filters as per your search requirement. For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

   Note:

   You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new services packs are available. The Avaya E-Notifications process manages this proactive notification system .

To sign up for notifications:

Procedure

1. Go to the Avaya Support Web Tips and Troubleshooting: eNotifications Management page at https://support.avaya.com/ext/index?page=content&id=PRCS100274#.
2. Set up e-notifications. For detailed information, see the **How to set up your E-Notifications** procedure.

Index

A

aca
- list measurements ... 247

acpfindvers ... 441

add
- cabinet ... 76
- fiber-link ... 172
- ipserver-interface ... 216
- media-gateway ... 278
- remote-office ... 344
- station ... 362
- user-profile-by-category ... 437

alarm categories ... 24

almcall ... 441

almclear ... 442

almdisplay ... 443

almenable ... 443

almnotif ... 444

almsnmpconf ... 444

almsummary ... 445

almsuppress ... 445

audience ... 21

audits
- clear audits ... 54
- status audits ... 54

authtype ... 445

autosat ... 446

B

busyout
- access-endpoint ... 34
- board ... 65
- campon-busyout ... 83
- cdr-link ... 94
- cti-link ... 137
- data-module ... 142
- ds1-facility ... 146
- fiber-link ... 173
- ipserver-interface ... 217
- journal-printer ... 235
- link ... 238
- mis ... 293
- pms-link ... 319
- port ... 326
- pri-endpoint ... 334
- processor-ip-interface ... 337
- sp-link ... 359
- station ... 362
- tdm ... 405
- trunk ... 423

busyout command ... 24

C

cancel
- hardware-group ... 189

change
- cabinet ... 78
- circuit-packs ... 97
- communication-interface links ... 102
- communication-interface processor-channels ... 102
- cti-link ... 138
- extended-user-profile ... 169
- extension ... 362
- fiber-link ... 174
- firmware download ... 181
- firmware station-download ... 185
- integ-annc-brd-loc ... 200
- ip-codec-set ... 202
- ip-interface ... 209
- ip-network-region ... 212
- ipserver-interface ... 217
- logging-levels ... 242
- media-gateway ... 281
- public-unknown-numbering ... 339
- remote-office ... 345
- synchronization ... 379
- system-parameters duplication ... 394
- system-parameters ip-options ... 396
- system-parameters ipserver-interface ... 396
- system-parameters maintenance ... 398
- system-parameters port-networks ... 404
- tftp-server ... 413
- user-profile ... 431
- user-profile-by-category ... 438

change bp ... 68

clan ethernet
- list measurements clan ethernet ... 247

clan ppp
- list measurements ... 248

clan sockets
- list measurements ... 249

clear
- errors ... 154
- firmware-counters ... 180
- isdnpri-testcall ... 230
- link ... 238
- mst ... 296
- pkt ... 317
- port ... 327

clock
- IPSI ... 483

cmpasswd ... 446

cmuseradd ... 446

cmuserdel ... 447

cmusermod 447
command interpreter 483
command syntax 22
common error codes 28
common output fields 26
common parameters 25
contention 23
corevector 448
craft2
  disable craft2 137
  enable craft2 137
custalmopt 449

D

defsat 449
dhelp 449
diagnostics
  IPSI 484
disable
  administered-connection 37
  announcement-board 48
  ess 159
  filexfer 179
  firmware download 183
  firmware station-download 186
  mst 296
  nr-registration 302
  suspend-alm-orig 376
  synchronization 380
  test-number 408
disp_dup_log 450
display
  alarms 41
  bulletin-board 76
  cabinet 78
  capacity 83
  circuit-packs 99
  communication-interface links 102
  communication-interface processor-channels 104
  disabled-tests 146
  errors 155
  events 168
  extended-user-profile 170
  failed-ip-network-region 171
  fiber-link 176
  firmware download 183
  firmware station-download 186
  initcauses 198
  ipserver-interface 221
  logging-levels 242
  media-gateway 282
  mst 297
  node-names 301
  port 327
  profile-base 338
  public-unknown-numbering 340
  remote-office 345
  signaling-group 351
  synchronization 381
  system-parameters duplication 395
  system-parameters ip-options 396
  system-parameters ipserver-interface 398
  system-parameters maintenance 404
  test-schedule 408
  tftp-server 413
  time 413
  user-profile 432
  user-profile-by-category 438
displaydenialevents 450
dkill 450
document changes 21
ds1
  list measurements 250
dsat 451
duplicate
  ip-network-region 213
  user-profile 434

E

enable
  administered-connection 37
  announcement-board 48
  ess 160
  filexfer 180
  mg-return 292
  nr-registration 303
  session 349
  suspend-alm-orig 377
  synchronization 382
  test-number 408
environment command 451
erase
  announcement 47
  terminal 407
error categories 24
error codes
  common 28
error messages 27
Ethernet configuration commands 484
exit 485
export
  user-profile 434

F

fasttop 451
filesync 452
ftpserv 454
fwdlreason 454

G

get
boot-image 67
ethernet-options 166
power-shutdown 334
get forced-takeover
ipserver-interface 222
go
shell 350

H

hardware_info 455
help 485
history
notify 198

I

import
user-profile 435
ip-address
trace route 419
ip codec
list measurements 252
ip dsp-resource
list measurements 253
IPSI clock 483
IPSI commands 483
IPSI diagnostics 484
ip signaling-groups
list measurements 265
ipsilogin 485
ipsisession 485
ipsiversion 486
ip voice-stats
list measurements 266

L

legal notice .....
Linux commands overview 441
list
aar route-chosen 33
announcement 47
ars route-chosen 51
audio-group 53
cabinet 78
calltype route-chosen 81
configuration 132
configuration power-supply 135
cti-link 140
directory 145
disabled-mos 145
ethernet-options 167
extension-type 170
fiber-link 176
history 196
ip-interface 210
ip-network-region 212
ip-route 214
ipserver-interface 223
isdnpri-testcall 231
locations 241
marked-ports 245
mct-history 245
media-gateway 282
media-gateway configuration list 134
moh-analog-group 295
monitored-station 296
mst 297
multimedia 299
night-service attendant 300
night-service hunt-group 300
night-service trunk-group 300
off-pbx-telephone station-mapping 309
pms-down 318
public-unknown-numbering 340
registered-ip-stations 342
remote-office 345
set-data 349
signaling-group 353
skill-status 357
station 363
survivable-processor 375
suspend-alm-orig 378
synchronization 382
sys-link 385
testcalls 410
trace media-gateway 416
trace ras 417
trace station 417
trace tac 418
trace vdn 418
trace vector 419
tti-ip-stations 431
user-profile 436
list aar analysis
aar analysis 32
list ars analysis
ars analysis 50
list configuration
software-versions 135
stations 136
listhistory 455
list measurements
ipserver-interface 223
list usage
audio-group 54
cti-link 140
integ-annc-board 200
loaddisplang 456

loadipsi 486
loadpwd 456
loadstbyipsis 487
locktrans 457
logc 460
logclear 458
logecho 458
logfilter 458
loginreport 459
logout 488
logv 460
logw 460

M

mark
  port 328
modserv 462
monitor
  bcms 61
  health 193
  security-violations 347
  socket-usage 358
  system 388
  traffic 421
  trunk 424
mv_lastlog 463
mv_status 463

N

netstat
  arp 49
  ip-route 215
network diagnostics 484

O

output fields
  common 26
overview 21, 23
overview, Linux commands 441
overview, maintenance commands 21

P

parameters, common 25
PCN 500
PCN notification 500
PCNs 500
pin
  change pin 314
  reset pin 314
ping 463
  ping 315
pingall 464
productid 464
PSN 500
PSN notification 500
PSNs 500

Q

query/display server IP addresses 484

R

raid_status 465
recycle
  carrier 93
refresh
  ip-route 216
  route-table 346
related documentation 30
release
  access-endpoint 35
  board 65
  cdr-link 95
  cti-link 141
  data-module 143
  ipserver-interface 224
  journal-printer 235
  mis 293
  modem-pool 294
  pms-link 320
  port 328
  pri-endpoint 335
  processor-ip-interface 337
  sp-link 360
  station 363
  tdm 405
  trunk 424
release command 24
remove
  file 179
  ipserver-interface 225
  remote-office 346
  user-profile 437
reset 488
  aesvcs link 38
  board 66
  fiber-link 177
  ipserver-interface 225
  ip-stations 226
  login-id 243
  maintenance 244
  media-gateway 284
  meet-me-vdn 291
  packet-interface 310
  pnc interchange 325
  port-network 329
  ssh-keys 361
  system 391

reset *(continued)*
val 438
resetbyipsis 489
resetipsi 488
restartcause 466
resume
hardware-group 189
rm_download_files 467
rtrenice 468

S

safety labels 22
sat 468
save
translation 422
save_trans 468
security alert label 22
server command 468
server IP addresses
query/display 484
set
boot-image 68
emergency 150
ethernet-options 167
ipserver-interface 226
media-processor 286
pnc 322
signaling-group 354
switch-node-clock 379
synchronization 383
tdm 405
time 414
tone-clock 415
set control gateway 489
set control interface 490
set diffserv 490
setnic 469
set options
options 306
set port duplex 490
set port flowcontrol 491
set port negotiation 491
set port speed 491
set services gateway 492
set services interface 492
set time slot occupancy notification 493
set vlan priority 493
set vlan tag 493
show arp 493
show control interface 494
show control stats 494
show firmware version 494
show host 494
show internet stats 494
show ip stats 495
show network stats 495
show port 495
show qos 496
show route 496
show route stats 496
show servers 496
show services interface 496
show services stats 497
show tcp stats 497
signing up for PCNs and PSNs 501
simultaneous commands 23
ssh-keygen 497
start 470
statapp 470
status
access-endpoint 35
administered-connection 38
aesvcs cti-link 38
aesvcs interface 39
aesvcs link 40
attendant 52
bri-port 69
cabinet 79
cdr-link 95
clan-all 99
clan-ip 100
clan-port 101
cleared-alarm-notif 101
conference 104
data-module 143
environment 151
ess clusters 161
ess port-networks 163
firmware download 184
firmware station-download 186
hardware-group 190
health 194
ip-board 201
ip-network-region 212
ip-synchronization 228
isdnpri-testcall 231
journal-link 234
link 238, 387
logins 243
media-gateway 284
media-processor 288
media-processor board 289
mg-announcements 291
nr-registration 303
off-pbx-telephone station 308
packet-interface 311
periodic-scheduled 312
pms-link 320
pnc 322
port-network 330
pri-endpoint 335
processor-ip-interface 337
psa 338

status *(continued)*
remote-access ... 343
remote-office ... 346
signaling-group ... 354
socket-usage ... 358
sp-link ... 360
station ... 364
switch-node ... 378
synchronization ... 383
sys-link ... 386
trunk ... 425
tsc-administered ... 428
tti ... 430
val-ip ... 439
video-bridge ... 439
statuslicense ... 471
stop ... 472
sudo ... 472
support
contact ... 31
swversion ... 472
syntax ... 22
systat ... 473

T

telnet ... 498
test
access-endpoint ... 36
aesvcs-server ... 40
alarms ... 44
analog-testcall ... 46
board ... 66
cdr-link ... 97
cti-link ... 141
customer-alarm ... 142
data-module ... 144
ds1-facility ... 147
ds1-loop ... 148
eda-external-device-alrm ... 149
environment ... 153
failed-ip-network-region ... 171
fiber-link ... 178
firmware download ... 185
firmware station-download ... 188
hardware-group ... 191
ipserver-interface ... 226
isdnpri-testcall ... 233
journal-printer ... 236
led ... 236
license ... 237
link ... 241
maintenance ... 244
media-gateway ... 286
modem-pool ... 294
packet-interface ... 312
pkt ... 318
pms-link ... 321
port ... 329
pri-endpoint ... 336
signaling-group ... 356
sp-link ... 360
station ... 375
synchronization ... 384
tdm ... 406
tone-clock ... 415
trunk ... 427
tsc-administered ... 429
testcustalm ... 474
testinads ... 474
testinadsport ... 474
testled ... 475
tlscertmanage ... 475
tone-receiver
list measurements ... 275
topsting ... 476
trace route ... 499
training ... 30

U

uname ... 477
unlocktrans ... 477
unused_login_audit ... 478
update_activate ... 478
update_deactivate ... 478
update_info ... 478
update_remove ... 479
update_show ... 479
update_unpack ... 480
userlock ... 480

V

videos ... 31
vilog ... 481

W

Warranty ... 31
webssl ... 481
wlog ... 481

X

xlnrecovery ... 482