Version 2.50

Part No. 317517-C Rev 00
July 2005

600 Technology Park Drive
Billerica, MA 01821-4130

Configuring and Troubleshooting the Contivity 221 VPN Switch

NORTEL NETWORKS™

Copyright © 2005 Nortel Networks

All rights reserved. July 2005.

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

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

Trademarks

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Check Point and Firewall 1 are trademarks of Check Point Software Technologies Ltd.

Java is a trademark of Sun Microsystems.

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

NETVIEW is a trademark of International Business Machines Corp (IBM).

OPENView is a trademark of Hewlett-Packard Company.

SPECTRUM is a trademark of Cabletron Systems, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted rights legend

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

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

Statement of conditions

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

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

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

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

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

Nortel Networks Inc. software license agreement

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

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

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

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

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

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

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

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

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

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

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

Contents

Preface 47

Before you begin 47
Text conventions 47
Related publications 48
Hard-copy technical manuals 49
How to get help 49

Chapter 1
Getting to Know Your Contivity 221 51

Introducing the Contivity 221 51
Features 51
Physical Features 52
4-Port Switch 52
Auto-negotiating 10/100 Mbps Ethernet LAN 52
Auto-sensing 10/100 Mbps Ethernet LAN 52
Auto-negotiating 10/100 Mbps Ethernet WAN 52
Auxiliary Port 52
Time and Date 53
Reset Button 53
Non-Physical Features 53
IPSec VPN Capability 53
Certificates 53
SSH 53
HTTPS 54
IEEE 802.1x for Network Security 54
Firewall 54
Brute-Force Password Guessing Protection 54
Content Filtering 54

Packet Filtering 55
Universal Plug and Play (UPnP) 55
Call Scheduling 55
PPPoE 55
PPTP Encapsulation 55
Dynamic DNS Support 55
IP Multicast 56
IP Alias 56
Central Network Management 56
SNMP 56
Network Address Translation (NAT) 56
Traffic Redirect 57
Port Forwarding 57
DHCP (Dynamic Host Configuration Protocol) 57
Full Network Management 57
RoadRunner Support 57
Logging and Tracing 57
Upgrade Contivity 221 Firmware 58
Embedded FTP and TFTP Servers 58
Applications for the Contivity 221 58
Secure Broadband Internet Access and VPN 58
Hardware Setup 59

Chapter 2
Introducing the WebGUI 61

WebGUI Overview 61
Accessing the Contivity 221 WebGUI 61
Resetting the Contivity 221 63
Procedure To Use The Reset Button 63
Uploading a Configuration File Via Console Port 64
Navigating the Contivity 221 WebGUI 65

Chapter 3
Wizard Setup 67

Wizard Overview 67

Wizard Setup: General Setup and System Name 67
Domain Name 68
Wizard Setup: Screen 2 68
Ethernet 68
PPTP 70
PPPoE Encapsulation 71
Wizard Setup: Screen 3 74
WAN IP Address Assignment 74
IP Address and Subnet Mask 74
DNS Server Address Assignment 75
WAN MAC Address 76
Basic Setup Complete 79

Chapter 4
System Screens 81

System Overview 81
DNS Overview 81
Private DNS Server 81
Configuring General Setup 82
Dynamic DNS 85
DYNDNS Wildcard 85
Configuring Dynamic DNS 85
Configuring Password 87
Pre-defined NTP Time Server List 89
Configuring Time and Date 90
ALG 94
Configuring ALG 94

Chapter 5
LAN Screens 97

LAN Overview 97
DHCP Setup 97
IP Pool Setup 97
DNS Servers 98
LAN TCP/IP 98

Factory LAN Defaults 98
RIP Setup 98
Multicast 99
Configuring IP 100
Configuring Static DHCP 103
Configuring IP Alias 104

Chapter 6
WAN Screens 107

WAN Overview 107
TCP/IP Priority (Metric) 107
Configuring Route 108
Configuring WAN ISP 109
Ethernet Encapsulation 109
PPPoE Encapsulation 110
PPTP Encapsulation 113
Service Type 114
Configuring WAN IP 116
Configuring WAN MAC 119
Traffic Redirect 120
Configuring Traffic Redirect 121
Configuring Dial Backup 123
Advanced Modem Setup 128
AT Command Strings 128
DTR Signal 128
Response Strings 128
Configuring Advanced Modem Setup 129

Chapter 7
Network Address Translation (NAT) Screens 131

NAT Overview 131
NAT Definitions 131
What NAT Does 132
How NAT Works 133
Port Restricted Cone NAT 133

NAT Application 134
NAT Mapping Types 135
Using NAT 136
SUA (Single User Account) Versus NAT 136
SUA Server 137
Default Server IP Address 137
Port Forwarding: Services and Port Numbers 138
Configuring Servers Behind SUA (Example) 138
Configuring SUA Server 139
Configuring Address Mapping 141
Trigger Port Forwarding 145
Trigger Port Forwarding Example 145
Two Points To Remember About Trigger Ports 146
Configuring Trigger Port Forwarding 147

Chapter 8
Static Route Screens 149

Static Route Overview 149
Configuring IP Static Route 149
Configuring Route Entry 151

Chapter 9
Firewalls 153

Firewall Overview 153
Types of Firewalls 153
Packet Filtering Firewalls 154
Application-level Firewalls 154
Stateful Inspection Firewalls 154
Introduction to Nortel Networks Firewall 155
Denial of Service 156
Basics 156
Types of DoS Attacks 157
Stateful Inspection 161
Stateful Inspection Process 162
Stateful Inspection and the Contivity 221 163

TCP Security 164
UDP/ICMP Security 165
Upper Layer Protocols 165
Guidelines For Enhancing Security With Your Firewall 166
Packet Filtering Vs. Firewall 166
Packet Filtering: 166
When To Use Filtering 167
Firewall 167
When To Use The Firewall 167

Chapter 10
Firewall Screens. 169

Access Methods 169
Firewall Policies Overview 169
Rule Logic Overview 170
Rule Checklist 171
Security Ramifications 171
Key Fields For Configuring Rules 172
Action 172
Service 172
Source Address 172
Destination Address 172
Connection Direction Examples 172
LAN to WAN Rules 173
WAN to LAN Rules 173
Configuring Firewall 174
Configuring Firewall Rules 177
Configuring Source and Destination Addresses 179
Configuring Custom Ports 180
Example Firewall Rule 181
Predefined Services 185
Alerts 188
Configuring Attack Alert 189
Threshold Values 189
Half-Open Sessions 189

TCP Maximum Incomplete and Blocking Period 190

Chapter 11
Content Filtering 193

Introduction to Content Filtering 193
Restrict Web Features 193
Days and Times 193
Configure Content Filtering 193

Chapter 12
Introduction to IPSec 197

VPN Overview 197
IPSec 197
Security Association 197
Other Terminology 198
Encryption 198
Data Confidentiality 198
Data Integrity 198
Data Origin Authentication 198
VPN Applications 198
IPSec Architecture 199
IPSec Algorithms 200
Key Management 201
Encapsulation 201
Transport Mode 201
Tunnel Mode 202
IPSec and NAT 202

Chapter 13
VPN Screens 205

VPN/IPSec Overview 205
IPSec Algorithms 205
AH (Authentication Header) Protocol 205
ESP (Encapsulating Security Payload) Protocol 206
My IP Address 207

Secure Gateway Address 207
Dynamic Secure Gateway Address 208
Summary Screen 208
Keep Alive 212
Nailed Up 213
NAT Traversal 213
NAT Traversal Configuration 214
ID Type and Content 215
ID Type and Content Examples 216
Pre-Shared Key 217
Configuring Contivity Client VPN Rule Setup 217
Configuring Advanced Setup 219
Configuring Branch Office VPN Rule Setup 221
Configuring an IP Policy 229
Port Forwarding Server 235
Configuring a Port Forwarding Server 235
IKE Phases 237
Negotiation Mode 239
Pre-Shared Key 239
Diffie-Hellman (DH) Key Groups 240
Perfect Forward Secrecy (PFS) 240
Configuring Advanced Branch Office Setup 240
SA Monitor 244
Global Settings 246

Chapter 14
Certificates 249

Certificates Overview 249
Advantages of Certificates 250
Self-signed Certificates 250
Configuration Summary 251
My Certificates 251
Certificate File Formats 254
Importing a Certificate 255
Creating a Certificate 256

My Certificate Details 260
Trusted CAs 264
Importing a Trusted CA's Certificate 267
Trusted CA Certificate Details 268
Trusted Remote Hosts 272
Verifying a Trusted Remote Host's Certificate 274
Trusted Remote Host Certificate Fingerprints 274
Importing a Trusted Remote Host's Certificate 276
Trusted Remote Host Certificate Details 277
Directory Servers 281
Add or Edit a Directory Server 282

Chapter 15
Bandwidth Management 285

Bandwidth Management Overview 285
Bandwidth Classes and Filters 286
Proportional Bandwidth Allocation 286
Application-based Bandwidth Management 286
Subnet-based Bandwidth Management 286
Application and Subnet-based Bandwidth Management 287
Reserving Bandwidth for Non-Bandwidth Class Traffic 287
Configuring Summary 288
Configuring Class Setup 289
Bandwidth Manager Class Configuration 291
Bandwidth Management Statistics 294
Monitor 296

Chapter 16
IEEE 802.1x 297

IEEE 802.1x Overview 297
RADIUS 297
Types of RADIUS Messages 297
EAP Authentication Overview 298
Configuring 802.1X 299

Chapter 17
Authentication Server 301

Introduction to Local User Database 301
Configuring Local User Database 301
Configuring RADIUS 303

Chapter 18
Remote Management Screens 307

Remote Management Overview 307
Remote Management Limitations 308
Remote Management and NAT 308
System Timeout 308
Introduction to HTTPS 309
Configuring WWW 310
HTTPS Example 312
Internet Explorer Warning Messages 313
Netscape Navigator Warning Messages 313
Avoiding the Browser Warning Messages 314
Login Screen 316
SSH Overview 319
How SSH works 320
SSH Implementation on the Contivity 221 321
Requirements for Using SSH 321
Configuring SSH 321
Secure Telnet Using SSH Examples 323
Example 1: Microsoft Windows 323
Example 2: Linux 324
Secure FTP Using SSH Example 325
Telnet 325
Configuring TELNET 326
Configuring FTP 327
Configuring SNMP 329
Supported MIBs 330
SNMP Traps 331
REMOTE MANAGEMENT: SNMP 331

Configuring DNS 333
Configuring Security 334

Chapter 19
UPnP 337

Universal Plug and Play Overview 337
How Do I Know If I'm Using UPnP? 337
NAT Traversal 337
Cautions with UPnP 338
UPnP Implementation 338
Configuring UPnP 338
Displaying UPnP Port Mapping 340
Installing UPnP in Windows Example 341
Installing UPnP in Windows Me 341
Installing UPnP in Windows XP 342
Using UPnP in Windows XP Example 344
Auto-discover Your UPnP-enabled Network Device 344
WebGUI Easy Access 347

Chapter 20
Logs Screens 349

Configuring View Log 349
Configuring Log Settings 351
Configuring Reports 354
Viewing Web Site Hits 356
Viewing Protocol/Port 357
Viewing LAN IP Address 359
Reports Specifications 361

Chapter 21
Call Scheduling Screens 363

Call Scheduling Introduction 363
Call Schedule Summary 363
Call Scheduling Edit 365
Applying Schedule Set(s) to a Remote Node 367

Chapter 22
Maintenance 369

Maintenance Overview 369
Status Screen 369
System Statistics 371
DHCP Table Screen 372
F/W Upload Screen 373
Configuration Screen 376
Back to Factory Defaults 377
Backup Configuration 378
Restore Configuration 378
Restart Screen 380

Chapter 23
Introducing the SMT 381

Introduction to the SMT 381
Accessing the SMT via the Console Port 381
Initial Screen 381
Logging Into the SMT 382
Navigating the SMT Interface 382
Main Menu 384
Changing the System Password 385
Note that as you type a password, the screen displays an asterisk “*” for each character you type. 387
SMT Menus at a Glance 387
Resetting the Contivity 221 389

Chapter 24
SMT Menu 1 - General Setup 391

Introduction to General Setup 391
Configuring General Setup 391
Configuring Dynamic DNS 394

Chapter 25
WAN and Dial Backup Setup 399

Introduction to WAN and Dial Backup Setup 399
WAN Setup 399
Dial Backup 401
Configuring Dial Backup in Menu 2 401
Advanced WAN Setup 403
Remote Node Profile (Backup ISP) 405
Editing PPP Options 408
Editing TCP/IP Options 409
Editing Login Script 412
Remote Node Filter 415

Chapter 26
LAN Setup 417

Introduction to LAN Setup 417
Accessing the LAN Menus 417
LAN Port Filter Setup 417
IP Alias Setup 421

Chapter 27
Internet Access 425

Introduction to Internet Access Setup 425
Ethernet Encapsulation 425
Configuring the PPTP Client 427
Configuring the PPPoE Client 428
Basic Setup Complete 430

Chapter 28
Remote Node Setup 431

Introduction to Remote Node Setup 431
Remote Node Setup 431
Remote Node Profile Setup 432
Ethernet Encapsulation 432
PPPoE Encapsulation 434

Outgoing Authentication Protocol 435
Nailed-Up Connection 436
PPTP Encapsulation 437
Edit IP 438
Remote Node Filter 441
Traffic Redirect Setup 443

Chapter 29
IP Static Route Setup 447

IP Static Route Setup 447

Chapter 30
Dial-in User Setup 451

Dial-in User Setup 451

Chapter 31
Network Address Translation (NAT) 453

Using NAT 453
SUA (Single User Account) Versus NAT 453
Applying NAT 453
NAT Setup 456
Address Mapping Sets 456
SUA Address Mapping Set 457
User-Defined Address Mapping Sets 459
Ordering Your Rules 460
Configuring a Server behind NAT 463
General NAT Examples 465
Internet Access Only 465
Example 2: Internet Access with an Inside Server 467
Example 3: Multiple Public IP Addresses With Inside Servers 468
Configuring Trigger Port Forwarding 473

Chapter 32
Introducing the Firewall 477

Using SMT Menus 477

Activating the Firewall 477

Chapter 33
Filter Configuration 479

Introduction to Filters 479
Filter Structure 480
Configuring a Filter Set 482
Configuring a Filter Rule 485
Configuring a TCP/IP Filter Rule 485
Configuring a Generic Filter Rule 489
Example Filter 492
Filter Types and NAT 495
Firewall Versus Filters 495
Applying a Filter 496
Applying LAN Filters 496
Applying Remote Node Filters 497

Chapter 34
SNMP Configuration 499

SNMP Configuration 499
SNMP Traps 500

Chapter 35
System Security 503

System Security 503
System Password 503
Configuring External RADIUS Server 503
IEEE 802.1x 505

Chapter 36
System Information & Diagnosis 509

Introduction to System Status 509
System Status 510
System Information and Console Port Speed 512

Chapter 37
System Information 513

Console Port Speed 514
Log and Trace 514
Syslog Logging 515
CDR 517
Packet Triggered 517
Filter Log 518
PPP Log 518
Firewall Log 519
Call-Triggering Packet 519
WAN DHCP 522

Chapter 38
Firmware and Configuration File Maintenance 525

Filename Conventions 525
Backup Configuration 526
Backup Configuration 527
Using the FTP Command from the Command Line 527
Example of FTP Commands from the Command Line 528
GUI-based FTP Clients 528
TFTP and FTP over WAN Management Limitations 529
Backup Configuration Using TFTP 529
TFTP Command Example 530
GUI-based TFTP Clients 530
Backup Via Console Port 531
Restore Configuration 532
Restore Using FTP 533
Restore Using FTP Session Example 534
Restore Via Console Port 534
Uploading Firmware and Configuration Files 536
Firmware File Upload 536
Configuration File Upload 537
FTP File Upload Command from the DOS Prompt Example 538
FTP Session Example of Firmware File Upload 538

TFTP File Upload 539
TFTP Upload Command Example 539
Uploading Via Console Port 540
Uploading Firmware File Via Console Port 540
Example Xmodem Firmware Upload Using HyperTerminal 541
Uploading Configuration File Via Console Port 542
Example Xmodem Configuration Upload Using HyperTerminal 543

Chapter 39
System Maintenance Menus 8 to 10 545

Command Interpreter Mode 545
Command Syntax 546
Command Usage 547
Call Control Support 548
Budget Management 548
Call History 550
Time and Date Setting 551
Resetting the Time 554

Chapter 40
Remote Management 555

Remote Management 555
Remote Management Limitations 557

Chapter 41
Call Scheduling 559

Introduction 559

Appendix A
Troubleshooting 563

Problems Starting Up the Contivity 221 563
Problems with the LAN LED 564
Problems with the LAN Interface 564
Problems with the WAN Interface 564
Problems with Internet Access 565

Problems Accessing an Internet Web Site 566
Problems with the Password 566
Problems with the WebGUI 567
Problems with Remote Management 567
Allowing Pop-up Windows, JavaScript and Java Permissions 567
Internet Explorer Pop-up Blockers 568
Allowing Pop-ups 568
Enabling Pop-up Blockers with Exceptions 569
Internet Explorer JavaScript 571
Internet Explorer Java Permissions 573
JAVA (Sun) 574
Netscape Pop-up Blockers 575
Allowing Pop-ups 575
Enable Pop-up Blockers with Exceptions 577
Netscape Java Permissions and JavaScript 579

Appendix B
Setting up Your Computer's IP Address 583

Windows 95/98/Me 583
Installing Components 584
Configuring 585
Verifying Settings 587
Windows 2000/NT/XP 588
Verifying Settings 591
Macintosh OS 8/9 592
Verifying Settings 593
Macintosh OS X 594
Verifying Settings 595

Appendix C
Triangle Route 597

The Ideal Setup 597
The "Triangle Route" Problem 597
The "Triangle Route" Solutions 598
IP Aliasing 598

Gateways on the WAN Side 599

Appendix D
Importing Certificates 601

Import Contivity 221 Certificates into Netscape Navigator 601
Importing the Contivity 221's Certificate into Internet Explorer 602
Enrolling and Importing SSL Client Certificates 608
Using a Certificate When Accessing the Contivity 221 Example 615

Appendix E
PPPoE 617

PPPoE in Action 617
Benefits of PPPoE 617
Traditional Dial-up Scenario 618
How PPPoE Works 618
Contivity 221 as a PPPoE Client 619

Appendix F
PPTP 621

What is PPTP? 621
How can we transport PPP frames from a PC to a broadband modem over Ethernet? 621
PPTP and the Contivity 221 622
PPTP Protocol Overview 622
Control & PPP connections 623
Call Connection 623
PPP Data Connection 624

Appendix G
Hardware Specifications 625

Cable Pin Assignments 625
Power Adaptor Specifications 627

Appendix H

IP Subnetting 631

IP Addressing 631
IP Classes 631
Subnet Masks 633
Subnetting 633
Example: Two Subnets 634
Example: Four Subnets 636
Example Eight Subnets 638
Subnetting With Class A and Class B Networks. 639

Appendix I
Command Interpreter 641

Command Syntax 641
Command Usage 641
Sys Commands 642
Device Commands 650
Exit Command 651
Ethernet Commands 651
IP Commands 652
PPPoE Commands 660
PPTP Commands 661
Configuration Commands 661
IPSec Commands 667
Sys Firewall Commands 673
Bandwidth Management Commands 674
Certificates Commands 676
RADIUS Commands 680
IEEE 802.1X Commands 681

Appendix J
NetBIOS Filter Commands 683

Introduction 683
Display NetBIOS Filter Settings 683
NetBIOS Filter Configuration 684
Example commands 685

Appendix K
Boot Commands 687

Appendix L
Log Descriptions 689

VPN/IPSec Logs 699
VPN Responder IPSec Log 699
Log Commands 708
Configuring What You Want the Contivity 221 to Log 708
Displaying Logs 709
Log Command Example 710

Appendix M
Brute-Force Password Guessing Protection 711

Appendix N
SIP 713

SIP Identities 713
SIP Number 713
SIP Service Domain 714
SIP Call Progression 714
SIP Servers 715
SIP User Agent Server 715
SIP Proxy Server 715
SIP Redirect Server 716
SIP Register Server 717
RTP 717
Index 723

Figures

Figure 1 Secure Internet Access and VPN Application 59
Figure 2 Login Screen 62
Figure 3 Change Password Screen 62
Figure 4 Replace Certificate Screen 63
Figure 5 Example Xmodem Upload 64
Figure 6 MAIN MENU Screen 65
Figure 7 Wizard 1 68
Figure 8 Wizard 2: Ethernet Encapsulation 69
Figure 9 Wizard 2: PPTP Encapsulation 70
Figure 10 Wizard2: PPPoE Encapsulation 73
Figure 11 Wizard 3 77
Figure 12 Private DNS Server Example 82
Figure 13 System General Setup 83
Figure 14 DDNS 86
Figure 15 Password 88
Figure 16 Time and Date 91
Figure 17 ALG 94
Figure 18 IP 100
Figure 19 Static DHCP 103
Figure 20 IP Alias 105
Figure 21 WAN: Route 109
Figure 22 Ethernet Encapsulation 110
Figure 23 PPPoE Encapsulation 112
Figure 24 PPTP Encapsulation 113
Figure 25 RR Service Type 115
Figure 26 WAN: IP 116
Figure 27 MAC Setup 119
Figure 28 Traffic Redirect WAN Setup 120
Figure 29 Traffic Redirect LAN Setup 121

Figure 30 Traffic Redirect 122
Figure 31 Dial Backup Setup 124
Figure 32 Advanced Setup 129
Figure 33 How NAT Works 133
Figure 34 Port Restricted Cone NAT 134
Figure 35 NAT Application With IP Alias 135
Figure 36 Multiple Servers Behind NAT Example 139
Figure 37 SUA/NAT Setup 140
Figure 38 Address Mapping 142
Figure 39 Address Mapping Edit 144
Figure 40 Trigger Port Forwarding Process: Example 146
Figure 41 Trigger Port 147
Figure 42 Example of Static Routing Topology 149
Figure 43 Static Route Screen 150
Figure 44 Edit IP Static Route 151
Figure 45 Contivity 221 Firewall Application 156
Figure 46 Three-Way Handshake 158
Figure 47 SYN Flood 159
Figure 48 Smurf Attack 160
Figure 49 Stateful Inspection 162
Figure 50 LAN to WAN Traffic 173
Figure 51 WAN to LAN Traffic 174
Figure 52 Enabling the Firewall 175
Figure 53 Creating/Editing A Firewall Rule 178
Figure 54 Adding/Editing Source and Destination Addresses 180
Figure 55 Creating/Editing A Custom Port 181
Figure 56 Firewall Edit Rule Screen Example 182
Figure 57 Firewall Rule Edit IP Example 183
Figure 58 Edit Custom Port Example 183
Figure 59 MyService Rule Configuration Example 184
Figure 60 My Service Example Rule Summary 185
Figure 61 Attack Alert 191
Figure 62 Content Filter 194
Figure 63 Encryption and Decryption 198
Figure 64 IPSec Architecture 200

Figure 65 Transport and Tunnel Mode IPSec Encapsulation 201
Figure 66 IPSec Summary Fields 208
Figure 67 Summary 209
Figure 68 NAT Router Between VPN Switches 214
Figure 69 VPN Contivity Client Rule Setup 218
Figure 70 VPN Contivity Client Advanced Rule Setup 220
Figure 71 VPN Branch Office Rule Setup 222
Figure 72 VPN Branch Office - IP Policy 230
Figure 73 VPN Branch Office - IP Policy - Port Forwarding Server 236
Figure 74 Two Phases to Set Up the IPSec SA 238
Figure 75 VPN Branch Office Advanced Rule Setup 241
Figure 76 VPN SA Monitor 245
Figure 77 VPN Global Setting 246
Figure 78 Certificate Configuration Overview 251
Figure 79 My Certificates 252
Figure 80 My Certificate Import 256
Figure 81 My Certificate Create 257
Figure 82 My Certificate Details 261
Figure 83 Trusted CAs 265
Figure 84 Trusted CA Import 267
Figure 85 Trusted CA Details 269
Figure 86 Trusted Remote Hosts 273
Figure 87 Remote Host Certificates 275
Figure 88 Certificate Details 275
Figure 89 Trusted Remote Host Import 276
Figure 90 Trusted Remote Host Details 278
Figure 91 Directory Servers 281
Figure 92 Directory Server Add 283
Figure 93 Subnet-based Bandwidth Management Example 287
Figure 94 Bandwidth Manager: Summary 288
Figure 95 Bandwidth Manager: Class Setup 290
Figure 96 Bandwidth Manager: Edit Class 292
Figure 97 Bandwidth Management Statistics 295
Figure 98 Bandwidth Manager Monitor 296
Figure 99 EAP Authentication 299

Figure 100 802.1X 300
Figure 101 Local User Database 302
Figure 102 RADIUS 304
Figure 103 HTTPS Implementation 310
Figure 104 WWW 311
Figure 105 Security Alert Dialog Box (Internet Explorer) 313
Figure 106 Figure 18-4 Security Certificate 1 (Netscape) 314
Figure 107 Security Certificate 2 (Netscape) 314
Figure 108 Login Screen (Internet Explorer) 316
Figure 109 Login Screen (Netscape) 317
Figure 110 Replace Certificate 318
Figure 111 Device-specific Certificate 318
Figure 112 Common Contivity 221 Certificate 319
Figure 113 SSH Communication Example 320
Figure 114 How SSH Works 320
Figure 115 SSH 322
Figure 116 SSH Example 1: Store Host Key 323
Figure 117 SSH Example 2: Test 324
Figure 118 SSH Example 2: Log in 324
Figure 119 Secure FTP: Firmware Upload Example 325
Figure 120 Telnet Configuration on a TCP/IP Network 326
Figure 121 Telnet 327
Figure 122 FTP 328
Figure 123 SNMP Management Model 329
Figure 124 SNMP 332
Figure 125 DNS 334
Figure 126 Security 335
Figure 127 Configuring UPnP 339
Figure 128 UPnP Ports 340
Figure 129 Add/Remove Programs: Windows Setup 342
Figure 130 Communications 342
Figure 131 Network Connections 343
Figure 132 Windows Optional Networking Components Wizard 343
Figure 133 Windows XP Networking Services 344
Figure 134 Internet Gateway Icon 345

Figure 135 Internet Connection Properties 345
Figure 136 Internet Connection Properties Advanced Setup 346
Figure 137 Service Settings 346
Figure 138 Internet Connection Icon 347
Figure 139 Internet Connection Status 347
Figure 140 Network Connections 348
Figure 141 My Network Places: Local Network 348
Figure 142 View Log 350
Figure 143 Log Settings 352
Figure 144 Reports 355
Figure 145 Web Site Hits Report Example 357
Figure 146 Protocol/Port Report Example 358
Figure 147 LAN IP Address Report Example 360
Figure 148 Call Schedule Summary 364
Figure 149 Call Schedule Edit 366
Figure 150 Applying Schedule Set(s) to a Remote Node 368
Figure 151 System Status 370
Figure 152 System Status: Show Statistics 371
Figure 153 DHCP Table 373
Figure 154 Firmware Upload 374
Figure 155 Firmware Upload In Process 375
Figure 156 Network Temporarily Disconnected 375
Figure 157 Firmware Upload Error 376
Figure 158 Configuration 377
Figure 159 Reset Warning Message 378
Figure 160 Configuration Upload Successful 379
Figure 161 Network Temporarily Disconnected 379
Figure 162 Restart Screen 380
Figure 163 Initial Screen 382
Figure 164 SMT Login 382
Figure 165 Main Menu 384
Figure 166 Menu 23.1 System Security: Change Password 385
Figure 167 SMT Overview 388
Figure 168 Menu 1: General Setup 391
Figure 169 Configure Dynamic DNS 395

Figure 170 Menu 2. 400
Figure 171 Menu 2: Dial Backup Setup 402
Figure 172 Menu 2.1 Advanced WAN Setup 404
Figure 173 Menu 11.2 Remote Node Profile (Backup ISP) 406
Figure 174 Menu 11.2.1: Remote Node PPP Options 409
Figure 175 Menu 11.2.2: Remote Node Network Layer Options 410
Figure 176 Menu 11.2.3: Remote Node Setup Script 414
Figure 177 Menu 11.2.4: Dial Backup Remote Node Filter 415
Figure 178 Menu 3: LAN Setup. 417
Figure 179 Menu 3.1: LAN Port Filter Setup 418
Figure 180 Menu 3: TCP/IP and DHCP Setup 418
Figure 181 Figure 21-4 Menu 3.2: TCP/IP and DHCP Ethernet Setup 419
Figure 182 Menu 3.2.1: IP Alias Setup 422
Figure 183 Menu 4: Internet Access Setup (Ethernet) 426
Figure 184 Internet Access Setup (PPTP) 428
Figure 185 Internet Access Setup (PPPoE) 429
Figure 186 Menu 11 Remote Node Setup 432
Figure 187 Menu 11.1: Remote Node Profile for Ethernet Encapsulation 433
Figure 188 Menu 11.1: Remote Node Profile for PPPoE Encapsulation 435
Figure 189 Menu 11.1: Remote Node Profile for PPTP Encapsulation 437
Figure 190 Menu 11.1.2: Remote Node Network Layer Options for Ethernet Encapsulation 439
Figure 191 Menu 11.1.4: Remote Node Filter (Ethernet Encapsulation) 442
Figure 192 Menu 11.1.4: Remote Node Filter (PPPoE or PPTP Encapsulation) . . . 442
Figure 193 Menu 11.1: Remote Node Profile 443
Figure 194 Menu 11.1.5: Traffic Redirect Setup 444
Figure 195 Menu 12: IP Static Route Setup 448
Figure 196 Menu 12. 1: Edit IP Static Route 449
Figure 197 Menu 14- Dial-in User Setup 451
Figure 198 Menu 14.1- Edit Dial-in User 452
Figure 199 Menu 4: Applying NAT for Internet Access 454
Figure 200 Menu 11.1.2: Applying NAT to the Remote Node 455
Figure 201 Menu 15: NAT Setup 456
Figure 202 Menu 15.1: Address Mapping Sets 457
Figure 203 Menu 15.1.255: SUA Address Mapping Rules 458

Figure 204 Menu 15.1.1: First Set 460
Figure 205 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set 462
Figure 206 Menu 15.2: NAT Server Setup 464
Figure 207 Multiple Servers Behind NAT Example 465
Figure 208 NAT Example 1 466
Figure 209 Menu 4: Internet Access & NAT Example 466
Figure 210 NAT Example 2 467
Figure 211 Menu 15.2: Specifying an Inside Server 468
Figure 212 NAT Example 3 469
Figure 213 Example 3: Menu 11.1.2 470
Figure 214 Example 3: Menu 15.1.1.1 471
Figure 215 Example 3: Final Menu 15.1.1 472
Figure 216 Example 3: Menu 15.2 473
Figure 217 Menu 15.3: Trigger Port Setup 474
Figure 218 Menu 21: Filter and Firewall Setup 477
Figure 219 Menu 21.2: Firewall Setup 478
Figure 220 Outgoing Packet Filtering Process 480
Figure 221 Filter Rule Process 481
Figure 222 Menu 21: Filter and Firewall Setup 482
Figure 223 Menu 21.1: Filter Set Configuration 483
Figure 224 Menu 21.1.1.1: TCP/IP Filter Rule 486
Figure 225 Executing an IP Filter 489
Figure 226 Menu 21.1.1.1: Generic Filter Rule 490
Figure 227 Telnet Filter Example 492
Figure 228 Example Filter: Menu 21.1.3.1 493
Figure 229 Example Filter Rules Summary: Menu 21.1.3 494
Figure 230 Protocol and Device Filter Sets 495
Figure 231 Filtering LAN Traffic 497
Figure 232 Filtering Remote Node Traffic 497
Figure 233 Menu 22: SNMP Configuration 499
Figure 234 Menu 23 System Security 503
Figure 235 Menu 23 System Security 504
Figure 236 Menu 23.2 System Security: RADIUS Server 504
Figure 237 Menu 23 System Security 506
Figure 238 Menu 23.4 System Security: IEEE802.1x 506

Figure 239 Menu 24: System Maintenance 510
Figure 240 Menu 24.1: System Maintenance: Status 511
Figure 241 System Information and Console Port Speed 512
Figure 242 Menu 24.2.1: System Maintenance Information: 513
Figure 243 Menu 24.2.2: System Maintenance: Change Console Port Speed 514
Figure 244 Menu 24.3: System Maintenance: Log and Trace 515
Figure 245 Menu 24.3.2: System Maintenance: Syslog Logging 515
Figure 246 Call-Triggering Packet Example 520
Figure 247 Menu 24.4: System Maintenance: Diagnostic 521
Figure 248 WAN & LAN DHCP 522
Figure 249 Menu 24.5 - System Maintenance - Backup Configuration 527
Figure 250 FTP Session Example 528
Figure 251 Menu 24.5 System Maintenance: Backup Configuration 531
Figure 252 Menu 24.5 System Maintenance: Starting Xmodem Download Screen . 531
Figure 253 Backup Configuration Example 532
Figure 254 Successful Backup Confirmation Screen 532
Figure 255 Telnet into Menu 24.6 533
Figure 256 Restore Using FTP Session Example 534
Figure 257 System Maintenance: Restore Configuration 534
Figure 258 System Maintenance: Starting Xmodem Download Screen 535
Figure 259 Successful Restoration Confirmation Screen 536
Figure 260 Telnet Into Menu 24.7.1 Upload System Firmware 537
Figure 261 Telnet Into Menu 24.7.2 System Maintenance 537
Figure 262 FTP Session Example of Firmware File Upload 538
Figure 263 Menu 24.7.1 as seen using the Console Port 541
Figure 264 Example Xmodem Upload 542
Figure 265 Menu 24.7.2 as seen using the Console Port 543
Figure 266 Example Xmodem Upload 544
Figure 267 Command Mode in Menu 24 546
Figure 268 Valid Commands 547
Figure 269 Call Control 548
Figure 270 Budget Management 549
Figure 271 Call History 550
Figure 272 Menu 24: System Maintenance 551
Figure 273 Menu 24.10 System Maintenance: Time and Date Setting 552

Figure 274 Menu 24.11 – Remote Management Control 556
Figure 275 Menu 26 Schedule Setup 559
Figure 276 Menu 26.1 Schedule Set Setup 560
Figure 277 Applying Schedule Set(s) to a Remote Node (PPPoE) 562
Figure 278 Pop-up Blocker 568
Figure 279 Internet Options 569
Figure 280 Internet Options 570
Figure 281 Pop-up Blocker Settings 571
Figure 282 Internet Options 572
Figure 283 Security Settings - Java Scripting 573
Figure 284 Security Settings - Java 574
Figure 285 Java (Sun) 575
Figure 286 Allow Popups From This Site 576
Figure 287 Netscape Search Toolbar 576
Figure 288 Popup Windows 577
Figure 289 Popup Windows 578
Figure 290 Allowed Sites 579
Figure 291 Advanced 580
Figure 292 Scripts & Plug-ins 581
Figure 293 WIndows 95/98/Me: Network: Configuration 584
Figure 294 Windows 95/98/Me: TCP/IP Properties: IP Address 586
Figure 295 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 587
Figure 296 Windows XP: Start Menu 588
Figure 297 Windows XP: Control Panel 588
Figure 298 Windows XP: Control Panel: Network Connections: Properties 589
Figure 299 Windows XP: Local Area Connection Properties 589
Figure 300 Windows XP: Advanced TCP/IP Settings 590
Figure 301 Windows XP: Internet Protocol (TCP/IP) Properties 591
Figure 302 Macintosh OS 8/9: Apple Menu 592
Figure 303 Macintosh OS 8/9: TCP/IP 593
Figure 304 Macintosh OS X: Apple Menu 594
Figure 305 Macintosh OS X: Network 594
Figure 306 Ideal Setup 597
Figure 307 “Triangle Route” Problem 598
Figure 308 IP Alias 599

Figure 309 Gateways on the WAN Side 599
Figure 310 Security Certificate 602
Figure 311 Login Screen 603
Figure 312 Certificate General Information before Import 604
Figure 313 Certificate Import Wizard 1 605
Figure 314 Certificate Import Wizard 2 606
Figure 315 Certificate Import Wizard 3 606
Figure 316 Root Certificate Store 607
Figure 317 Certificate General Information after Import 607
Figure 318 Contivity 221 Trusted CA Screen 609
Figure 319 CA Certificate Example 610
Figure 320 Personal Certificate Import Wizard 1 611
Figure 321 Personal Certificate Import Wizard 2 612
Figure 322 Personal Certificate Import Wizard 3 613
Figure 323 Personal Certificate Import Wizard 4 614
Figure 324 Personal Certificate Import Wizard 5 614
Figure 325 Personal Certificate Import Wizard 6 615
Figure 326 Access the Contivity 221 Via HTTPS 615
Figure 327 SSL Client Authentication 616
Figure 328 Contivity 221 Secure Login Screen 616
Figure 329 Single-PC per Router Hardware Configuration 618
Figure 330 Contivity 221 as a PPPoE Client 619
Figure 331 Transport PPP frames over Ethernet 622
Figure 332 PPTP Protocol Overview 623
Figure 333 Example Message Exchange between PC and an ANT 624
Figure 334 Console/Dial Backup Port Pin Layouts 626
Figure 335 Ethernet Cable Pin Assignments 627
Figure 336 NetBIOS Display Filter Settings Command Example 684
Figure 337 Option to Enter Debug Mode 687
Figure 338 Boot Module Commands 688
Figure 339 Example VPN Initiator IPSec Log 699
Figure 340 Example VPN Responder IPSec Log 700
Figure 341 SIP User Agent Server 715
Figure 342 SIP Proxy Server 716
Figure 343 SIP Redirect Server 717

Figure 344 Contivity 221 SIP ALG 719

Tables

Table 1 Feature Specifications 51
Table 2 Wizard 2: Ethernet Encapsulation 69
Table 3 Wizard 2: PPTP Encapsulation 71
Table 4 Wizard2: PPPoE Encapsulation 73
Table 5 Private IP Address Ranges 74
Table 6 Example of Network Properties for LAN Servers with Fixed IP Addresses 76
Table 7 Wizard 3 77
Table 8 System General Setup 83
Table 9 DDNS 86
Table 10 Password 88
Table 11 Default Time Servers 90
Table 12 Time and Date 92
Table 13 ALG 95
Table 14 IP 100
Table 15 Static DHCP 103
Table 16 IP Alias 105
Table 17 WAN: Route 109
Table 18 Ethernet Encapsulation 110
Table 19 PPPoE Encapsulation 112
Table 20 PPTP Encapsulation 114
Table 21 RR Service Type 115
Table 22 WAN: IP 117
Table 23 Traffic Redirect 122
Table 24 Dial Backup Setup 125
Table 25 Advanced Setup 129
Table 26 NAT Definitions 132
Table 27 NAT Mapping Type 136
Table 28 Services and Port Numbers 138
Table 29 SUA/NAT Setup 140

Table 30 Address Mapping 142
Table 31 Address Mapping Edit 144
Table 32 Trigger Port 147
Table 33 IP Static Route Summary 150
Table 34 Edit IP Static Route 151
Table 35 Common IP Ports 157
Table 36 ICMP Commands That Trigger Alerts 160
Table 37 Legal NetBIOS Commands 160
Table 38 Legal SMTP Commands 161
Table 39 Firewall Rules Summary: First Screen 175
Table 40 Creating/Editing A Firewall Rule 178
Table 41 Adding/Editing Source and Destination Addresses 180
Table 42 Creating/Editing A Custom Port 181
Table 43 Predefined Services 186
Table 44 Attack Alert 191
Table 45 Content Filter 194
Table 46 VPN and NAT 203
Table 47 AH and ESP 206
Table 48 Summary 209
Table 49 Local ID Type and Content Fields 215
Table 51 Matching ID Type and Content Configuration Example 216
Table 50 Peer ID Type and Content Fields 216
Table 52 Mismatching ID Type and Content Configuration Example 217
Table 53 VPN Contivity Client Rule Setup 218
Table 54 VPN Contivity Client Advanced Rule Setup 220
Table 55 VPN Branch Office Rule Setup 223
Table 56 VPN Branch Office - IP Policy 231
Table 57 VPN Branch Office - IP Policy - Port Forwarding Server 236
Table 58 VPN Branch Office Advanced Rule Setup 241
Table 59 VPN SA Monitor 245
Table 60 VPN Global Setting 246
Table 61 My Certificates 252
Table 62 My Certificate Import 256
Table 63 My Certificate Create 258
Table 64 My Certificate Details 262

Table 65 Trusted CAs 265
Table 66 Trusted CA Import 267
Table 67 Trusted CA Details 270
Table 68 Trusted Remote Hosts 273
Table 69 Trusted Remote Host Import 277
Table 70 Trusted Remote Host Details 279
Table 71 Directory Servers 282
Table 72 Directory Server Add 283
Table 73 Application and Subnet-based Bandwidth Management Example 287
Table 74 Bandwidth Manager: Summary 288
Table 75 Bandwidth Manager: Class Setup 290
Table 76 Bandwidth Manager: Edit Class 292
Table 77 Services and Port Numbers 294
Table 78 Bandwidth Management Statistics 295
Table 79 Bandwidth Manager Monitor 296
Table 80 802.1X 300
Table 81 Local User Database 302
Table 82 RADIUS 305
Table 83 WWW 311
Table 84 SSH 322
Table 85 Telnet 327
Table 86 FTP 328
Table 87 SNMP Traps 331
Table 88 SNMP 332
Table 89 DNS 334
Table 90 Security 335
Table 91 Configuring UPnP 339
Table 92 UPnP Ports 340
Table 93 View Log 350
Table 94 Log Settings 353
Table 95 Reports 355
Table 96 Web Site Hits Report 357
Table 97 Protocol/ Port Report 358
Table 98 LAN IP Address Report 360
Table 99 Report Specifications 361

Table 100 Call Schedule Summary 364
Table 101 Call Schedule Edit 366
Table 102 System Status 370
Table 103 System Status: Show Statistics 371
Table 104 DHCP Table 373
Table 105 Firmware Upload 374
Table 106 Restore Configuration 378
Table 107 Main Menu Commands 383
Table 108 Main Menu Summary 384
Table 109 General Setup Menu Fields 392
Table 110 Configure Dynamic DNS Menu Fields 395
Table 111 MAC Address Cloning in WAN Setup 400
Table 112 Menu 2: Dial Backup Setup 402
Table 113 Advanced WAN Port Setup: AT Commands Fields 404
Table 114 Advanced WAN Port Setup: Call Control Parameters 405
Table 115 Fields in Menu 11.2 Remote Node Profile (Backup ISP) 406
Table 116 Remote Node PPP Options Menu Fields 409
Table 117 Remote Node Network Layer Options Menu Fields 410
Table 118 Menu 11.2.3: Remote Node Script Menu Fields 414
Table 119 DHCP Ethernet Setup Menu Fields 419
Table 120 LAN TCP/IP Setup Menu Fields 421
Table 121 IP Alias Setup Menu Field 422
Table 122 Menu 4: Internet Access Setup Menu Fields 426
Table 123 New Fields in Menu 4 (PPTP) Screen 428
Table 124 New Fields in Menu 4 (PPPoE) screen 429
Table 125 Fields in Menu 11.1 433
Table 126 Fields in Menu 11.1 (PPPoE Encapsulation Specific) 436
Table 127 Fields in Menu 11.1 (PPTP Encapsulation) 438
Table 128 Remote Node Network Layer Options Menu Fields 439
Table 129 Menu 11.1: Remote Node Profile (Traffic Redirect Field) 443
Table 130 Menu 11.1.5: Traffic Redirect Setup 444
Table 131 IP Static Route Menu Fields 449
Table 132 Menu 14.1- Edit Dial-in User 452
Table 133 Applying NAT in Menus 4 & 11.1.2 455
Table 134 SUA Address Mapping Rules 458

Table 135 Fields in Menu 15.1.1 461
Table 136 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set 462
Table 137 Menu 15.3: Trigger Port Setup Description 474
Table 138 Abbreviations Used in the Filter Rules Summary Menu 484
Table 139 Rule Abbreviations Used 484
Table 140 TCP/IP Filter Rule Menu Fields 486
Table 141 Generic Filter Rule Menu Fields 491
Table 142 SNMP Configuration Menu Fields 500
Table 143 SNMP Traps 500
Table 144 Menu 23.2 System Security: RADIUS Server 504
Table 145 Menu 23.4 System Security: IEEE802.1x 507
Table 146 System Maintenance: Status Menu Fields 511
Table 147 Fields in System Maintenance: Information 514
Table 148 System Maintenance Menu Syslog Parameters 515
Table 149 System Maintenance Menu Diagnostic 522
Table 150 Filename Conventions 526
Table 151 General Commands for GUI-based FTP Clients 528
Table 152 General Commands for GUI-based TFTP Clients 530
Table 153 Valid Commands 547
Table 154 Budget Management 549
Table 155 Call History Fields 550
Table 156 Time and Date Setting Fields 552
Table 157 Menu 24.11 – Remote Management Control 556
Table 158 Menu 26.1 Schedule Set Setup 561
Table 159 Troubleshooting the Start-Up of Your Contivity 221 563
Table 160 Troubleshooting the LAN LED 564
Table 161 Troubleshooting the LAN Interface 564
Table 162 Troubleshooting the WAN Interface 564
Table 163 Troubleshooting Internet Access 565
Table 164 Troubleshooting Web Site Internet Access 566
Table 165 Troubleshooting the Password 566
Table 166 Troubleshooting the WebGUI 567
Table 167 Troubleshooting Remote Management 567
Table 168 General Specifications 625
Table 169 Console/Dial Backup Port Pin Assignments 626

Table 170 North American AC Power Adaptor Specifications 627
Table 171 European Union AC Power Adaptor Specifications 627
Table 172 UK AC Power Adaptor Specifications 628
Table 173 Japan AC Power Adaptor Specifications 628
Table 174 Australia and New Zealand AC Power Adaptor Specification 629
Table 175 Classes of IP Addresses 632
Table 176 Allowed IP Address Range By Class 632
Table 177 “Natural” Masks 633
Table 178 Alternative Subnet Mask Notation 634
Table 179 Subnet 1 635
Table 180 Subnet 2 635
Table 181 Subnet 1 636
Table 182 Subnet 2 637
Table 183 Subnet 3 637
Table 184 Subnet 4 637
Table 185 Eight Subnets 638
Table 186 Class C Subnet Planning 638
Table 187 Class B Subnet Planning 639
Table 188 Sys Commands 642
Table 189 Device Commands 650
Table 190 Exit Command 651
Table 191 Ether Commands 651
Table 192 IP Commands 652
Table 193 PPPoE Commands 660
Table 194 PPTP Commands 661
Table 195 Config Commands 661
Table 196 IPSec Commands 667
Table 197 Sys Firewall Commands 673
Table 198 Bandwidth Management Commands 674
Table 199 Certificates Commands 676
Table 200 RADIUS Commands 680
Table 201 IEEE 802.1X Commands 681
Table 202 NetBIOS Filter Default Settings 684
Table 203 System Error Logs 689
Table 204 System Maintenance Logs 689

Table 205 UPnP Logs 690
Table 206 Content Filtering Logs 690
Table 207 Attack Logs 691
Table 208 Access Logs 693
Table 209 ACL Setting Notes 697
Table 210 ICMP Notes 697
Table 211 Sys log 698
Table 212 Sample IKE Key Exchange Logs 701
Table 213 Sample IPSec Logs During Packet Transmission 703
Table 214 RFC-2408 ISAKMP Payload Types 704
Table 215 PKI Logs 704
Table 216 Certificate Path Verification Failure Reason Codes 706
Table 217 IEEE 802.1X Logs 707
Table 218 Log Categories and Available Settings 708
Table 219 Brute-Force Password Guessing Protection Commands 711
Table 220 SIP Call Progression 714

Preface

Congratulations on your purchase of the Contivity 221 VPN Switch.

Before you begin

This manual is designed to guide you through the configuration of your Contivity 221 for its various applications.

This manual may refer to the Contivity 221 VPN Switch as the Contivity 221.



Note: You may use the System Management Terminal (SMT), WebGUI or command interpreter interface to configure your Contivity 221. Not all features can be configured through all interfaces. This User's Guide primarily shows SMT configuration but includes the other interfaces where appropriate.

The WebGUI parts of this guide contain background information on features configurable by the WebGUI and the SMT. The SMT parts of this guide contain background information solely on features not configurable by the WebGUI.

Text conventions

This guide uses the following text conventions:

“Enter” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to use one of the predefined choices.

The SMT menu titles and labels are in **Bold Times New Roman** font.

The choices of a menu item are in **Bold Arial** font.

"Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to use one of the predefined choices.

A single keystroke is in Arial font and enclosed in square brackets, for instance, [ENTER] means the Enter, or carriage return, key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.

Mouse action sequences are denoted using a comma. For example, "click the **Apple** icon, **Control Panels** and then **Modem**" means first click the **Apple** icon, then point your mouse pointer to **Control Panels** and then click **Modem**.

For brevity's sake, we will use "e.g." as a shorthand for "for instance" and "i.e." for "that is" or "in other words" throughout this manual.

Related publications

For more information about using the Contivity 221 VPN Switch, refer to the following publications:

- *Quick Start Guide*

  The *Quick Start Guide* is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- *WebGUI Online Help*

  Embedded WebGUI help for descriptions of individual screens and supplementary information

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

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

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.

Chapter 1
Getting to Know Your Contivity 221

This chapter introduces the main features and applications of the Contivity 221.

Introducing the Contivity 221

The Contivity 221 VPN Switch is an ideal secure gateway for all data passing between the Internet and the LAN.

By integrating NAT, firewall and VPN capability, Nortel Networks' Contivity 221 is a complete security solution that protects your Intranet and efficiently manages data traffic on your network.

The embedded WebGUI is easy to operate and totally independent of your operating system platform.

Features

This section lists the Contivity 221's key features.

Table 1 Feature Specifications

Feature	Specification
Number of Static Routes	12
Number of NAT Sessions	1024
Number of SUA Servers	12
Number of Address Mapping Rules	10

Table 1 Feature Specifications

Feature	Specification
Number of IPSec VPN Tunnels/Security Phase 1 Associations	5
Number of IPSec VPN Tunnels/Security Phase 2 Associations	60

Physical Features

4-Port Switch

A combination of switch and router makes your Contivity 221 a cost-effective and viable network solution. You can connect up to four computers to the Contivity 221 without the cost of a hub. Use a hub to add more than four computers to your LAN.

Auto-negotiating 10/100 Mbps Ethernet LAN

The LAN interfaces automatically detect if they are on a 10 or a 100 Mbps Ethernet.

Auto-sensing 10/100 Mbps Ethernet LAN

The LAN interfaces automatically adjust to either a crossover or straight-through Ethernet cable.

Auto-negotiating 10/100 Mbps Ethernet WAN

The 10/100 Mbps Ethernet WAN port attaches to the Internet via broadband modem or router and automatically detects if it's on a 10 or a 100 Mbps Ethernet.

Auxiliary Port

The Contivity 221 uses the same port for console management and for an auxiliary WAN backup. The AUX port can be used in reserve as a traditional dial-up connection when/if ever the broadband connection to the WAN port fails.

Time and Date

The Contivity 221 allows you to get the current time and date from an external server when you turn on your Contivity 221. You can also set the time manually.

Reset Button

The Contivity 221 reset button is built into the rear panel. Use this button to restore the factory default password to setup, IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.3.

Non-Physical Features

IPSec VPN Capability

Establish Virtual Private Network (VPN) tunnels to connect (home) office computers to your company network using data encryption and the Internet; thus providing secure communications without the expense of leased site-to-site lines. VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.



Note: The Contivity 221 supports five simultaneous VPN connections.

Certificates

The Contivity 221 can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.

SSH

The Contivity 221 uses the SSH (Secure Shell) secure communication protocol to provide secure encrypted communication between two hosts over an unsecured network.

HTTPS

HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL is a web protocol that encrypts and decrypts web sessions. Use HTTPS for secure WebGUI access to the Contivity 221

IEEE 802.1x for Network Security

The Contivity 221 supports the IEEE 802.1x standard for user authentication. With the local user profile, the Contivity 221 allows you to configure up 32 user profiles without a network authentication server. In addition, centralized user and accounting management is possible on an optional network authentication server.

Firewall

The Contivity 221 has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The Contivity 221 firewall supports TCP/UDP inspection, DoS detection and protection, real time alerts, reports and logs.

Brute-Force Password Guessing Protection

The Contivity 221 has a special protection mechanism to discourage brute-force password guessing attacks on the Contivity 221's management interfaces. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered. Please see the appendices for details about this feature.

Content Filtering

The Contivity 221 can block web features such as ActiveX controls, Java applets and cookies, as well as disable web proxies. The Contivity 221 can block specific URLs by using the keyword feature. It also allows the administrator to define time periods and days during which content filtering is enabled.

Packet Filtering

The packet filtering mechanism blocks unwanted traffic from entering/leaving your network.

Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the Contivity 221 and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

Call Scheduling

Configure call time periods to restrict and allow access for users on remote nodes.

PPPoE

PPPoE facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The Contivity 221 supports one PPTP server connection at any given time.

Dynamic DNS Support

With Dynamic DNS (Domain Name System) support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

IP Multicast

Deliver IP packets to a specific group of hosts using IP multicast. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236); the Contivity 221 supports both versions 1 and 2.

IP Alias

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The Contivity 221 supports three logical LAN interfaces via its single physical Ethernet LAN interface with the Contivity 221 itself as the gateway for each LAN network.

Central Network Management

Central Network Management (CNM) allows an enterprise or service provider network administrator to manage your Contivity 221. The enterprise or service provider network administrator can configure your Contivity 221, perform firmware upgrades and do troubleshooting for you.

SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Contivity 221 supports SNMP agent functionality, which allows a manager station to manage and monitor the Contivity 221 through the network. The Contivity 221 supports SNMP version one (SNMPv1).

Network Address Translation (NAT)

NAT (Network Address Translation - NAT, RFC 1631) allows the translation of multiple IP addresses used within one network to different IP addresses known within another network.

Traffic Redirect

Traffic Redirect forwards WAN traffic to a backup gateway when the Contivity 221 cannot connect to the Internet, thus acting as an auxiliary backup when your regular WAN connection fails.

Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Contivity 221 has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client.

Full Network Management

The embedded WebGUI is an all-platform web-based utility that allows you to easily access the Contivity 221's management settings and configure the firewall. The Contivity 221 also provides the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection.

RoadRunner Support

In addition to standard cable modem services, the Contivity 221 supports Time Warner's RoadRunner Service.

Logging and Tracing

- Built-in message logging and packet tracing.
- Unix syslog facility support.
- Firewall logs.
- Content filtering logs.

Upgrade Contivity 221 Firmware

The firmware of the Contivity 221 can be upgraded via the console port or the LAN.

Embedded FTP and TFTP Servers

The Contivity 221's embedded FTP and TFTP Servers enable fast firmware upgrades as well as configuration file backups and restoration.

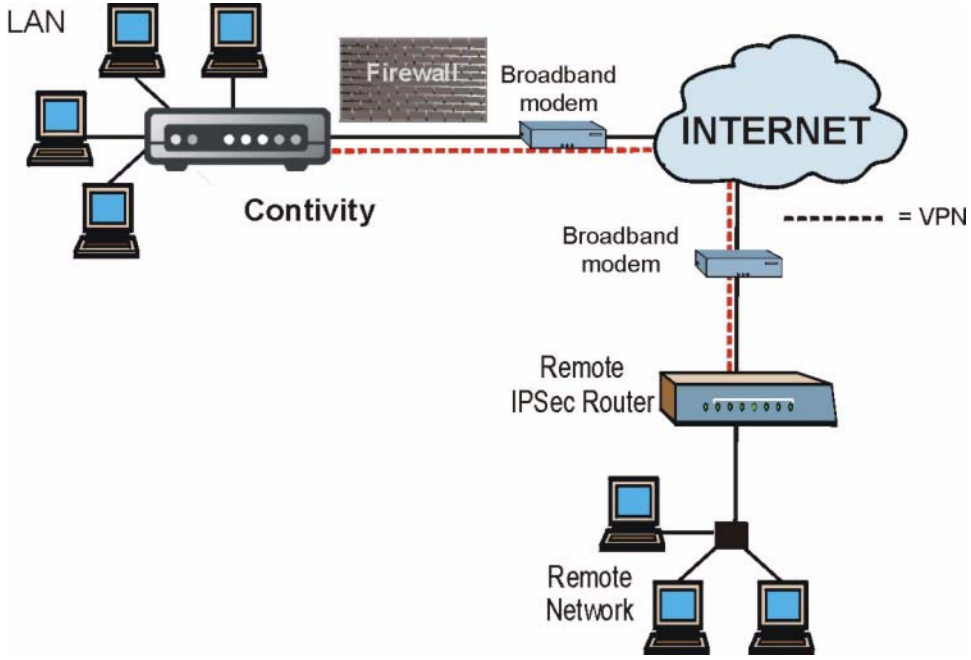
Applications for the Contivity 221

Secure Broadband Internet Access and VPN

You can connect a cable, DSL or other modem to the Contivity 221 via Ethernet for broadband Internet access. The Contivity 221 also provides IP address sharing and a firewall-protected local network with traffic management.

VPN is an ideal cost-effective way to connect branch offices and business partners over the Internet without the need (and expense) of leased lines between sites. The LAN computers can share the five VPN tunnels for secure connections to remote computers.

Figure 1 Secure Internet Access and VPN Application



Hardware Setup

Please refer to your *Quick Start Guide* for hardware connection instructions.

Note: To keep the Contivity 221 operating at optimal internal temperature, keep the bottom, sides and rear clear of obstructions and away from the exhaust of other equipment.

After installing your Contivity 221, continue with the rest of this user's guide for configuration instructions.

Chapter 2
Introducing the WebGUI

This chapter describes how to access the Contivity 221 WebGUI and provides an overview of its screens.

WebGUI Overview

The WebGUI is an HTML-based management interface that allows easy Contivity 221 setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the WebGUI you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See the **Troubleshooting** chapter if you want to make sure these functions are allowed in Internet Explorer.

Accessing the Contivity 221 WebGUI

Make sure your Contivity 221 hardware is properly connected and prepare your computer/computer network to connect to the Contivity 221 (refer to the *Quick Start Guide*).

1 Launch your web browser.

2 Type "192.168.1.1" as the URL.

3 Type the user name (“admin” is the default) and the password ("setup" is the default) and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

Figure 2 Login Screen



4 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 3 Change Password Screen



5 Click **Apply** in the **Replace Certificate** screen to create a certificate using your Contivity 221’s MAC address that will be specific to this device.

Figure 4 Replace Certificate Screen



You should now see the **MAIN MENU** screen (see MAIN MENU Screen).

Note: The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back into the Contivity 221 if this happens to you.

Resetting the Contivity 221

If you forget your password or cannot access the SMT menu, you will need to reload the factory-default configuration file or use the **RESET** button the back of the Contivity 221. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to “setup”, also.

Procedure To Use The Reset Button

1 Press the **RESET** button for ten seconds, and then release it. The Contivity 221 restarts. Otherwise, go to step 2.

2 Turn the Contivity 221 off.

3 While pressing the **RESET** button, turn the Contivity 221 on.

4 Continue to hold the **RESET** button for about 10 or 15 seconds. The Contivity 221 restarts.

5 Release the **RESET** button and wait for the Contivity 221 to finish restarting.

Uploading a Configuration File Via Console Port

1 Download the default configuration file from the Nortel Networks FTP site, unzip it and save it in a folder.

2 Turn off the Contivity 221, begin a terminal emulation software session and turn on the Contivity 221 again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.

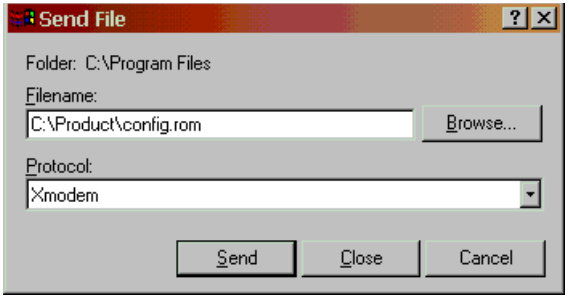
3 Enter "y" at the prompt below to go into debug mode.

4 Enter "atlc" after "Enter Debug Mode" message.

5 Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.

6 Click **Transfer**, then **Send File** to display the following screen.

Figure 5 Example Xmodem Upload



7 After successful firmware upload, enter "atgo" to restart the router.

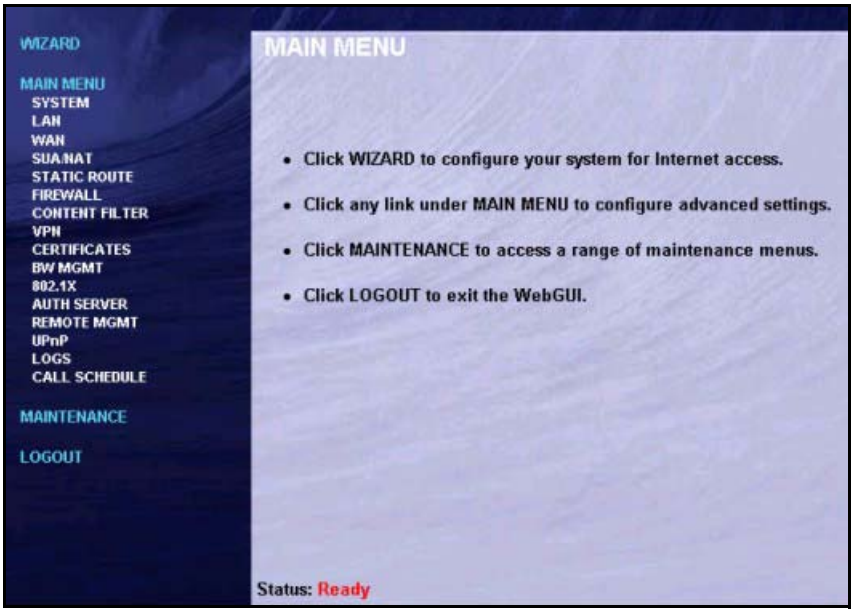
Navigating the Contivity 221 WebGUI

The following summarizes how to navigate the WebGUI from the **MAIN MENU** screen.

Note: Follow the instructions you see in the MAIN MENU screen or click the help icon (located in the top right corner of most screens to view online help.

Note: The help icon does not appear in the MAIN MENU screen.

Figure 6 MAIN MENU Screen



Chapter 3
Wizard Setup

This chapter provides information on the Wizard screens in the WebGUI.

Wizard Overview

The WebGUI's setup wizard helps you configure your device to access the Internet. The second screen has three variations depending on what encapsulation type you use. Refer to your ISP checklist in the *Quick Start Guide* to know what to enter in each field. Leave a field blank if you don't have that information.

Wizard Setup: General Setup and System Name

General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.

In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.

In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Contivity 221 **System Name**.

Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the Contivity 221 via DHCP.

Click **Next** to configure the Contivity 221 for Internet access.

Figure 7 Wizard 1



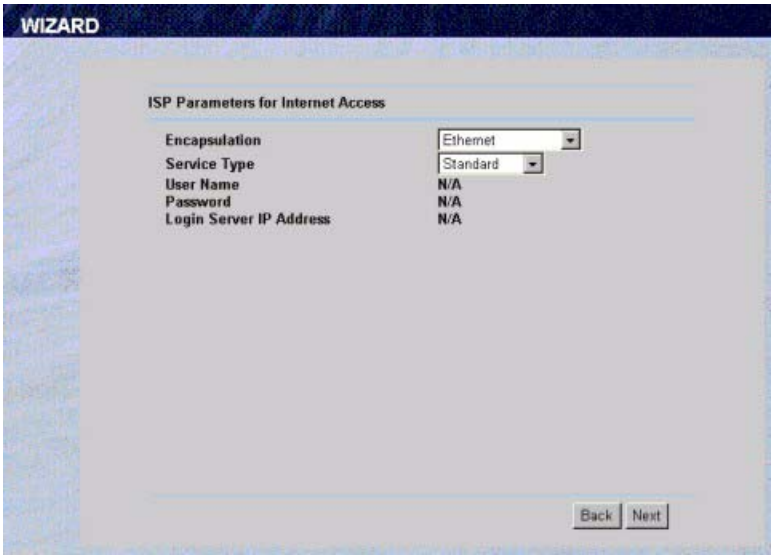
Wizard Setup: Screen 2

The Contivity 221 offers three choices of encapsulation. They are **Ethernet**, **PPTP** or **PPPoE.**

Ethernet

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Figure 8 Wizard 2: Ethernet Encapsulation



The following table describes the fields in this screen.

Table 2 Wizard 2: Ethernet Encapsulation

Label	Description
Encapsulation	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection.
Service Type	Choose from **Standard**, **RR-Telstra** (Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method) or **RR-Toshiba** (Roadrunner Toshiba authentication method). For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a WAN-to-WAN/Contivity221 firewall rule that allows access for port 1026 (UDP). The following fields are not applicable (**N/A**) for the **Standard** service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.

Table 2 Wizard 2: Ethernet Encapsulation

Label	Description
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

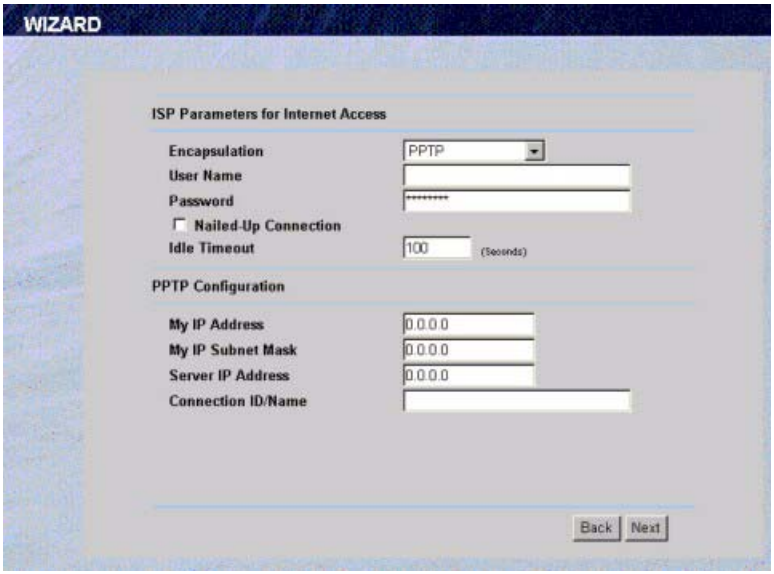
PPTP

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

Note: The CONTIVITY 221 supports one PPTP server connection at any given time

Figure 9 Wizard 2: PPTP Encapsulation



The following table describes the fields in this screen.

Table 3 Wizard 2: PPTP Encapsulation

Label	Description
Encapsulation	Select **PPTP** from the drop-down list box.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Nailed Up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server. The default is 45 seconds.
	PPTP Configuration
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks. It preserves the existing Microsoft Dial-Up Networking experience and requires no new learning or procedures.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

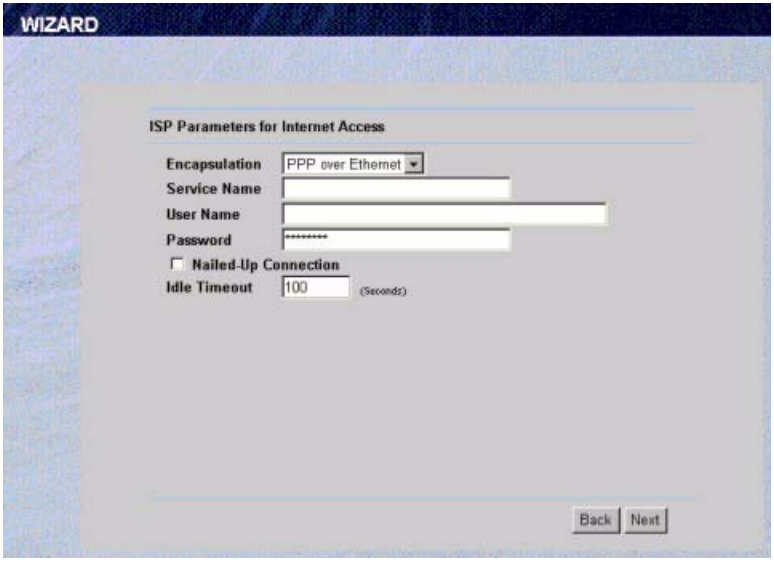
One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the Contivity 221 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Contivity 221 does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Refer to the *Appendices* for more information on PPPoE.

Figure 10 Wizard2: PPPoE Encapsulation



The following table describes the fields in this screen.

Table 4 Wizard2: PPPoE Encapsulation

Label	Description
Encapsulation	Choose an encapsulation method from the pull-down list box. PPPoE forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Nailed Up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is **100** seconds.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

Wizard Setup: Screen 3

The third wizard screen allows you to configure WAN IP address assignment, DNS server address assignment and the WAN MAC address.

WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 5 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.



Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Contivity 221. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Contivity 221, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Contivity 221 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Contivity 221 unless you are instructed to do otherwise.

DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.nortelnetworks.com is 47.249.48.20. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The Contivity 221 can get the DNS server addresses in the following ways.

The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.

If the ISP did not give you DNS server information, leave the DNS Server fields in DHCP Setup set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

WAN MAC Address

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

You can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (configuration file). It will not change unless you change the setting or upload a different "rom" file.

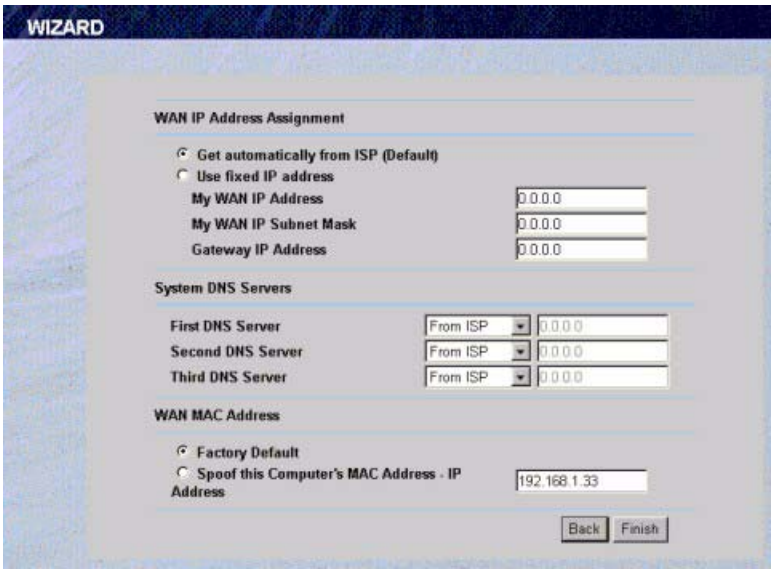
Your Contivity 221's WAN Port is set at half-duplex mode as most cable/DSL modems only support half-duplex mode. Make sure your modem is in half-duplex mode. Your Contivity 221 supports full duplex mode on the LAN side.

Table 6 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(Contivity 221 LAN IP)

The third wizard screen varies according to the type of encapsulation that you select in the second wizard screen.

Figure 11 Wizard 3



The following table describes the fields in this screen.

Table 7 Wizard 3

Label	Description
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**
IP Subnet Mask	Enter the IP subnet mask in this field if you selected **Use Fixed IP Address**. This field is not available when you select PPPoE encapsulation in the previous wizard screen.
Gateway IP Address	Enter the gateway IP address in this field if you selected **Use Fixed IP Address**. This field is not available when you select PPPoE encapsulation in the previous wizard screen.
DNS Server Address Assignment	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, e.g., the IP address of www.nortelnetworks.com is 47.249.48.20. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

Table 7 Wizard 3

Label	Description
Get automatically from ISP	Select this option if your ISP does not give you DNS server addresses. This option is selected by default.
Use fixed IP address - DNS Server IP Address	Select this option If your ISP provides you a DNS server address.
	System DNS Servers (if applicable) DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The Contivity 221 uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Contivity 221's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. If you chose **From ISP**, but the Contivity 221 has a fixed WAN IP address, **From ISP** changes to **None** after you click **Finish**. If you chose **From ISP** for the second or third DNS server, but the ISP does not provide a second or third IP address, **From ISP** changes to **None** after you click **Finish**. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **None** if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server. Select **Private DNS** if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right. With a private DNS server, you must also configure the first DNS server entry in the **LAN IP** screen to use **DNS Relay**. You must also configure a VPN branch office rule since the Contivity 221 uses a VPN tunnel when it relays DNS queries to the private DNS server. One of the rule's IP policies must include the LAN IP address of the Contivity 221 as a local IP address and the IP address of the DNS server as a remote IP address. A **Private DNS** entry with the IP address set to 0.0.0.0 changes to **None** after you click **Apply**. A duplicate **Private DNS** entry changes to **None** after you click **Apply**.
WAN MAC Address	The MAC address field allows you to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN.

Table 7 Wizard 3

Label	Description
Factory Default	Select this option to use the factory assigned default MAC Address.
Spoof this Computer's MAC address - IP Address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (configuration file). It will not change unless you change the setting or upload a different rom file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to complete and save the wizard setup.

Basic Setup Complete

Well done! You have successfully set up your Contivity 221 to operate on your network and access the Internet.

Chapter 4
System Screens

This chapter provides information on the System screens.

System Overview

This chapter provides background information on features that you cannot configure in the Wizard.

DNS Overview

There are three places where you can configure DNS (Domain Name System) setup on the Contivity 221.

Use the **System General** screen to configure the Contivity 221 to use a DNS server to resolve domain names for Contivity 221 system features like VPN, DDNS and the time server.

Use the **LAN IP** screen to configure the DNS server information that the Contivity 221 sends to the DHCP client devices on the LAN.

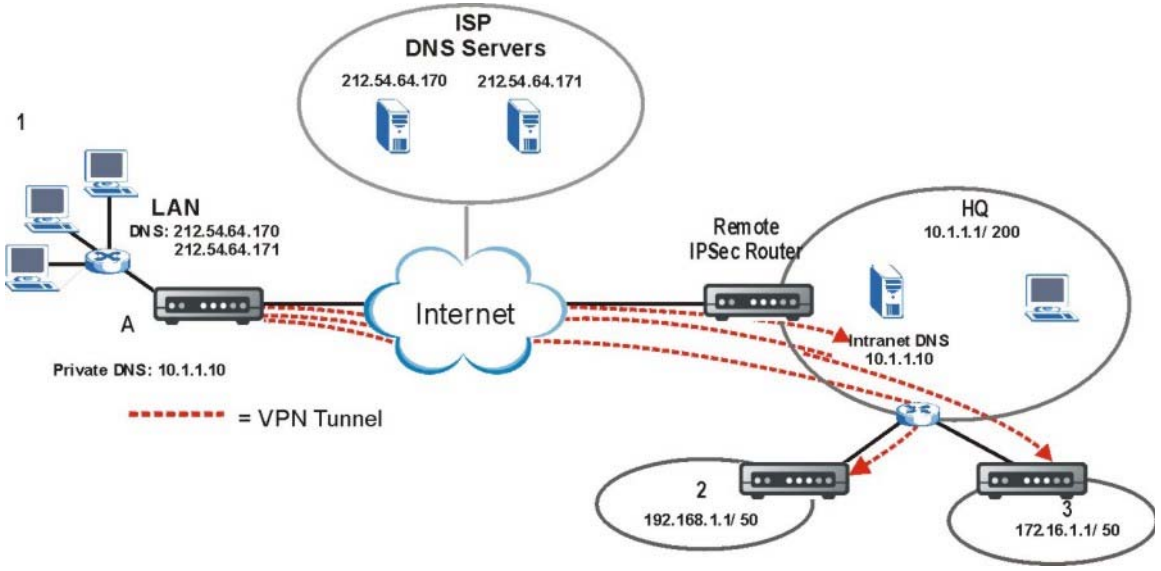
Use the **Remote Management DNS** screen to configure the Contivity 221 to accept or discard DNS queries.

Private DNS Server

In cases where you want to use domain names to access Intranet servers on a remote private network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

The following figure depicts an example where three VPN tunnels are created from Contivity 221 A; one to branch office **2**, one to branch office **3** and another to headquarters (**HQ**). In order to access computers that use private domain names on the **HQ** network, the Contivity 221 at branch office **1** uses the Intranet DNS server in headquarters.

Figure 12 Private DNS Server Example

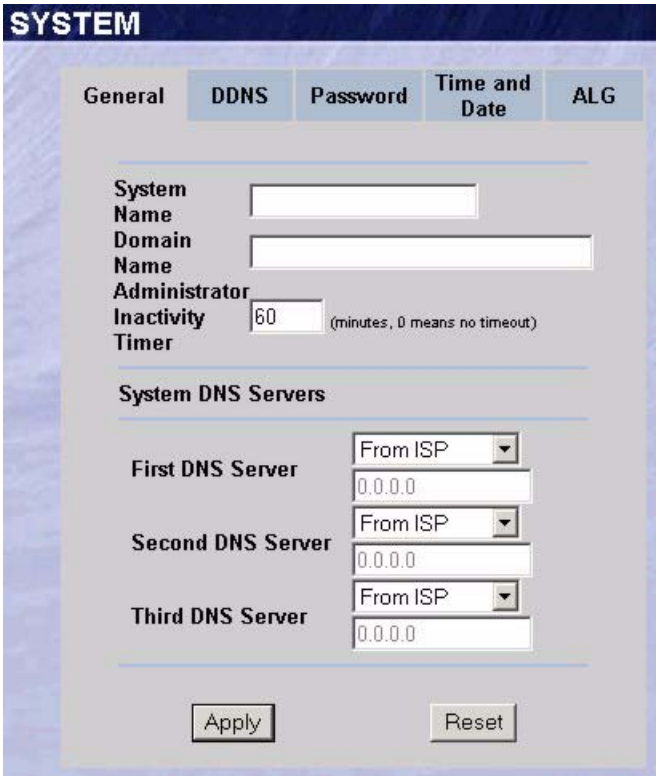


Note: If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

Configuring General Setup

Click **SYSTEM** to open the **General** screen.

Figure 13 System General Setup



The following table describes the fields in this screen.

Table 8 System General Setup

Label	Description
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.

Table 8 System General Setup

Label	Description
Administrator Inactivity Timer	Type how many minutes a management session (either via the WebGUI or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.
System DNS Servers (if applicable)	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The Contivity 221 uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Contivity 221's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. If you chose **From ISP**, but the Contivity 221 has a fixed WAN IP address, **From ISP** changes to **None** after you click **Apply**. If you chose **From ISP** for the second or third DNS server, but the ISP does not provide a second or third IP address, **From ISP** changes to **None** after you click **Apply**. Select **User-Defined** if you have the IP address of a DNS server. The IP address can be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right. A **User-Defined** entry with the IP address set to 0.0.0.0 changes to **None** after you click **Apply**. A duplicate **User-Defined** entry changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server. Select **Private DNS** if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right. With a private DNS server, you must also configure the first DNS server entry in the **LAN IP** screen to use **DNS Relay**. You must also configure a VPN branch office rule since the Contivity 221 uses a VPN tunnel when it relays DNS queries to the private DNS server. One of the rule's IP policies must include the LAN IP address of the Contivity 221 as a local IP address and the IP address of the DNS server as a remote IP address. A **Private DNS** entry with the IP address set to 0.0.0.0 changes to **None** after you click **Apply**. A duplicate **Private DNS** entry changes to **None** after you click **Apply**.

Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

Configuring Dynamic DNS



Note: If you have a private WAN IP address, then you cannot use Dynamic DNS.

To change your Contivity 221's DDNS, click **SYSTEM**, then the **DDNS** tab. The screen appears as shown.

Figure 14 DDNS



The following table describes the fields in this screen.

Table 9 DDNS

Label	Description
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").
User	Enter your user name (up to 31 characters).

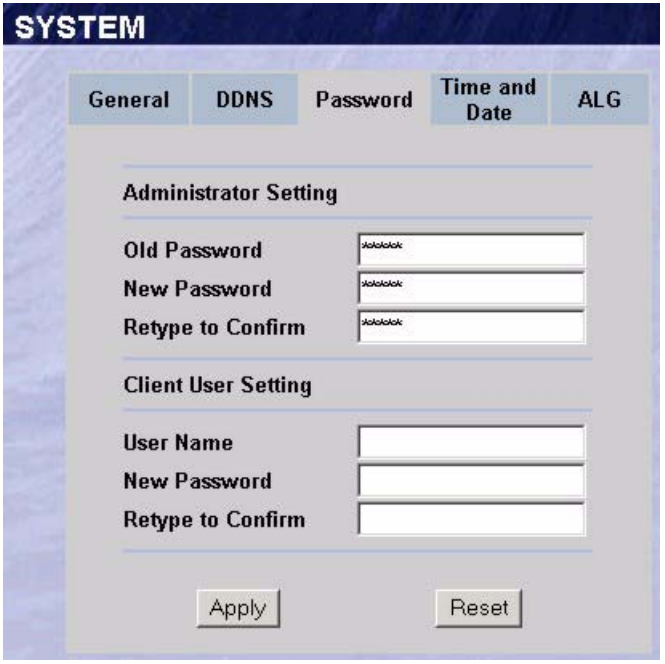
Table 9 DDNS

Label	Description
Password	Enter the password associated with the user name above (up to 31 characters).
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Off Line	This option is available when **CustomDNS** is selected in the **DDNS Type field**. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
DDNS Server Auto Detect IP Address	Select this option only when there are one or more NAT routers between the Contivity 221 and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. **Note:** The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the Contivity 221 and the DDNS server.
Use Specified IP Address	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.
Use IP Address	Enter the IP address if you select the **User Specify** option.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring Password

To change your Contivity 221's password (recommended), click **SYSTEM**, then the **Password** tab. The screen appears as shown. This screen allows you to change the Contivity 221's password.

Figure 15 Password



The following table describes the fields in this screen.

Table 10 Password

Label	Description
Administrator Setting	The administrator can access and configure all of the Contivity 221's features.
Old Password	Type your existing system administrator password ("setup" is the default password).
New Password	Type your new system password (up to 31 characters). Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.

Table 10 Password

Label	Description
Client User Setting	The client user is the person who is to use the Contivity 221's Contivity Client VPN tunnel. The client user can do the following: • Configure the **WAN ISP** and **IP** screens. • Configure the VPN Contivity Client settings (except the **Advanced** screen's exclusive use mode for client tunnel and MAC address allowed settings). • View the SA monitor. • Configure the **VPN Global Setting** screen. • View logs. • View the **Maintenance Status** screen. • Use the **Maintenance F/W Upload** and **Restart** screens.
User Name	Type a user name for the client user (up to 31 characters).
New Password	Type a password for the client user (up to 31 characters). Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Retype the client user password for confirmation.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Pre-defined NTP Time Server List

The Contivity 221 uses the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

The Contivity 221 can use this pre-defined list of time servers regardless of the Time Protocol you select.

When the Contivity 221 uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the Contivity 221 goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

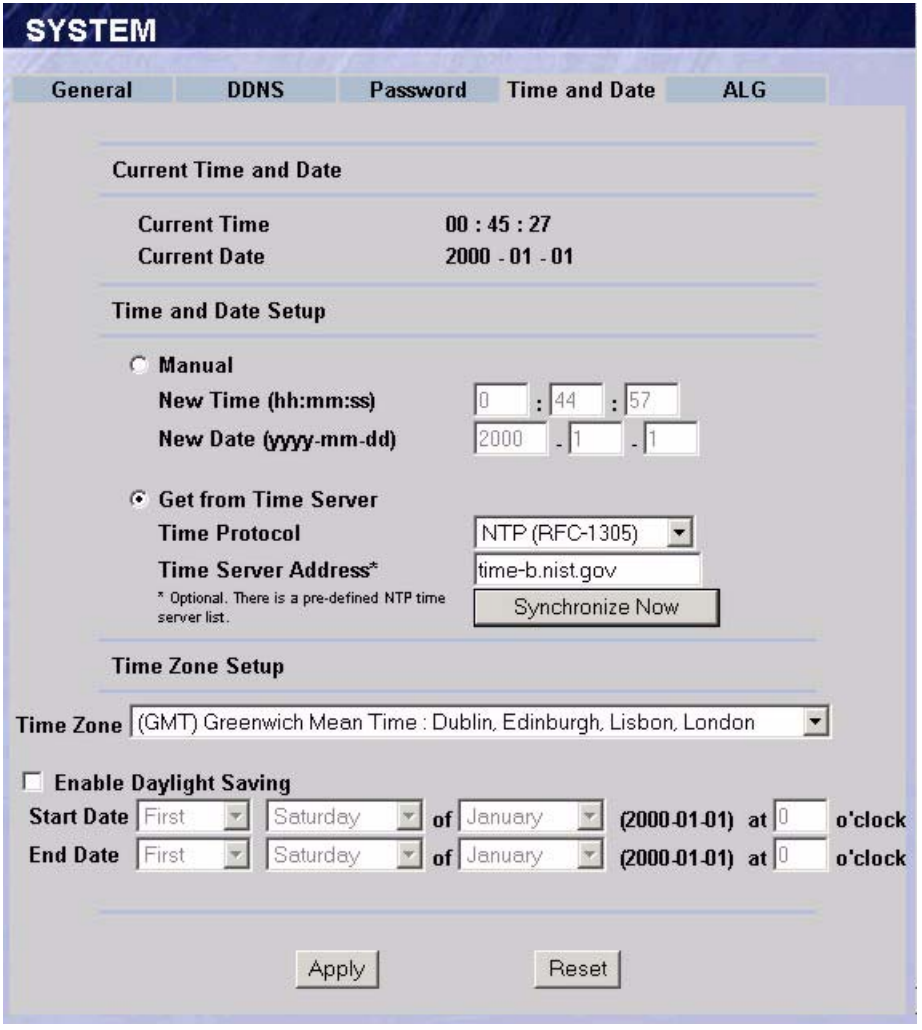
Table 11 Default Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

Configuring Time and Date

To change your Contivity 221's time and date, click **SYSTEM**, then **Time and Date**. The screen appears as shown. Use this screen to configure the Contivity 221's time based on your local time zone.

Figure 16 Time and Date



The following table describes the fields in this screen.

Table 12 Time and Date

Label	Description
Current Time and Date	
Current Time	This field displays the time of your Contivity 221. Each time you reload this page, the Contivity 221 synchronizes the time with the time server.
Current Date	This field displays the date of your Contivity 221. Each time you reload this page, the Contivity 221 synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the Contivity 221 get the time and date from the time server you specified below.
Time Protocol	Select the time service protocol that your time server sends when you turn on the Contivity 221. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305)**, is similar to **Time (RFC 868)**.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Synchronize Now	Click this button to have the Contivity 221 get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (including the time server address).
Time Zone Setup	

Table 12 Time and Date

Label	Description
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use daylight savings time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **April** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Last**, **Sunday**, **October** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

ALG

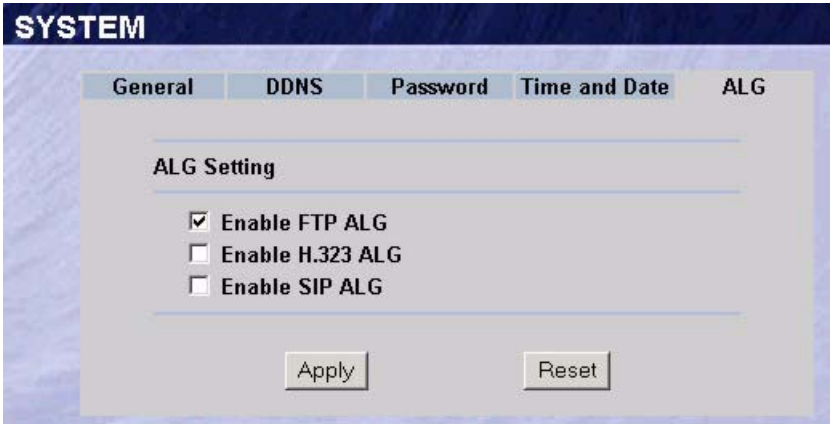
An Application Layer Gateway (ALG) allows applications to pass through NAT and the firewall. You may also need to configure NAT and firewall rules depending upon the type of access you want to allow.

An ALG also lets bandwidth management manage the application's bandwidth (you must also configure bandwidth management).

Configuring ALG

To change your Contivity 221's ALG settings, click **SYSTEM**, then **ALG**. The screen appears as shown.

Figure 17 ALG



The following table describes the labels in this screen.

Table 13 ALG

Label	Description
Enable FTP ALG	Select this check box to allow FTP (File Transfer Protocol) to send and receive files through the Contivity 221.
Enable H.323 ALG	Select this check box to allow applications using H.323 to go through the Contivity 221. H.323 is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. H.323 is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.
Enable SIP ALG	Select this check box to allow SIP (Session Initiation Protocol) applications to go through the Contivity 221. The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol. To avoid retranslating the SIP device's IP address, do not use the SIP ALG with a SIP device that is using STUN (Simple Traversal of User Datagram Protocol (UDP) through NAT).
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 5
LAN Screens

This chapter describes how to configure LAN settings.

LAN Overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Contivity 221 as a DHCP server or disable it. When configured as a server, the Contivity 221 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The Contivity 221 is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

DNS Servers

Use the **LAN IP** screen to configure the DNS server information that the Contivity 221 sends to the DHCP client devices on the LAN.

LAN TCP/IP

The Contivity 221 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

Factory LAN Defaults

The LAN parameters of the Contivity 221 are preset in the factory with the following values:

IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)

DHCP server enabled with 32 client IP addresses starting from 192.168.1.3.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded WebGUI help regarding what fields need to be configured.

RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the Contivity 221 will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

RIP Version controls the format and the broadcasting method of the RIP packets that the Contivity 221 sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

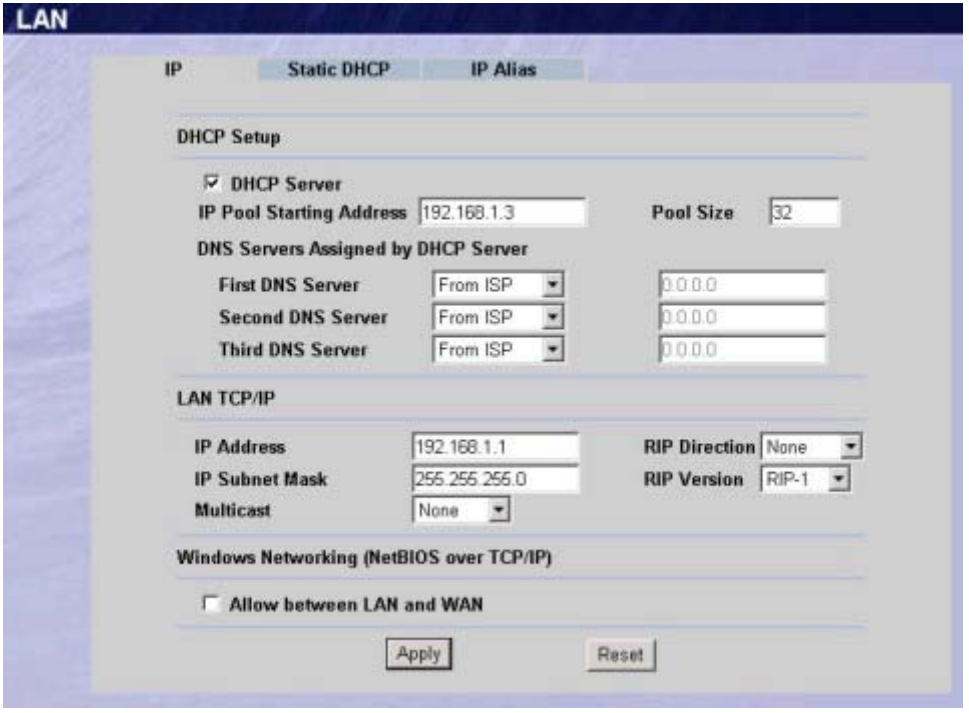
IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The Contivity 221 supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the Contivity 221 queries all directly connected networks to gather group membership. After that, the Contivity 221 periodically updates this information. IP multicasting can be enabled/disabled on the Contivity 221 LAN and/or WAN interfaces in the WebGUI (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

Configuring IP

Click **LAN** to open the **IP** screen.

Figure 18 IP



The following table describes the fields in this screen.

Table 14 IP

Label	Description
DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave the **DHCP Server** check box selected. Clear it to disable the Contivity 221 acting as a DHCP server. When configured as a server, the Contivity 221 provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the workstation must be manually configured. When set as a server, fill in the following four fields.

Table 14 IP

Label	Description
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool. The default is 192.168.1.3.
Pool Size	This field specifies the size, or count, of the IP address pool. The default is 32.
DNS Servers Assigned by DHCP Server	The Contivity 221 passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The Contivity 221 only passes this information to the LAN DHCP clients when you select the **DHCP Server** check box. When you clear the **DHCP Server** check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Contivity 221's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **DNS Relay** to have the Contivity 221 act as a DNS proxy. The Contivity 221's LAN IP address displays in the field to the right (read-only). The Contivity 221 tells the DHCP clients on the LAN that the Contivity 221 itself is the DNS server. When a computer on the LAN sends a DNS query to the Contivity 221, the Contivity 221 forwards the query to the Contivity 221's system DNS server (configured in the **SYSTEM General** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
LAN TCP/IP	
IP Address	Type the IP address of your Contivity 221 in dotted decimal notation (192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Contivity 221 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Contivity 221 255.255.255.0.

Table 14 IP

Label	Description
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the Contivity 221 will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. **None** is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Contivity 221 sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*.
Windows Networking (NetBIOS over TCP/IP)	
Allow between LAN and WAN	Select this option to forward NetBIOS packets between the LAN port and the WAN port.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

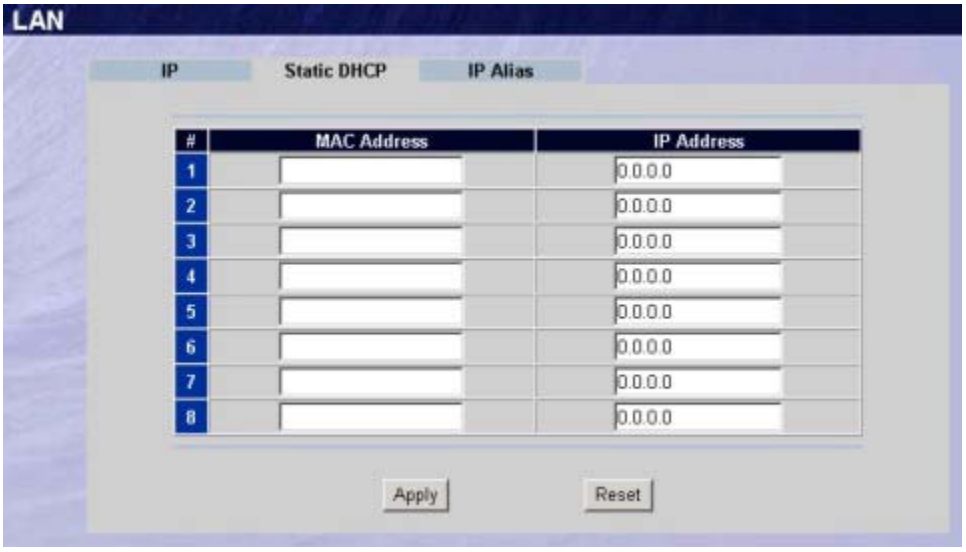
Configuring Static DHCP

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your Contivity 221's Static DHCP settings, click **LAN**, then the **Static DHCP** tab. The screen appears as shown.

Figure 19 Static DHCP



The following table describes the fields in this screen.

Table 15 Static DHCP

Label	Description
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	This field specifies the size, or count of the IP address pool.

Table 15 Static DHCP

Label	Description
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring IP Alias

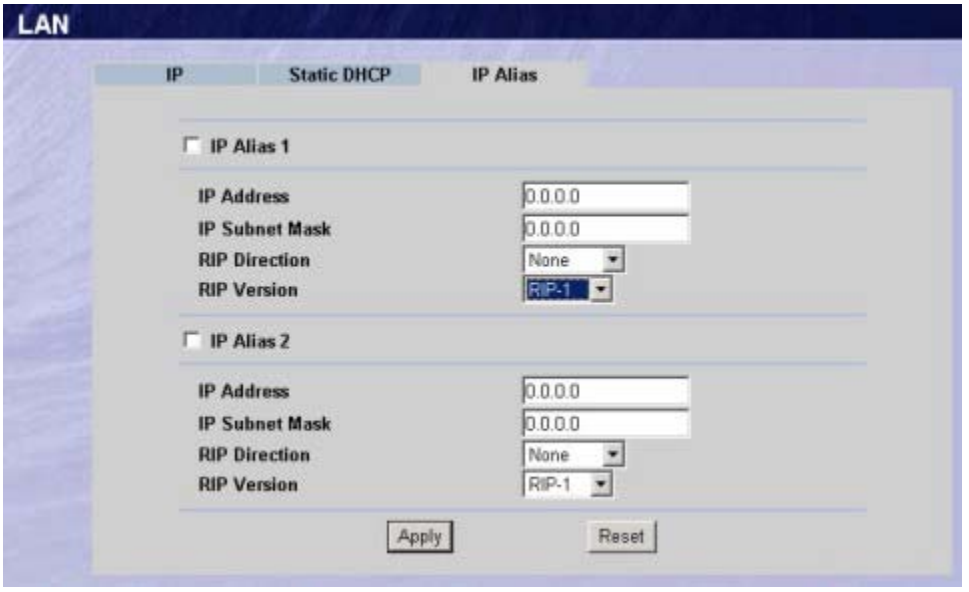
IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Contivity 221 supports three logical LAN interfaces via its single physical Ethernet interface with the Contivity 221 itself as the gateway for each LAN network.



Note: Make sure that the subnets of the logical networks do not overlap.

To change your Contivity 221's IP Alias settings, click **LAN**, then the **IP Alias** tab. The screen appears as shown.

Figure 20 IP Alias



The following table describes the fields in this screen.

Table 16 IP Alias

Label	Description
IP Alias 1,2	Select the check box to configure another LAN network for the Contivity 221.
IP Address	Enter the IP address of your Contivity 221 in dotted decimal notation.
IP Subnet Mask	Your Contivity 221 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Contivity 221.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/ **None**. When set to **Both** or **Out Only**, the Contivity 221 will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

Table 16 IP Alias

Label	Description
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Contivity 221 sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 6
WAN Screens

This chapter describes how to configure WAN settings.

WAN Overview

This chapter provides background information on features that you cannot configure in the Wizard.

TCP/IP Priority (Metric)

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the Contivity 221's routes to the Internet. If any two of the default routes have the same metric, the Contivity 221 uses the following pre-defined priorities:

1. Normal route: designated by the ISP (see "Configuring WAN IP") or a static route
2. Traffic-redirect route (see "Configuring Traffic Redirect")
3. Dial-backup route (see "Configuring Dial Backup")

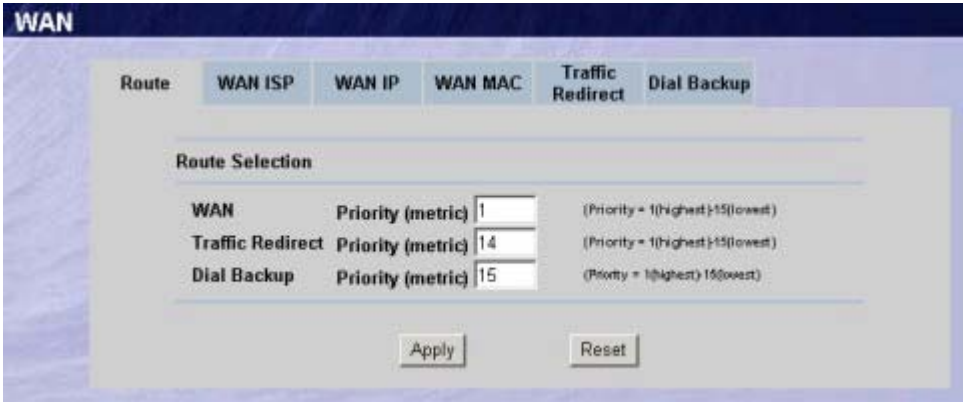
For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the Contivity 221 tries the traffic-redirect route next. In the same manner, the Contivity 221 uses the dial-backup route if the traffic-redirect route also fails.

If you want the dial-backup route to take first priority over the traffic-redirect route or even the normal route, all you need to do is set the dial-backup route's metric to "1" and the others to "2" (or greater).

Configuring Route

Click **WAN** to open the **Route** screen.

Figure 21 WAN: Route



The following table describes the fields in this screen.

Table 17 WAN: Route

Label	Description
WAN Traffic Redirect Dial Backup	The default WAN connection is "1' as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is **WAN**, **Traffic Redirect** and then **Dial Backup** (dial backup does not apply to all Contivity 221 models): You have two choices for an auxiliary connection in the event that your regular WAN connection goes down. If **Dial Backup** is preferred to **Traffic Redirect**, then type "14" in the **Dial Backup Priority (metric)** field (and leave the **Traffic Redirect Priority (metric)** at the default of "15").
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring WAN ISP

To change your Contivity 221's WAN ISP settings, click **WAN**, then the **WAN ISP** tab. The screen differs by the encapsulation.

Ethernet Encapsulation

The screen shown next is for **Ethernet** encapsulation.

Figure 22 Ethernet Encapsulation



The following table describes the fields in this screen.

Table 18 Ethernet Encapsulation

Label	Description
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from **Standard**, **Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method) or **RR-Toshiba** (Roadrunner Toshiba authentication method). The following fields do not appear with the **Standard** service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

PPPoE Encapsulation

The Contivity 221 supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

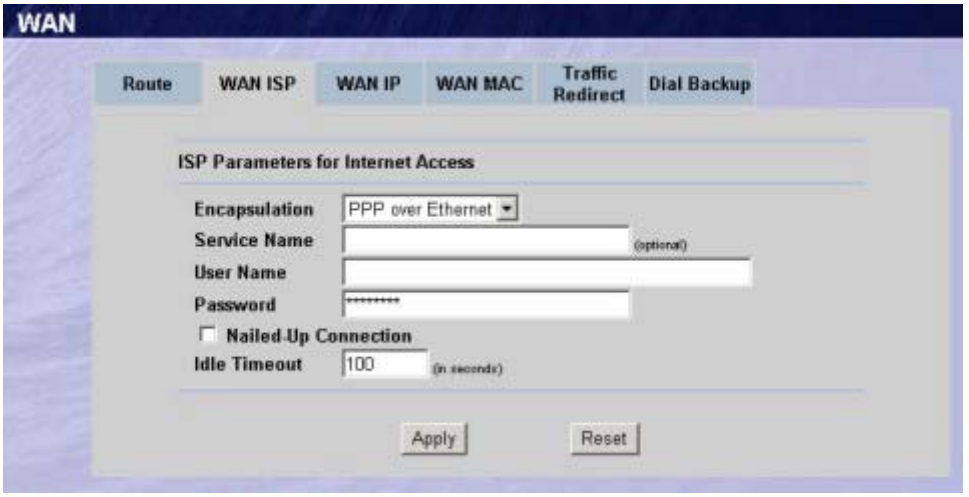
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the Contivity 221 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Contivity 221 does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

The screen shown next is for **PPPoE** encapsulation.

Figure 23 PPPoE Encapsulation



The following table describes the fields in this screen.

Table 19 PPPoE Encapsulation

Label	Description
Encapsulation	The PPPoE choice is for a dial-up connection using PPPoE. The router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. DSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the **User Name** above.
Nailed Up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.

Table 19 PPPoE Encapsulation

Label	Description
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

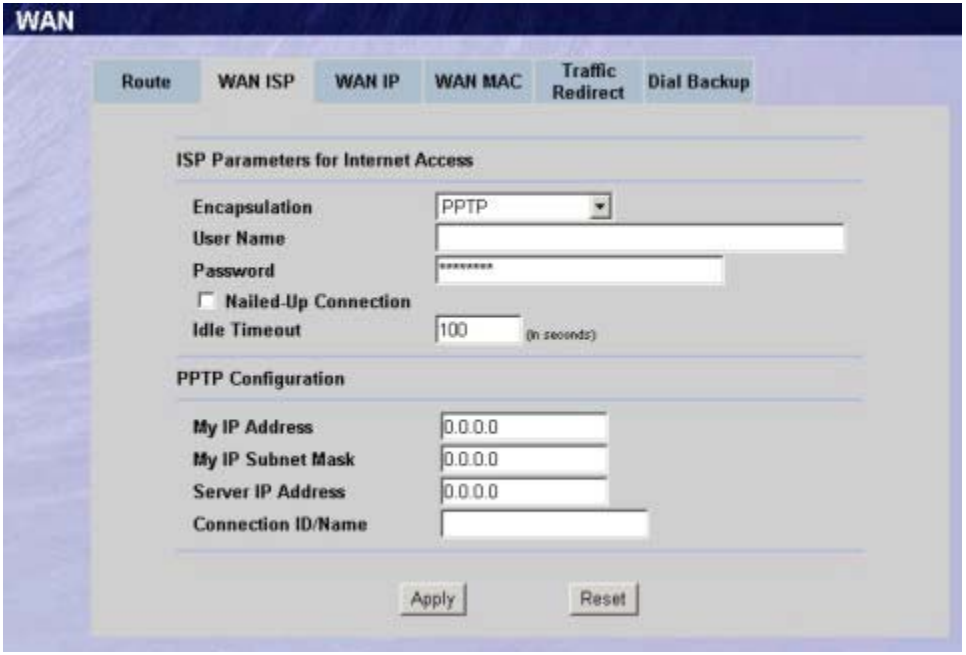
PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

The screen shown next is for **PPTP** encapsulation.

Figure 24 PPTP Encapsulation



The following table describes the fields in this screen.

Table 20 PPTP Encapsulation

Label	Description
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The Contivity 221 supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Nailed-up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the Contivity 221 automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your Contivity 221 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Contivity 221.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Service Type

The screen shown next is for **RR- Service Type**.

Figure 25 RR Service Type



The following table describes the fields in this screen.

Table 21 RR Service Type

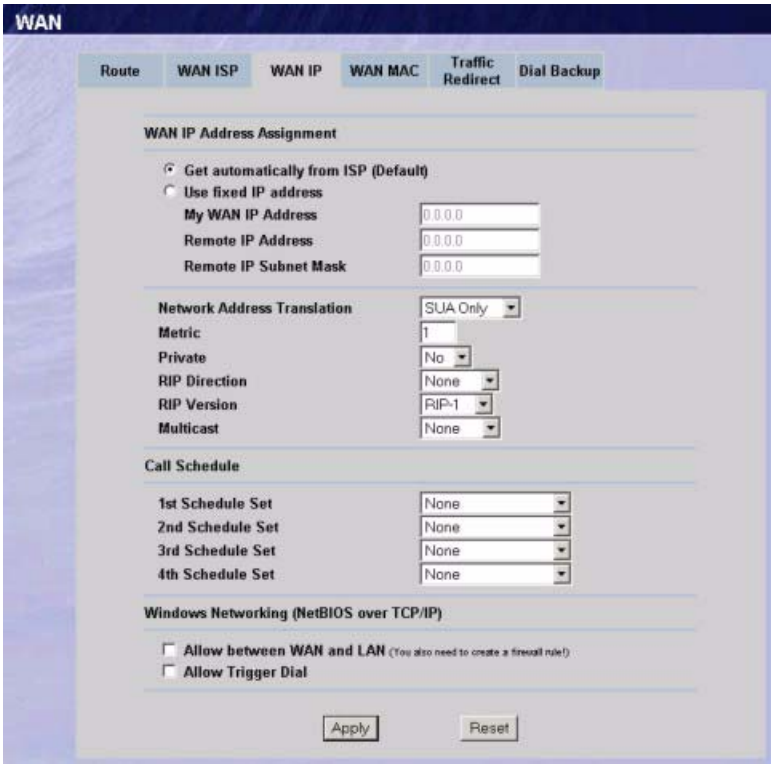
Label	Description
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (Roadrunner Manager authentication method) or **RR-Telstra**. Choose a Roadrunner service type if your ISP is Time Warner's Roadrunner; otherwise choose **Standard**.
User Name	Enter the username given to you by your ISP.
Password	Enter the password associated with the login name above.
Login Server IP Address	The Contivity 221 will find the Roadrunner Server IP address if this field is left blank. If it does not, then you must enter the authentication server IP address.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring WAN IP

To change your Contivity 221's WAN IP settings, click **WAN**, then the **WAN IP** tab. This screen varies according to the type of encapsulation you select.

If your ISP did *not* assign you a fixed IP address, click **Get automatically from ISP (Default)**; otherwise click **Use fixed IP Address** and enter the IP address in the following field.

Figure 26 WAN: IP



The following table describes the fields in this screen.

Table 22 WAN: IP

Label	Description
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**
IP Subnet Mask	Enter the IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Gateway IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose **None** to disable NAT**.** Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set.
Metric (PPPoE and PPTP only)	This field sets this route's priority among the routes the Contivity 221 uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Private (PPPoE and PPTP only)	This parameter determines if the Contivity 221 will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.

Table 22 WAN: IP

Label	Description
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **None**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the Contivity 221 will broadcast its routing table periodically. When set to **Both** or **In Only**, the Contivity 221 will incorporate RIP information that it receives. When set to **None**, the Contivity 221 will not send any RIP packets and will ignore any RIP packets received. By default, **RIP Direction** is set to **Both**.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Contivity 221 sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**.
Multicast	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Call Schedule (PPPoE and PPTP encapsulation)	Apply call schedule sets for this remote node. Use the **Call Schedule** screens to configure call schedule sets (see Chapter 21, “Call Scheduling Screens).
Windows Networking (NetBIOS over TCP/IP):	Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

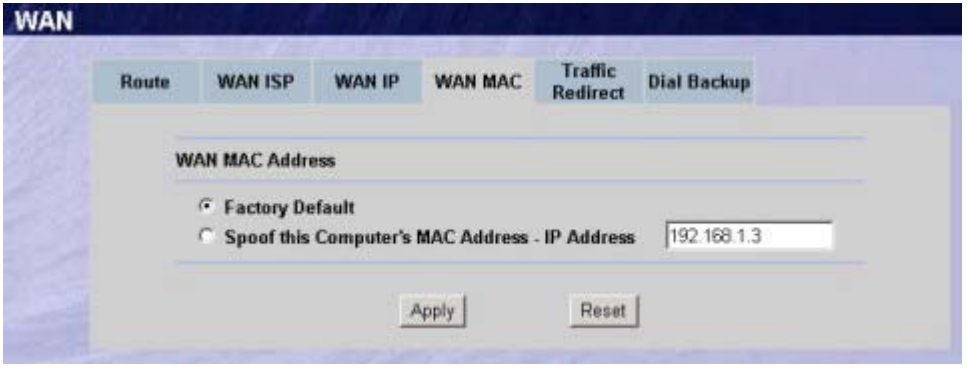
Table 22 WAN: IP

Label	Description
Allow From WAN to LAN	Select this option to forward NetBIOS packets from the WAN port to the LAN port.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring WAN MAC

To change your Contivity 221's WAN MAC settings, click **WAN**, then the **WAN MAC** tab. The screen appears as shown.

Figure 27 MAC Setup



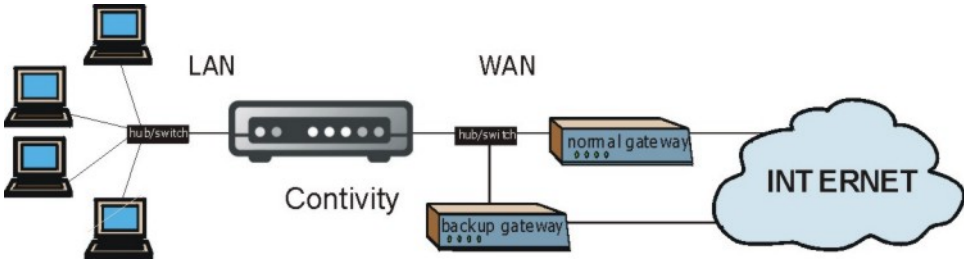
The MAC address screen allows users to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Spoof this computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (configuration file). It will not change unless you change the setting or upload a different ROM file.

Traffic Redirect

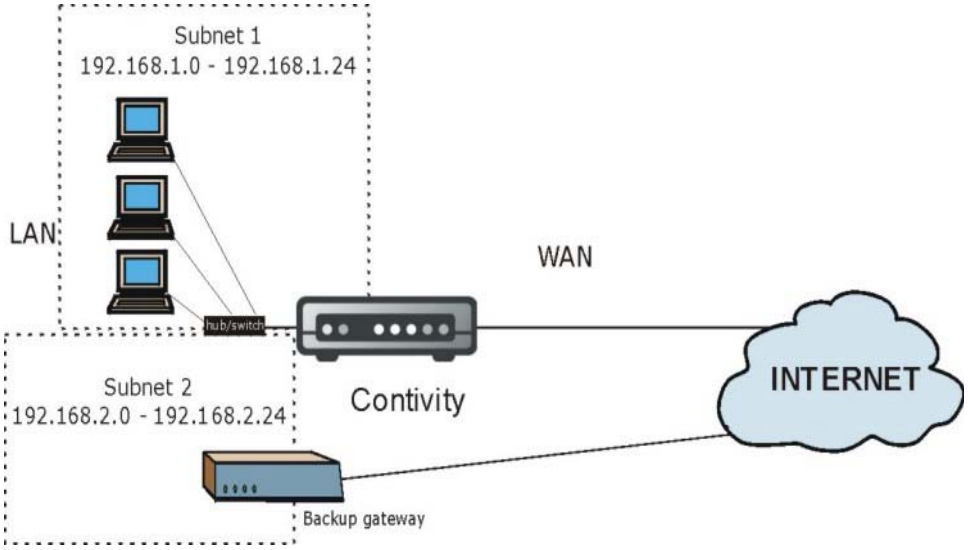
Traffic redirect forwards WAN traffic to a backup gateway when the Contivity 221 cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the Contivity 221 still provides firewall protection. This feature is not available on all models.

Figure 28 Traffic Redirect WAN Setup



The following network topology allows you to avoid triangle route security issues (see the *Appendices*) when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the Contivity 221 itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/Contivity 221 firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

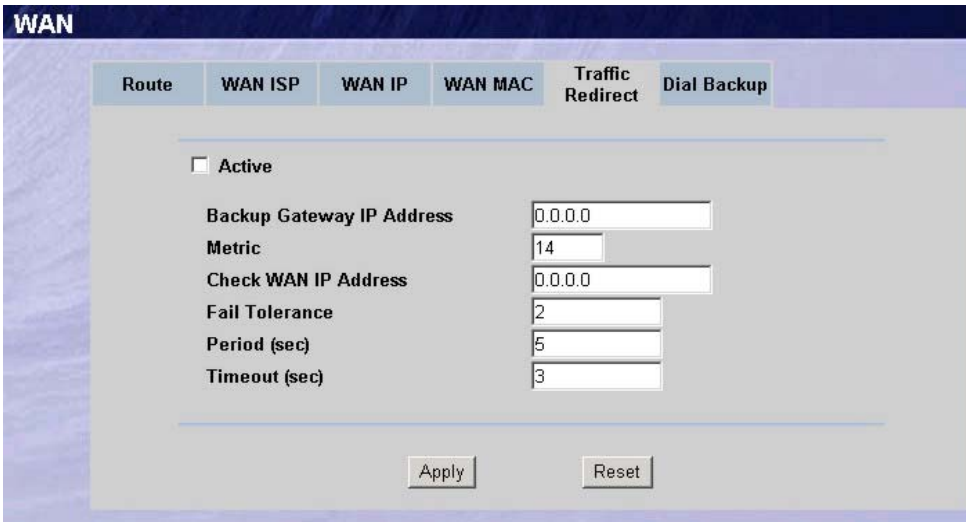
Figure 29 Traffic Redirect LAN Setup



Configuring Traffic Redirect

To change your Contivity 221's Traffic Redirect settings, click **WAN**, then the **Traffic Redirect** tab. The screen appears as shown.

Figure 30 Traffic Redirect



The following table describes the fields in this screen.

Table 23 Traffic Redirect

Label	Description
Active	Select this check box to have the Contivity 221 use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The Contivity 221 automatically forwards traffic to this IP address if the Contivity 221's Internet connection terminates.
Metric	This field sets this route's priority among the routes the Contivity 221 uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the Contivity 221 will use the default gateway IP address. Configure this field to test your Contivity 221's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you are using PPTP or PPPoE Encapsulation, type "0.0.0.0" to configure the Contivity 221 to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.

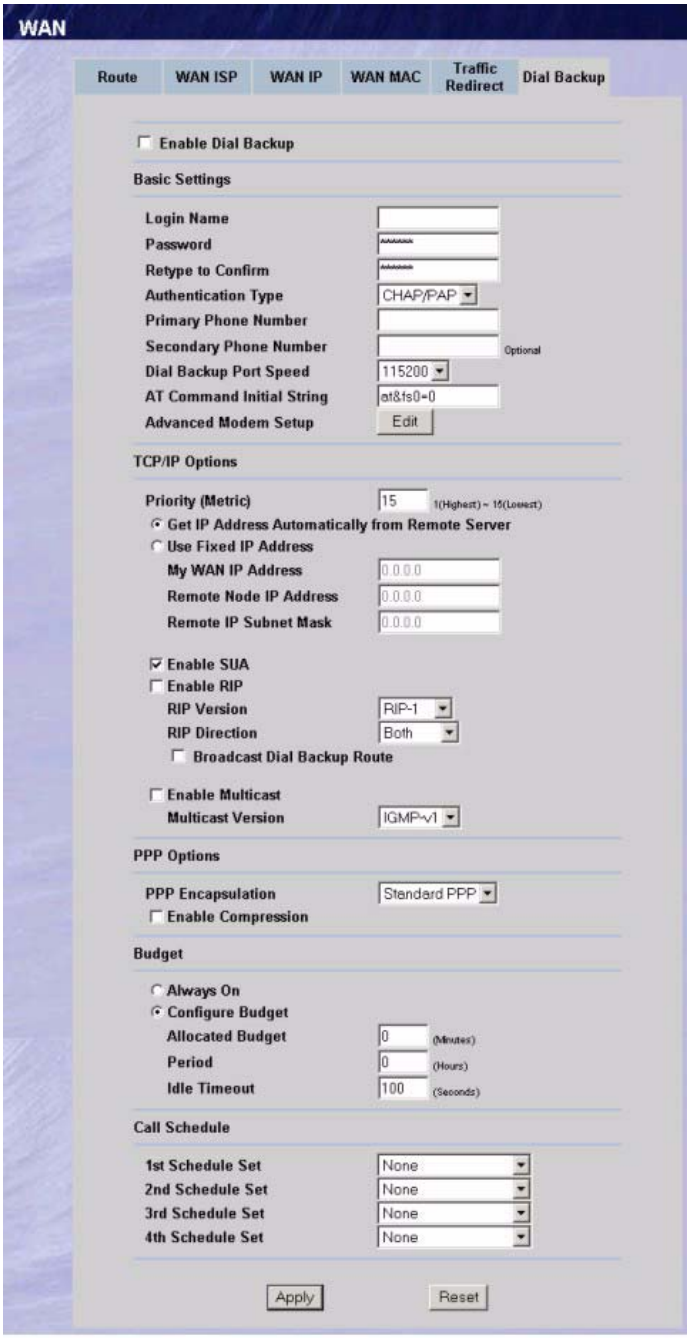
Table 23 Traffic Redirect

Label	Description
Fail Tolerance	Type the number of times your Contivity 221 may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
Period (sec)	Type the number of seconds for the Contivity 221 to wait between checks to see if it can connect to the WAN IP address (**Check WAN IP Address** field) or default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout (sec)	Type the number of seconds for your Contivity 221 to wait for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The WAN connection is considered "down" after the Contivity 221 times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring Dial Backup

To change your Contivity 221's Dial Backup settings, click **WAN**, then the **Dial Backup** tab. The screen appears as shown.

Figure 31 Dial Backup Setup



The following table describes the fields in this screen.

Table 24 Dial Backup Setup

Label	Description
Enable Dial Backup	Select this check box to turn on dial backup.
Basic Settings	
Login Name	Type the login name assigned by your ISP.
Password	Type the password assigned by your ISP.
Retype to Confirm	Type your password again in this field.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your Contivity 221 accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your Contivity 221 accepts CHAP only. **PAP** - Your Contivity 221 accept PAP only.
Primary/ Secondary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your Contivity 221 dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Dial Backup Port Speed	Use the drop-down list box to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: 9600, 19200, 38400, 57600, 115200 or 230400 bps.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.
Advanced Modem Setup	Click this button to display the **Advanced Setup** screen and edit the details of your dial backup setup.
TCP/IP Options	
Priority (Metric)	This field sets this route's priority among the three routes the Contivity 221 uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority. If the three routes have the same metrics, the priority of the routes is as follows: **WAN**, **Traffic Redirect**, **Dial Backup**.
Get IP Address Automatically from Remote Server	Type the login name assigned by your ISP for this remote node.

Table 24 Dial Backup Setup

Label	Description
Used Fixed IP Address	Select this check box if your ISP assigned you a fixed IP address, then enter the IP address in the following field.
Contivity 221 WAN IP Address	Leave the field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Type your WAN IP address here if you know it (static). This is the address assigned to your local Contivity 221, not the remote router.
Remote IP Subnet Mask	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Type the remote gateway's subnet mask here if you know it (static).
Remote Node IP Address	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Type the remote gateway's IP address here if you know it (static).
Contivity 221 Operating Mode	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network. Select **SUA Only** or **None**. **SUA** (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the Contivity 221 will use Address Mapping Set 255. Select **None** to disable NAT.
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Contivity 221 sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

Table 24 Dial Backup Setup

Label	Description
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the Contivity 221 will broadcast its routing table periodically. When set to **Both** or **In Only**, the Contivity 221 will incorporate RIP information that it receives.
Broadcast Dial Backup Route	Select this check box to forward the backup route broadcasts to the WAN.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast Version	Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*.
Budget	
Always On	Select this check box to have the dial backup connection on all of the time.
Configure Budget	Select this check box to have the dial backup connection on during the time that you select.
Allocated Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour).
Idle Timeout	Type the number of seconds of idle time (when there is no traffic from the Contivity 221 to the remote node) for the Contivity 221 to wait before it automatically disconnects the dial backup connection. This option applies only when the Contivity 221 initiates the call. The dial backup connection never times out if you set this field to "0" (it is the same as selecting **Always On**).
Call Schedule Sets	Specify call schedule sets to use on the dial backup connection. the call schedule sets must already be configured (see Chapter 21, “Call Scheduling Screens).

Table 24 Dial Backup Setup

Label	Description
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Advanced Modem Setup

AT Command Strings

For regular telephone lines, the default "Dial" string tells the modem that the line uses tone dialing. "ATDT" is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to "ATDP".

For ISDN lines, there are many more protocols and operational modes. Please consult the documentation of your TA. You may need additional commands in both "Dial" and "Init" strings.

DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the "Drop DTR When Hang Up" check box is selected, the Contivity 221 uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command "ATH".

Response Strings

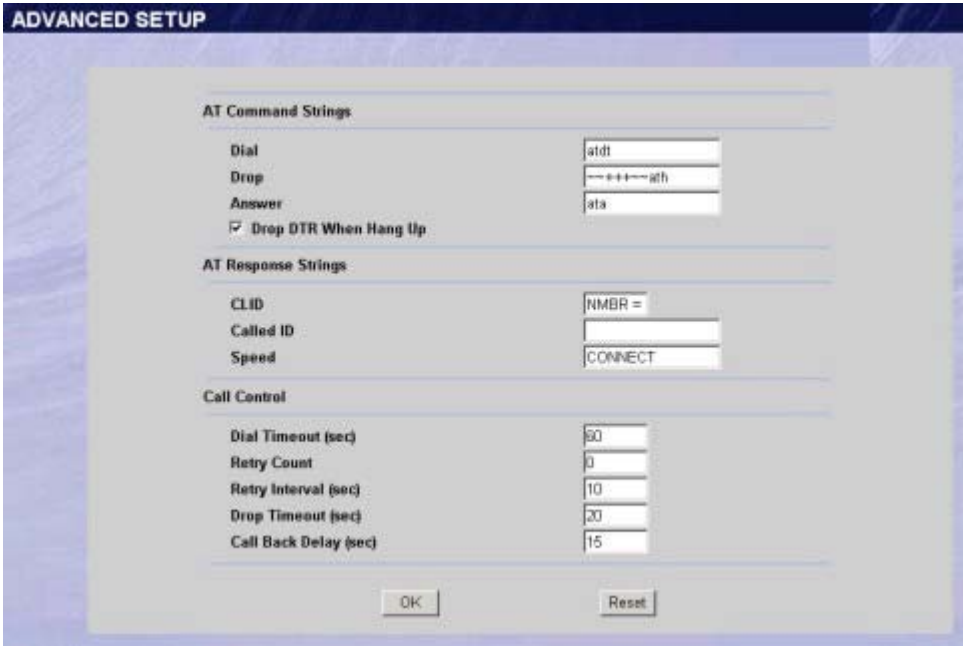
The response strings tell the Contivity 221 the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; please consult the documentation of your WAN device to find the correct tags.

Configuring Advanced Modem Setup

Click the **Edit** button in the **Dial Backup** screen to display the **Advanced Setup** screen shown next.

Note: Consult the manual of your WAN device connected to your dial backup port for specific AT commands.

Figure 32 Advanced Setup



The following table describes the fields in this screen.

Table 25 Advanced Setup

Label	Description	Example
AT Command Strings		
Dial	Type the AT Command string to make a call.	atdt

Table 25 Advanced Setup

Label	Description	Example
Drop	Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~~~+++~~ath" can be used if your modem has a slow response time.	~~+++~~at h
Answer	Type the AT Command string to answer a call.	ata
Drop DTR When Hang Up	Select this check box to have the Contivity 221 drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out.	
AT Response Strings		
CLID	Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the Contivity 221 capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR
Called ID	Type the keyword preceding the dialed number.	
Speed	Type the keyword preceding the connection speed.	CONNECT
Call Control		
Dial Timeout (sec)	Type a number of seconds for the Contivity 221 to try to set up an outgoing call before timing out (stopping).	60
Retry Count	Type a number of times for the Contivity 221 to retry a busy or no-answer phone number before blacklisting the number.	0
Retry Interval (sec)	Type a number of seconds for the Contivity 221 to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.	10
Drop Timeout (sec)	Type the number of seconds for the Contivity 221 to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.	20
Call Back Delay (sec)	Type a number of seconds for the Contivity 221 to wait between dropping a callback request call and dialing the corresponding callback call.	15
Apply	Click **Apply** to save your changes back to the Contivity 221.	
Reset	Click **Reset** to begin configuring this screen afresh.	

Chapter 7
Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the Contivity 221.

NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

NAT Definitions

Inside/outside denotes where a host is located relative to the Contivity 221. For example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router. For example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 26 NAT Definitions

Term	Description
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Note: NAT never changes the IP address (either local or global) of an outside host.

What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

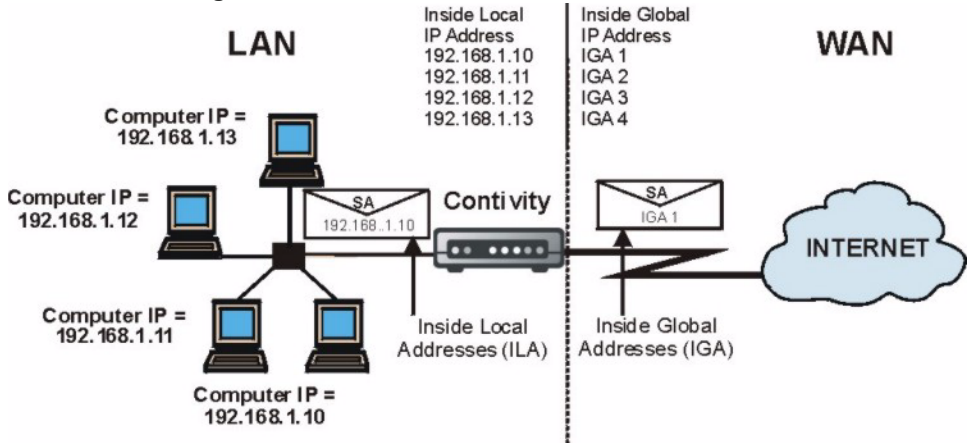
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. You can make designated servers on the LAN accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall

protection. With no servers defined, your Contivity 221 filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Contivity 221 keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 33 How NAT Works



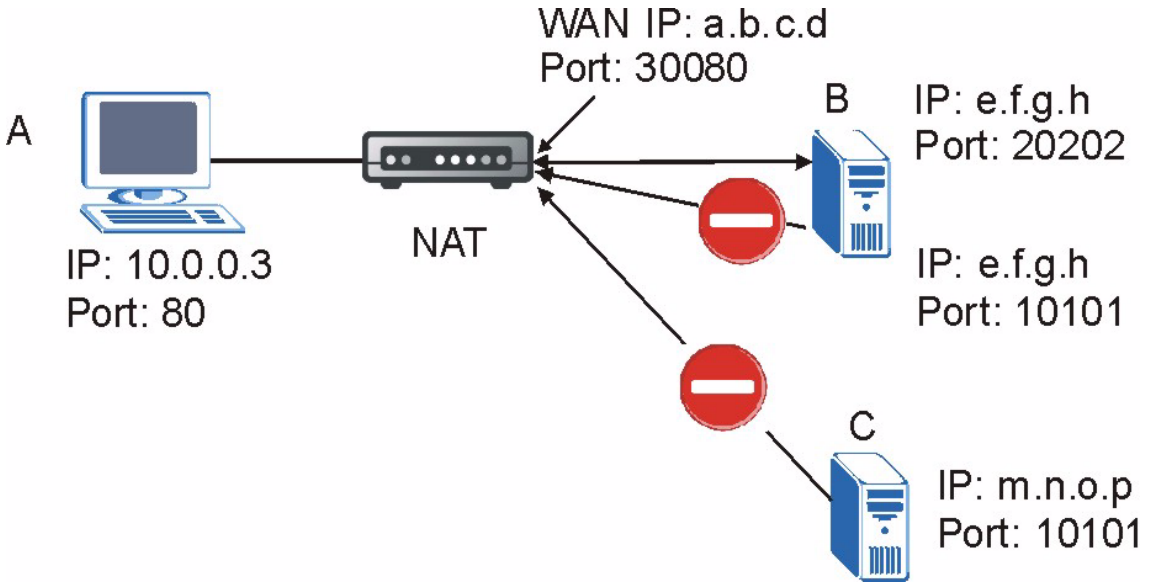
Port Restricted Cone NAT

The Contivity 221 uses port restricted cone NAT.

Port restricted cone NAT maps all requests from the same private IP address and port to the same public IP address and port. A host on the Internet can only send a packet to the private IP address and port if the private IP address and port has previously sent a packet to that host's IP address and port.

In the following figure, B can send packets, with source IP address e.f.g.h and port 20202 to A because A previously sent a packet to IP address e.f.g.h and port 20202. B cannot send packets, with source IP address e.f.g.h and port 10101 to A because A has not sent a packet to IP address e.f.g.h and port 10101.

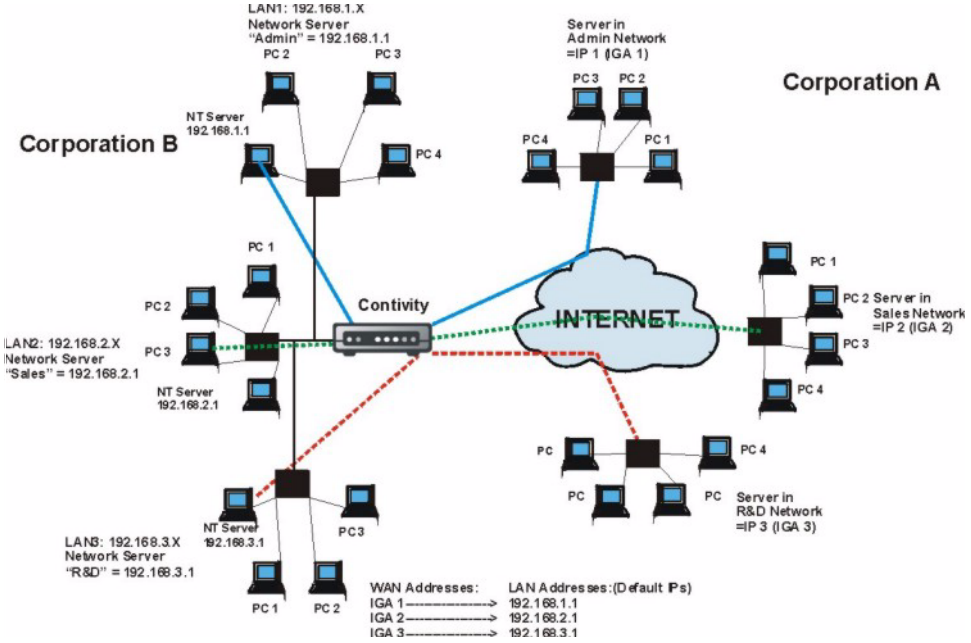
Figure 34 Port Restricted Cone NAT



NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the Contivity 221 can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 35 NAT Application With IP Alias



NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the Contivity 221 maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the Contivity 221 maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Single User Account feature (the SUA Only option).
- **Many to Many Overload**: In Many-to-Many Overload mode, the Contivity 221 maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One**: In Many-One-to-One mode, the Contivity 221 maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. Port numbers do **not** change for **One-to-One** and **Many-One-to-One** NAT mapping types.

The following table summarizes these types.

Table 27 NAT Mapping Type

Type	IP Mapping	SMT Abbreviations
One-to-One	ILA1←→ IGA1	1-1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M-1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M-M Ov
Many-One-to-One	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M-1-1
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

Using NAT

Note: You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the Contivity 221.

SUA (Single User Account) Versus NAT

SUA (Single User Account) is an implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The Contivity 221 also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA Only** or **Full Feature** in **WAN IP**.

SUA Server

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.



Note: If you do not assign a Default Server IP Address, the Contivity 221 discards all packets received for ports that are not specified here or in the remote management setup.

Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on SUA/NAT.

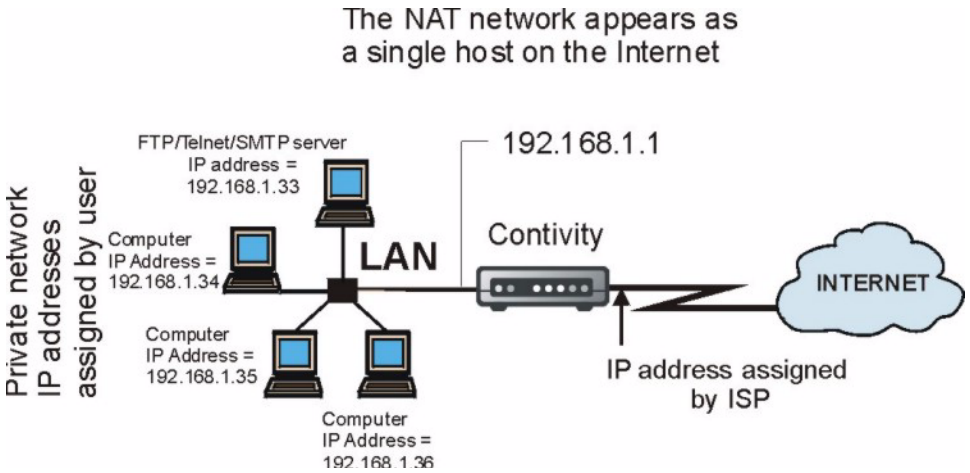
Table 28 Services and Port Numbers

Services	Port Number
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 22-25 to one server, port 80 to another and assign a default server IP address of 192.168.1.35 as shown in the next figure

Figure 36 Multiple Servers Behind NAT Example



Configuring SUA Server

Note: If you do not assign a Default Server IP Address, then all packets received for ports not specified in this screen will be discarded.

Click **SUA/NAT** to open the **SUA Server** screen.

Refer to the firewall chapters for port numbers commonly used for particular services.

Figure 37 SUA/NAT Setup



The following table describes the fields in this screen.

Table 29 SUA/NAT Setup

Label	Description
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen will be discarded.
#	Number of an individual SUA server entry.
Active	Select this check box to enable the SUA server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number here. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field

Table 29 SUA/NAT Setup

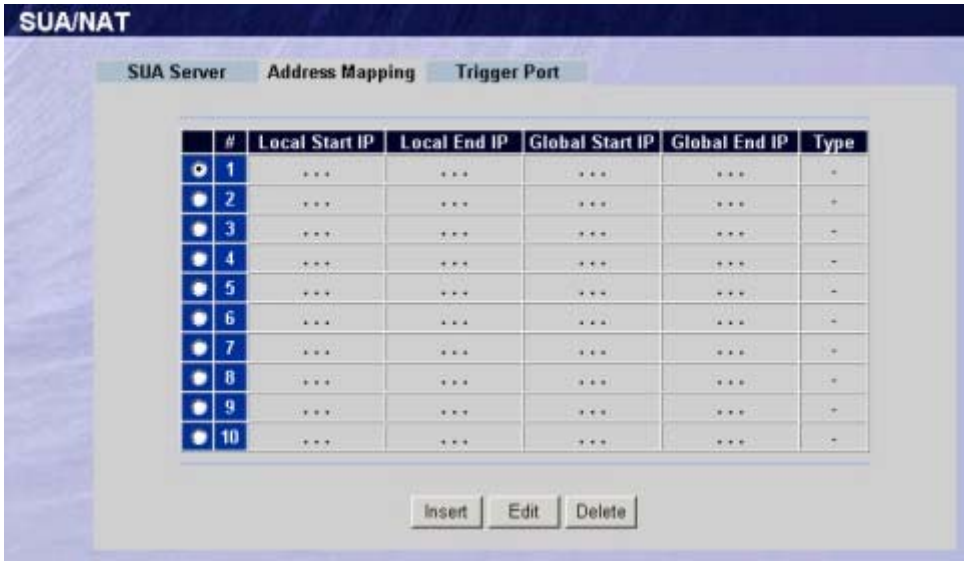
Label	Description
End Port	
Server IP Address	Enter the inside IP address of the server here.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring Address Mapping

Ordering your rules is important because the Contivity 221 applies the rules in the order that you specify. When a rule matches the current packet, the Contivity 221 takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your Contivity 221's Address Mapping settings, click **SUA/NAT**, then the **Address Mapping** tab. The screen appears as shown.

Figure 38 Address Mapping



The following table describes the fields in this screen.

Table 30 Address Mapping

Label	Description
Local Start IP	This refers to the Inside Local Address (ILA), that is the starting local IP address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global Address (IGA), that is the starting global IP address. This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.

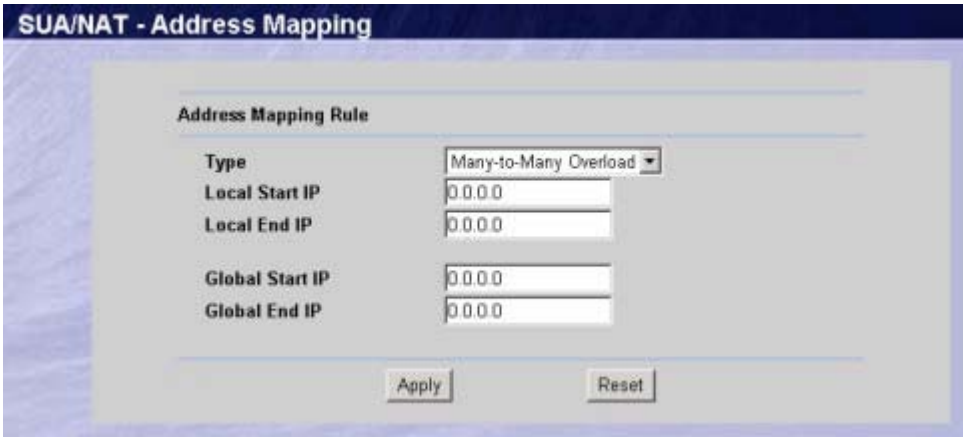
Table 30 Address Mapping

Label	Description
Type	1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. 2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Single User Account feature. 3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One** mode maps each local IP address to unique global IP addresses. 5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Edit	Click **Edit** to go to the **Address Mapping Rule** screen.
Delete	Click **Delete** to delete an address mapping rule.
Insert	Click **Insert** to insert a new mapping rule before an existing one.

Configuring Address Mapping

To edit an Address Mapping rule, click the **Edit** button to display the screen shown next.

Figure 39 Address Mapping Edit



The following table describes the fields in this screen.

Table 31 Address Mapping Edit

Label	Description
Type	Choose the port mapping type from one of the following. 1. **One-to-One**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Single User Account feature. 3. **Many-to-Many Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One**: Many One-to-one mode maps each local IP address to unique global IP addresses. 5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.

Table 31 Address Mapping Edit

Label	Description
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Trigger Port Forwarding

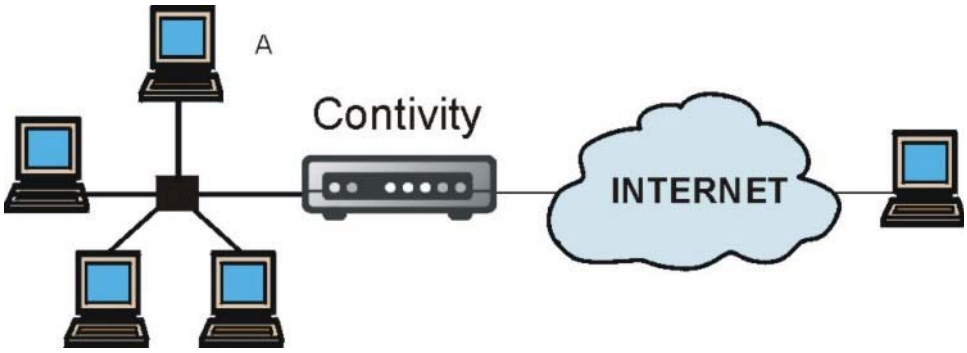
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The Contivity 221 records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the Contivity 221's WAN port receives a response with a specific port number and protocol ("incoming" port), the Contivity 221 forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 40 Trigger Port Forwarding Process: Example



1. Jane (A) requests a file from the Real Audio server (port 7070).
2. Port 7070 is a “trigger” port and causes the Contivity 221 to record Jane’s computer IP address. The Contivity 221 associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The Contivity 221 forwards the traffic to Jane’s computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The Contivity 221 times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/ Internet Protocol).

Two Points To Remember About Trigger Ports

Trigger events only happen on data that is coming from inside the Contivity 221 and going to the outside.

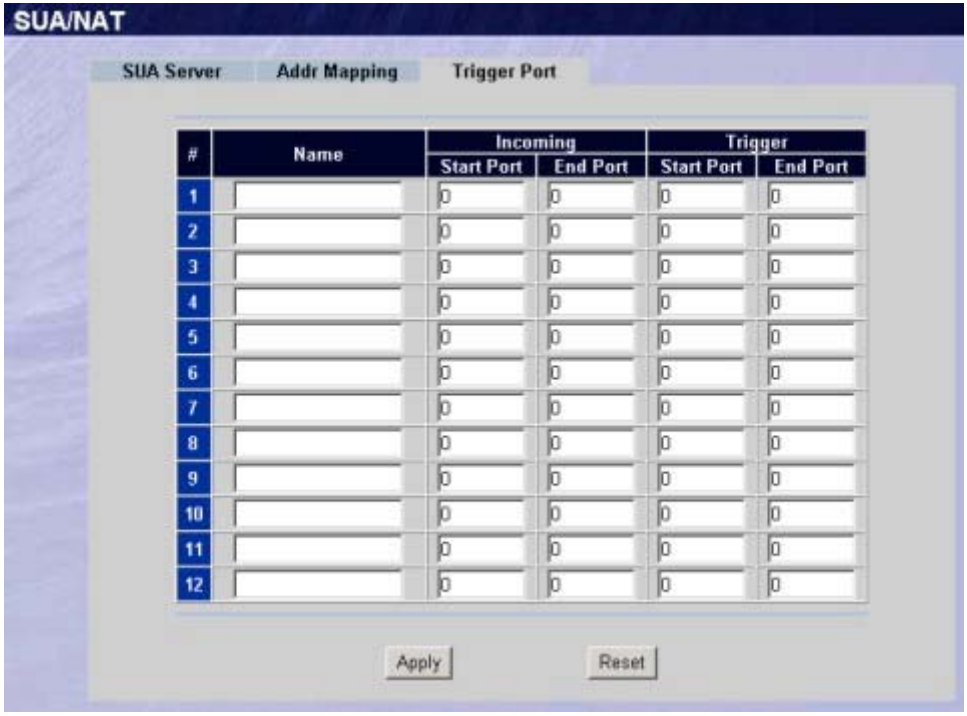
If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can’t trigger it.

Configuring Trigger Port Forwarding

To change your Contivity 221's trigger port settings, click **SUA/NAT** and the **Trigger Port** tab. The screen appears as shown.

Note: Only one LAN computer can use a trigger port (range) at a time.

Figure 41 Trigger Port



The following table describes the fields in this screen.

Table 32 Trigger Port

Label	Description
No.	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.

Table 32 Trigger Port

Label	Description
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Contivity 221 forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the Contivity 221 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

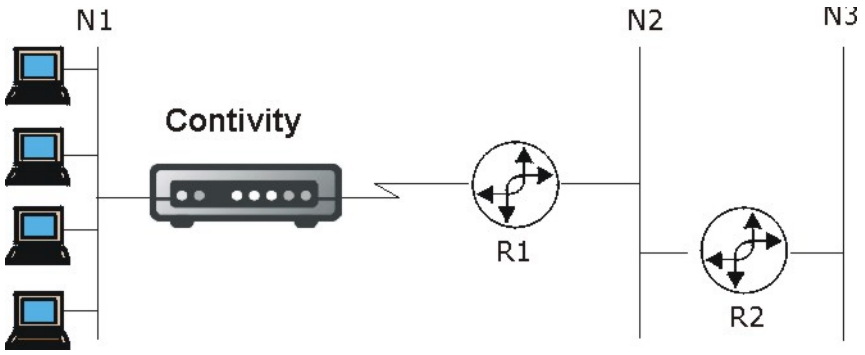
Chapter 8
Static Route Screens

This chapter shows you how to configure static routes for your Contivity 221.

Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the Contivity 221 has no knowledge of the networks beyond. For instance, the Contivity 221 knows about network N2 in the following figure through remote node Router 1. However, the Contivity 221 is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you o tell the Contivity 221 about the networks beyond the remote nodes.

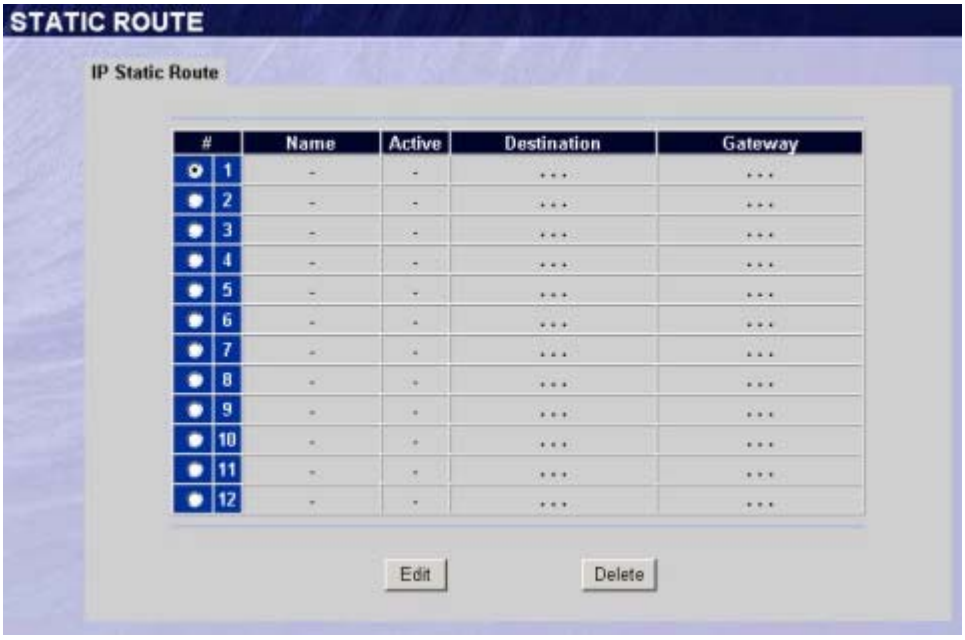
Figure 42 Example of Static Routing Topology



Configuring IP Static Route

Click **STATIC ROUTE** to open the **Route Entry** screen.

Figure 43 Static Route Screen



The following table describes the fields in this screen

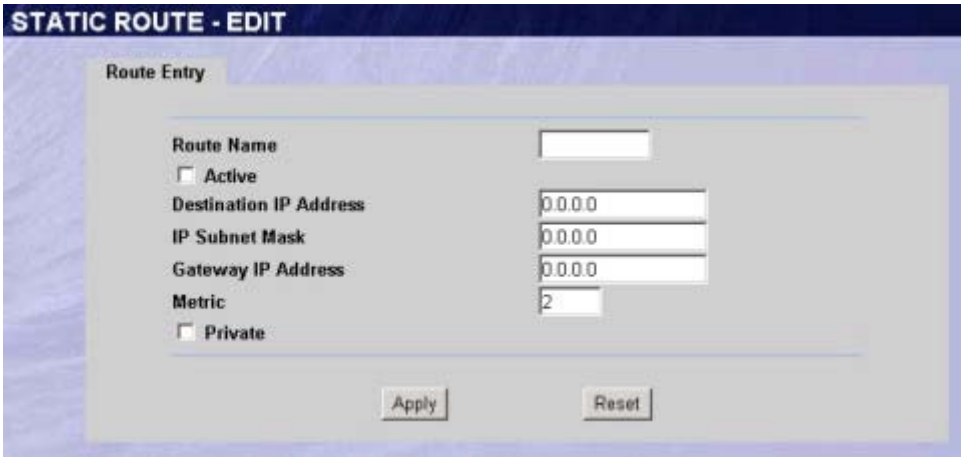
Table 33 IP Static Route Summary

Label	Description
#	Number of an individual static route.
Name	Name that describes or identifies this route.
Active	This field shows whether this static route is active (**Yes**) or not (**No**).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the Contivity 221's LAN or WAN port. The gateway helps forward packets to their destinations.
Edit	Click a static route index number and then click **Edit** to set up a static route on the Contivity 221.

Configuring Route Entry

Select a static route index number and click **Edit**. The screen shown next appears. Fill in the required information for each static route.

Figure 44 Edit IP Static Route



The following table describes the fields in this screen.

Table 34 Edit IP Static Route

Label	Description
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the Contivity 221's LAN or WAN port. The gateway helps forward packets to their destinations.

Table 34 Edit IP Static Route

Label	Description
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Contivity 221 will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 9
Firewalls

This chapter gives some background information on firewalls and introduces the Contivity 221 firewall.

Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

Types of Firewalls

There are three main types of firewalls:

1. Packet Filtering Firewalls
2. Application-level Firewalls
3. Stateful Inspection Firewalls

Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level firewalls have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

1. Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.
2. Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support.Please also see “Stateful Inspection” for more information.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

Introduction to Nortel Networks Firewall

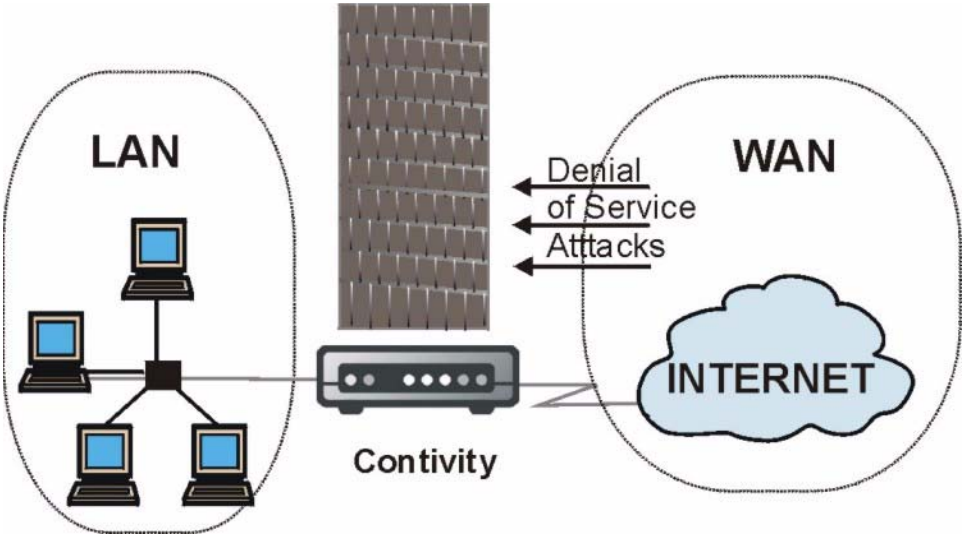
The Contivity 221 firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the WebGUI). The Contivity 221's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The Contivity 221 can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The Contivity 221 also has packet-filtering capabilities.

The Contivity 221 is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The Contivity 221 has one Ethernet WAN port and one Ethernet LAN port, which are used to physically separate the network into two areas.

- The WAN (Wide Area Network) port attaches to the broadband modem (cable or ADSL) connecting to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, "inbound access" will not be allowed unless the remote host is authorized to use a specific service.

Figure 45 Contivity 221 Firewall Application



Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The Contivity 221 is pre-configured to automatically detect and thwart all known DoS attacks.

Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An “extension number”, called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 35 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

Types of DoS Attacks

There are four types of DoS attacks:

- Those that exploit bugs in a TCP/IP implementation.
- Those that exploit weaknesses in the TCP/IP specification.
- Brute-force attacks that flood a network with useless data.
- IP Spoofing.

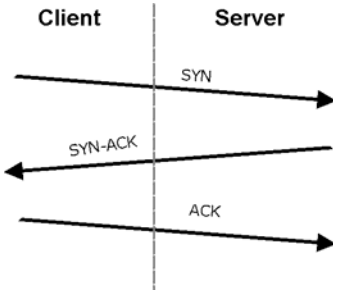
1 "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.

Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

2 Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

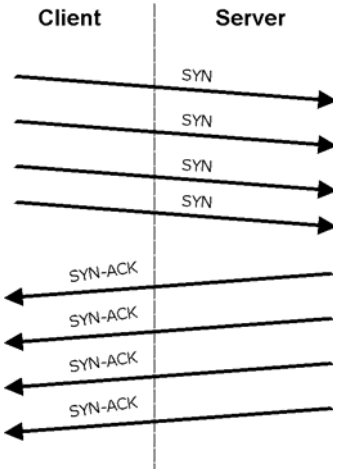
Figure 46 Three-Way Handshake



Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

SYN Attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

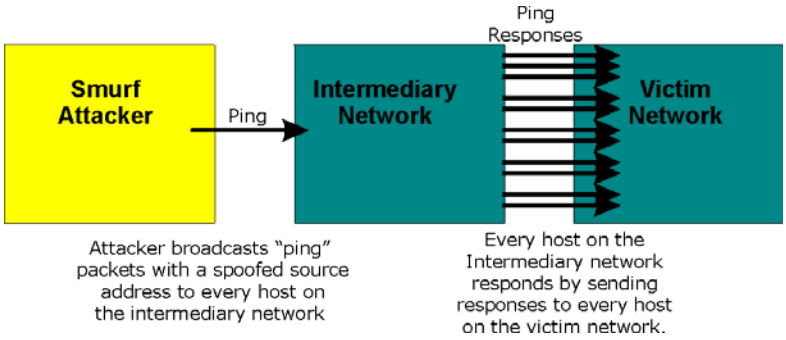
Figure 47 SYN Flood



In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

3 A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

Figure 48 Smurf Attack



- ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 36 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

Table 37 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

Table 38 Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

- Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

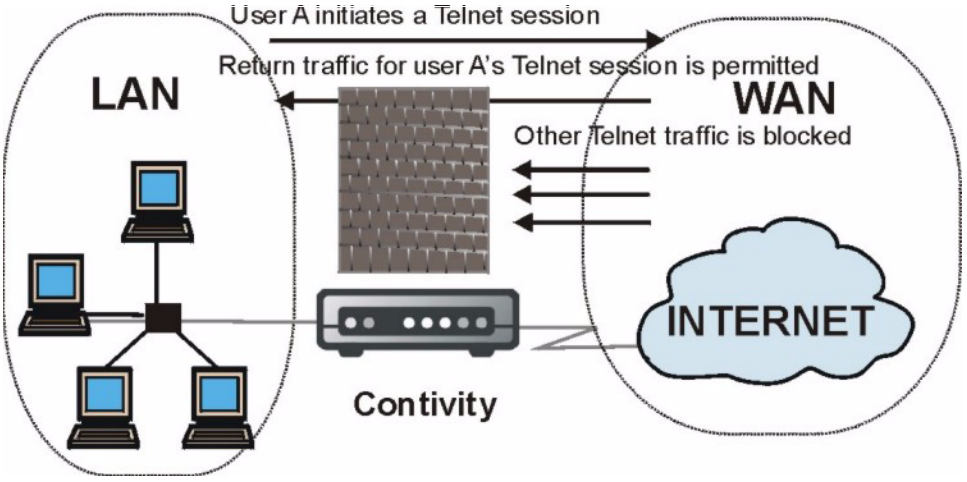
4 Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The Contivity 221 blocks all IP Spoofing attempts.

Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This “remembering” is called *saving the state.* When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The Contivity 221 uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the Contivity 221’s stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

Figure 49 Stateful Inspection



The previous figure shows the Contivity 221's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a

new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then **Action for packets that don't match firewall rules** field determines the action for this packet.

4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

Stateful Inspection and the Contivity 221

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

- Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic from the Internet to specific hosts on the LAN.
- Allow access to a Web server to everyone but competitors.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.



Note: The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the Contivity 221 itself (as with the "virtual connections" created for UDP and ICMP).

TCP Security

The Contivity 221 uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases, (see "Upper Layer Protocols"), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the Contivity 221 receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the Contivity 221 is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the Contivity 221 inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these; it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the WebGUI's Custom Ports feature to do this.

Guidelines For Enhancing Security With Your Firewall

1. Change the default password via SMT or WebGUI.
2. Think about access control *before* you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a break on the console port might give unauthorized individuals total control of the firewall, even with access control configured.
3. Limit who can telnet into your router.
4. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

Packet Filtering Vs. Firewall

Below are some comparisons between the Contivity 221's filtering and firewall functions.

Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

When To Use Filtering

1. To block/allow LAN packets by their MAC addresses.
2. To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
3. To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
4. To block/allow IP trace route.

Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

When To Use The Firewall

1. To prevent DoS attacks and prevent hackers cracking your network.
2. A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
3. To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.

4. The firewall performs better than filtering if you need to check many rules.
5. Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
6. The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

Chapter 10
Firewall Screens

This chapter shows you how to configure your Contivity 221 firewall.

Access Methods

The WebGUI is, by far, the most comprehensive firewall configuration tool your Contivity 221 has to offer. For this reason, it is recommended that you configure your firewall using the WebGUI. SMT screens allow you to activate the firewall. CLI commands provide limited configuration options and are only recommended for advanced users, please refer to the *Appendices* for firewall CLI commands.

Firewall Policies Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

LAN to LAN/Contivity 221	WAN to LAN
LAN to WAN	WAN to WAN/Contivity 221

By default, the Contivity 221's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/Contivity 221
  This allows computers on the LAN to manage the Contivity 221 and communicate between networks or subnets connected to the LAN interface.
- LAN to WAN
- By default, the Contivity 221's stateful packet inspection blocks packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/Contivity 221
  This prevents computers on the WAN from using the Contivity 221 as a gateway to communicate with other computers on the WAN and/or managing the Contivity 221.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.



Note: If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the Contivity 221's default rules.

Rule Logic Overview

Note: Study these points carefully before configuring rules.

Rule Checklist

1. State the intent of the rule. For example, “This restricts all IRC access from the LAN to the Internet.” Or, “This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server.”
2. Is the intent of the rule to forward or block traffic?
3. What direction of traffic does the rule apply to?
4. What IP services will be affected?
5. What computers on the LAN are to be affected (if any)?
6. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the WebGUI screens.

Key Fields For Configuring Rules

Action

Should the action be to **Block** or **Forward**?



Note: "Block" means the firewall silently discards the packet.

Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. Please see "Predefined Services" for more information on predefined services.

Source Address

What is the connection's source address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

Destination Address

What is the connection's destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

Connection Direction Examples

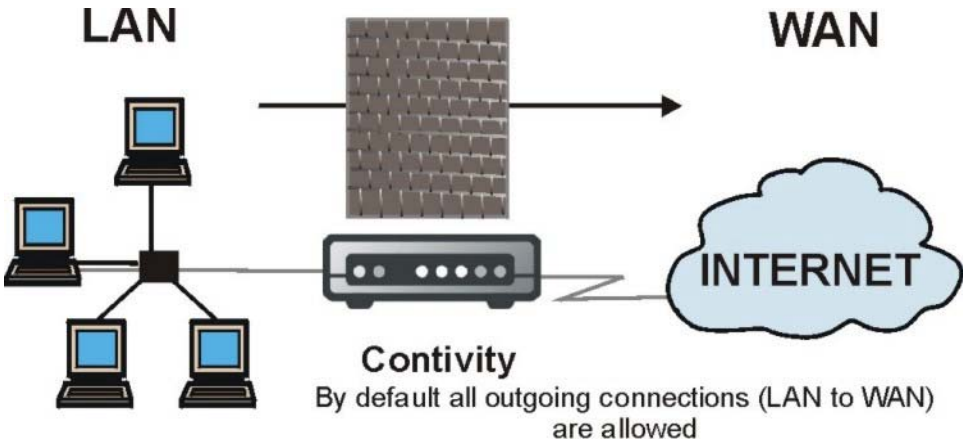
This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/Contivity 221, WAN and WAN/Contivity 221 rules apply to packets coming in on the associated interface (LAN or WAN respectively). LAN to LAN/Contivity 221 means policies for LAN-to-Contivity 221 (the policies for managing the Contivity 221 through the LAN interface) and policies for LAN-to-LAN (the policies that control routing between two subnets on the LAN). Similarly, WAN to WAN/Contivity 221 polices apply in the same way to the WAN ports.

LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

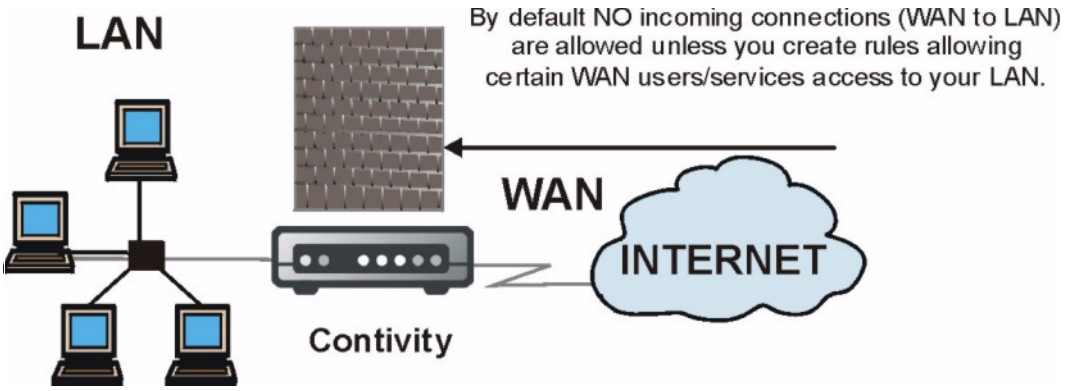
Figure 50 LAN to WAN Traffic



WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it. See the following figure.

Figure 51 WAN to LAN Traffic



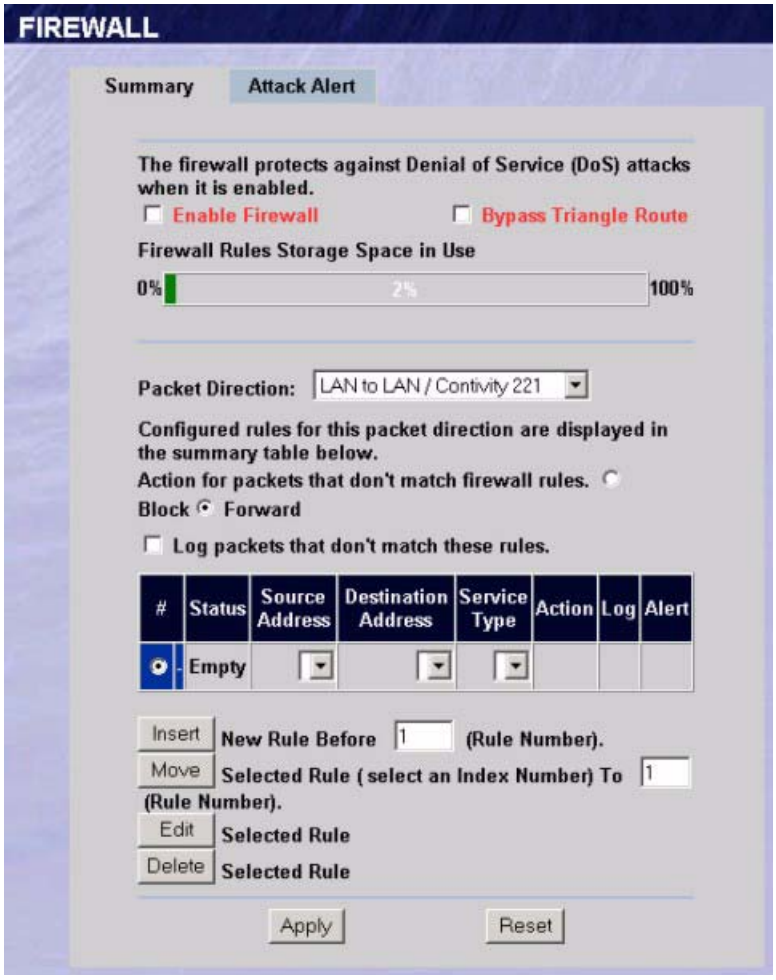
Configuring Firewall

Note: The ordering of your rules is very important as rules are applied in turn.

Click **FIREWALL** to open the **Summary** screen. Enable (or activate) the firewall by selecting the **Enable Firewall** check box as seen in the following screen.

Note: Bypassing triangle routes may let traffic from the WAN go directly to a LAN computer without passing through the Contivity 221. See the appendices for more on triangle route topology and how to deal with this problem.

Figure 52 Enabling the Firewall



The following table describes the fields in this screen.

Table 39 Firewall Rules Summary: First Screen

Label	Description
Enable Firewall	Select this check box to activate the firewall. The Contivity 221 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the Contivity 221 firewall ignore the use of triangle route topology on the network. See the *Appendices* for more on triangle route topology.

Table 39 Firewall Rules Summary: First Screen

Label	Description
Firewall Rules Storage Space in Use	This read-only bar shows how much of the Contivity 221's memory for recording firewall rules it is currently using. The bar turns from green to red when the maximum is being approached.
Packet Direction	Use the drop-down list box to select a direction of travel of packets (**LAN to LAN/Contivity 221**, **LAN to WAN**, **WAN to WAN/Contivity 221** or **WAN to LAN** for which you want to configure firewall rules.
Block/ Forward	Use the option buttons to select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that are traveling in the selected direction.
Log packets that don't match these rules.	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The **Move** field below allows you to reorder your rules.
Status	This field displays whether a firewall is turned on (**Active**) or not (**Inactive**). Rules that have not been configured display **Empty**.
Source Address	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Destination Address	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Service Type	This drop-down list box displays the services to which this firewall rule applies. Please note that a blank service type is equivalent to **Any**. Please see Table 43for more information.
Action	This is the specified action for that rule, either **Block** or **Forward**. Note that **Block** means the firewall silently discards the packet.
Log	This field shows you if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**).
Alert	This field tells you whether this rule generates an alert (**Yes**) or not (**No**) when the rule is matched.

Table 39 Firewall Rules Summary: First Screen

Label	Description
Insert	Type the index number for where you want to put a rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. Click **Insert** to display the screen where you configure a firewall rule.
Move	Select a rule’s Index option button and type a number for where you want to put that rule. Click **Move** to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Rule to (Rule Number)	Click a rule's option button and type the number for where you want to put that rule.
Edit	Click **Edit** to create or edit a rule.
Delete	Click **Delete** to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

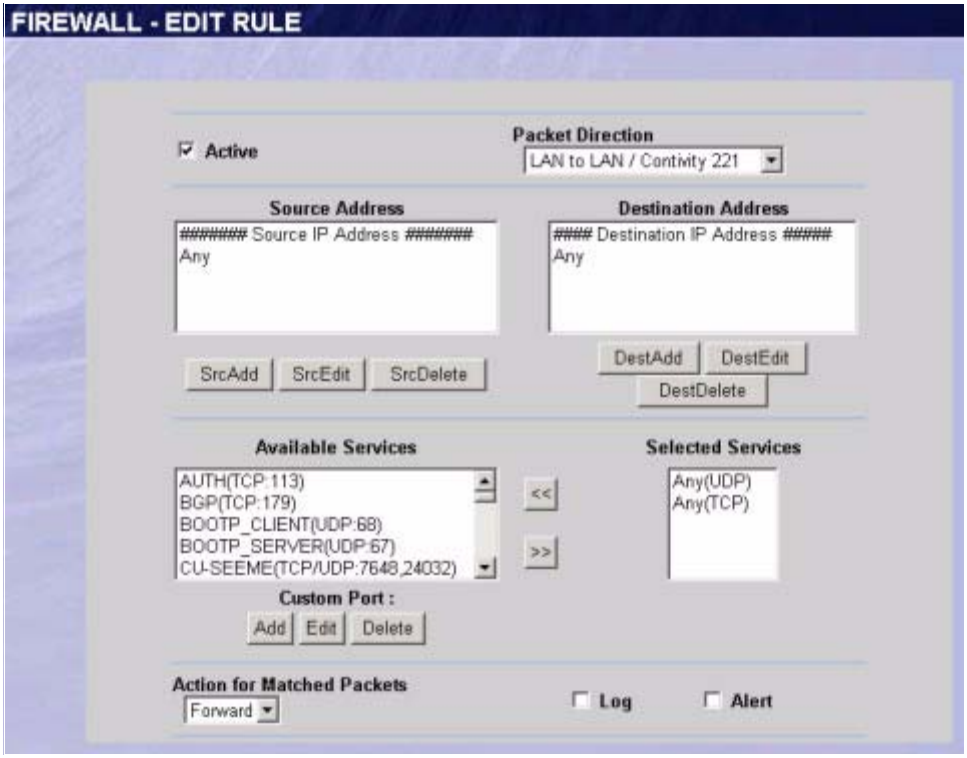
Configuring Firewall Rules

Follow these directions to create a new rule.

In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

Click **Insert** to display the following screen.

Figure 53 Creating/Editing A Firewall Rule



The following table describes the fields in this screen.

Table 40 Creating/Editing A Firewall Rule

Label	Description
Active	Check the **Active** check box to have the Contivity 221 use this rule. Leave it unchecked if you do not want the Contivity 221 to use the rule after you apply it
Packet Direction	Use the drop-down list box to select the direction of packet travel to which you want to apply this firewall rule.
Source Address	Click **SrcAdd** to add a new address, **SrcEdit** to edit an existing one or **SrcDelete** to delete one. Please see the next section for more information on adding and editing source addresses.
Destination Address	Click **DestAdd** to add a new address, **DestEdit** to edit an existing one or **DestDelete** to delete one. Please see the following section on adding and editing destination addresses.

Table 40 Creating/Editing A Firewall Rule

Label	Description
Services Available/ Selected Services	Please see Table 43 for more information on services available. Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **<<**.
Custom Port	
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Edit	Select a custom service (denoted by an "*") from the **Available Services** list and click this button to edit the service.
Delete	Select a custom service (denoted by an "*") from the **Available Services** list and click this button to remove the service.
Action for Matched Packets	Use the drop down list box to select whether to discard (**Block**) or allow the passage of (**Forward**) packets that match this rule.
Log	This field determines if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**). Go to the **Log Settings** page and select the **Access Control** logs category to have the Contivity 221 record these logs.
Alert	Check the **Alert** check box to determine that this rule generates an alert when the rule is matched.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving,

Configuring Source and Destination Addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen**.** Either action displays the following screen.

Figure 54 Adding/Editing Source and Destination Addresses



The following table describes the fields in this screen.

Table 41 Adding/Editing Source and Destination Addresses

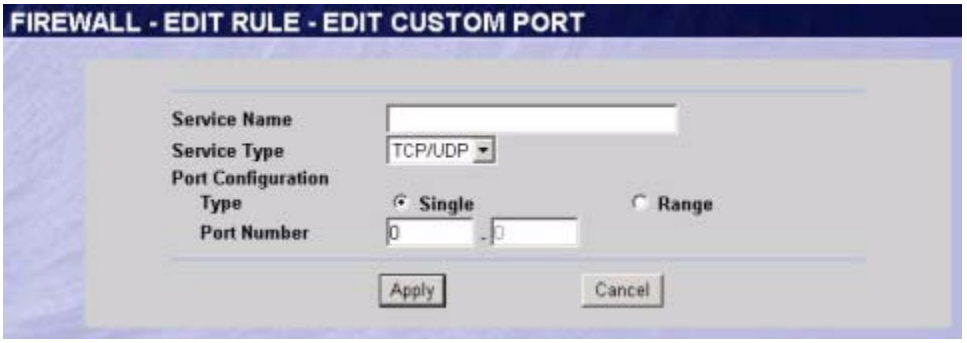
Label	Description
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving,

Configuring Custom Ports

Configure customized ports for services not predefined by the Contivity 221 *(see "Predefined Services"* for a list of predefined services*)*. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

Click the **Add** button under **Custom Port** while editing a firewall to configure a custom port. This displays the following screen.

Figure 55 Creating/Editing A Custom Port



The following table describes the fields in this screen.

Table 42 Creating/Editing A Custom Port

Label	Description
Service Name	Enter a unique name for your custom port.
Service Type	Choose the IP port (**TCP**, **UDP** or **Both**) that defines your customized port from the drop down list box.
Port Configuration Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.
Port Number	Enter a single port number or the range of port numbers that define your customized service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving,

Example Firewall Rule

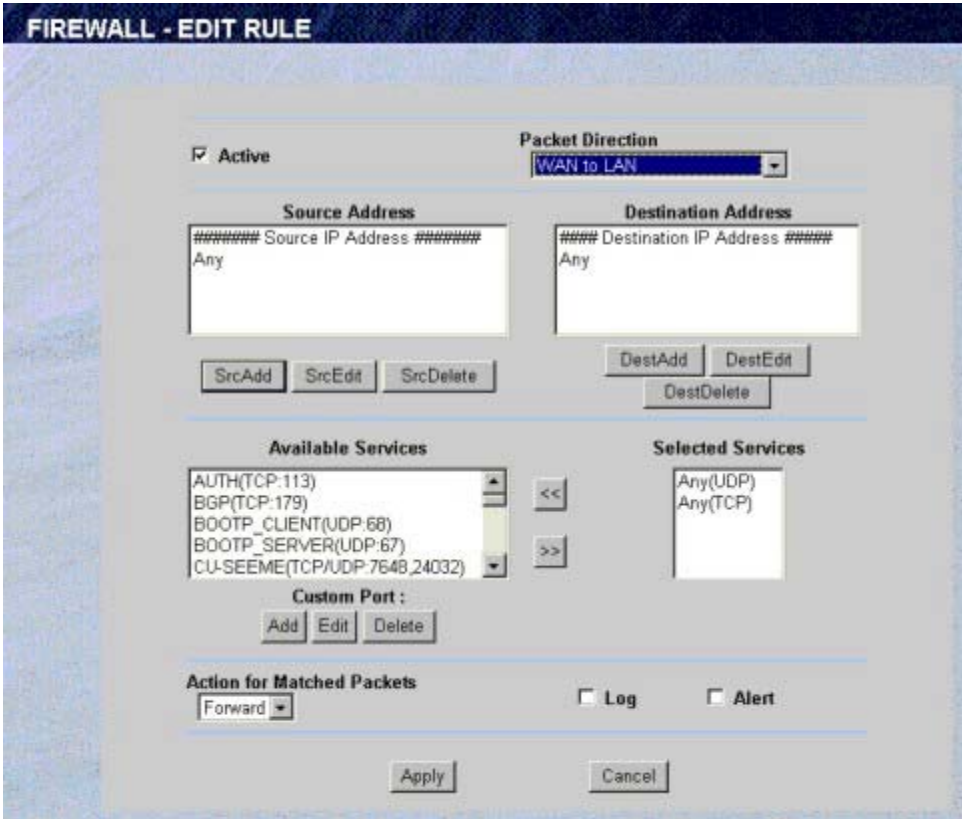
The following Internet firewall rule example allows a hypothetical “My Service” connection from the Internet.

1 Click the **Firewall** link and then the **Summary** tab.

2 In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

3 Click **Insert** to display the firewall rule configuration screen.

Figure 56 Firewall Edit Rule Screen Example



4 Select **WAN to LAN** as the **Packet Direction**.

5 Select **Any** in the Destination Address box and then click **DestDelete**.

6 Click **DestAdd** under the Source Address box.

7 Configure the **Firewall Rule Edit IP** screen as follows and click **Apply**.

Figure 57 Firewall Rule Edit IP Example



8 In the firewall rule configuration screen, click **Add** under **Custom Port** to open the **Edit Custom Port** screen. Configure it as follows and click **Apply**.

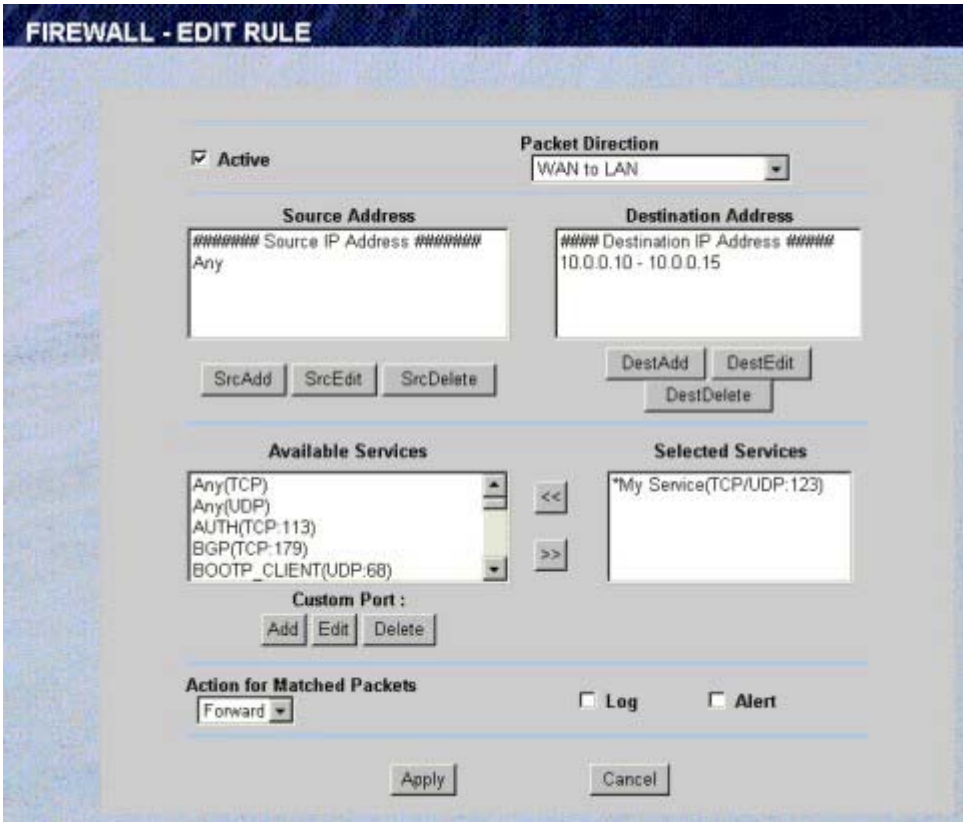
Figure 58 Edit Custom Port Example



9 The firewall rule configuration screen displays, use the arrows between **Available Services** and **Selected Services** to configure it as follows. Click **Apply** when you are done.

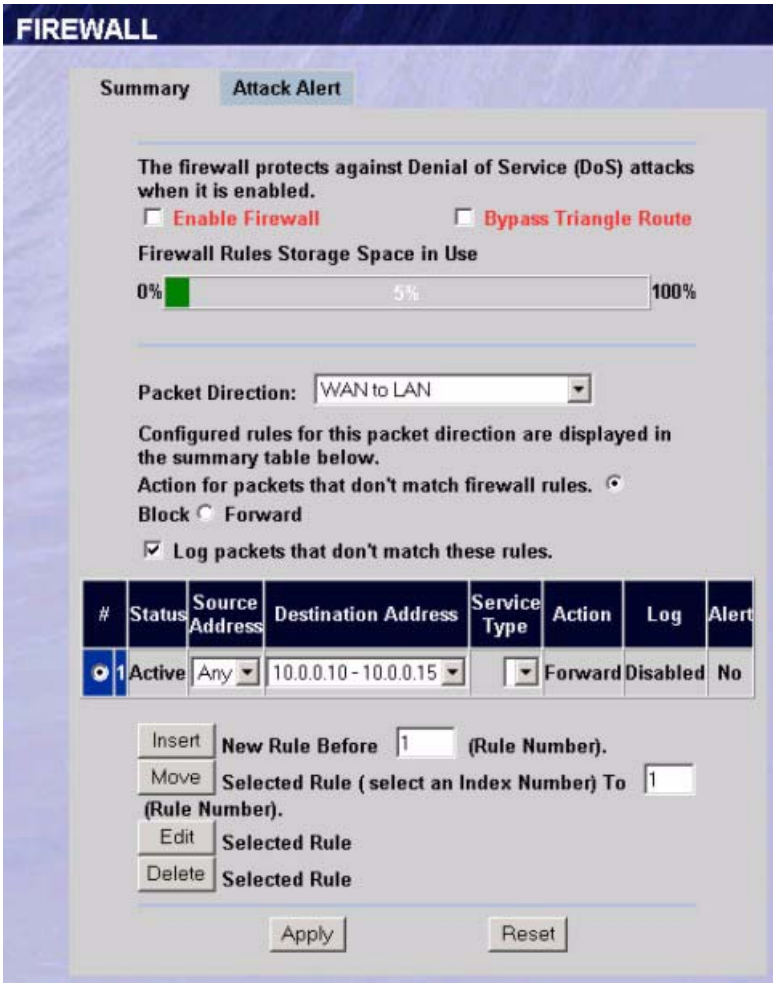
Note: Custom ports show up with an "*" before their names in the Services list box and the Rule Summary list box. Click Apply after you've created your custom port.

Figure 59 MyService Rule Configuration Example



On completing the configuration procedure for this Internet firewall rule, the **Rule Summary** screen should look like the following. Rule 1: Allows a “My Service” connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN. Remember to click **Apply** when you have finished configuring your rule(s) to save your settings back to the Contivity 221.

Figure 60 My Service Example Rule Summary



Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see Figure 53) displays all predefined services that the Contivity 221 already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port

number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Custom services may also be configured using the **Custom Ports** function discussed later.

Table 43 Predefined Services

Service	Description
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.nortelnetworks.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.

Table 43 Predefined Services

Service	Description
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/ UDP:162)	Traps for use with the SNMP (RFC:1215).

Table 43 Predefined Services

Service	Description
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SIP-V2(UDP:5060)	The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Attack Alert** screen *(*Figure 61 check the **Generate alert when attack detected** check box) or when a rule is matched in the **Rule Edit** screen (see Figure 53). Configure the **Log Settings** screen to have the Contivity 221 send an immediate e-mail message to you when an event generates an alert.

Configuring Attack Alert

Attack alerts are the first defense against DOS attacks. In the **Attack Alert** screen, shown later, you may choose to generate an alert whenever an attack is detected. For DoS attacks, the Contivity 221 uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for normal small offices with ADSL bandwidth. Factors influencing choices for threshold values are:

- The maximum number of opened sessions.
- The minimum capacity of server backlog in your LAN network.
- The CPU power of servers in your LAN network.
- Network bandwidth.
- Type of traffic for certain servers.

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.
You should make any changes to the threshold values before you continue configuring firewall rules.

Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see Figure 46). For UDP, "half-open" means that the firewall has detected no return traffic.

The Contivity 221 measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the Contivity 221 starts deleting half-open sessions as required to accommodate new connection requests. The Contivity 221 continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the Contivity 221 starts deleting half-open sessions as required to accommodate new connection requests. The Contivity 221 continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

TCP Maximum Incomplete and Blocking Period

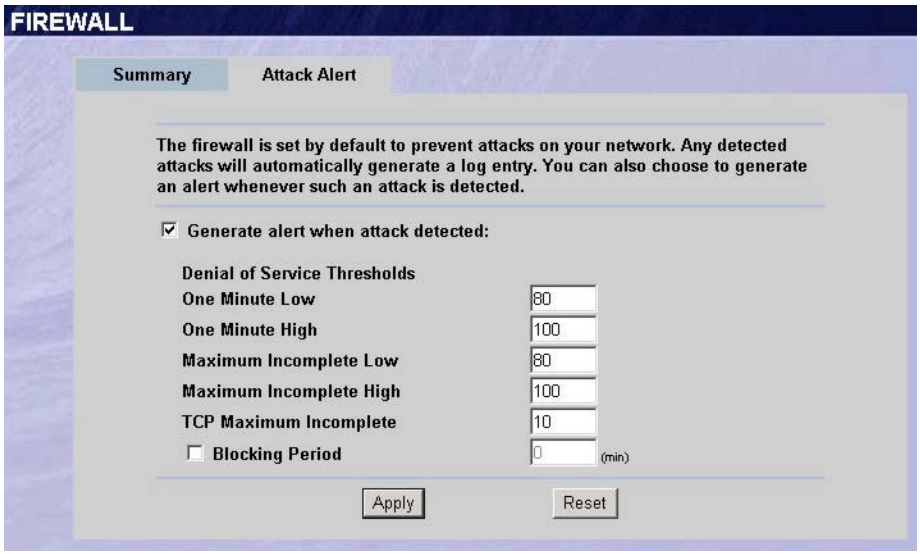
An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the Contivity 221 starts deleting half-open sessions according to one of the following methods:

- If the **Blocking Period** timeout is 0 (the default), then the Contivity 221 deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
- If the **Blocking Period** timeout is greater than 0, then the Contivity 221 blocks all new connection requests to the host giving the server time to handle the present connections. The Contivity 221 continues to block all new connection requests until the **Blocking Period** expires.

The Contivity 221 also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click the **Attack Alert** tab to bring up the next screen.

Figure 61 Attack Alert



The following table describes the fields in this screen.

Table 44 Attack Alert

Label	Description
Generate alert when attack detected	A detected attack automatically generates a log entry. Check this box to generate an alert (as well as a log) whenever an attack is detected.
Denial of Service Thresholds	
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The Contivity 221 continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the Contivity 221 deletes half-open sessions as required to accommodate new connection attempts. The numbers, say 80 in the **One Minute Low** field and 100 in this field, cause the Contivity 221 to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.

Table 44 Attack Alert

Label	Description
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The Contivity 221 continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the Contivity 221 deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number. The above values, say 80 in the **Maximum Incomplete Low** field and 100 in this field, cause the Contivity 221 to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.
Blocking Period	When **TCP Maximum Incomplete** is reached you can choose if the next session should be allowed or blocked. If you select the **Blocking Period** check box, any new sessions will be blocked for the length of time you specify in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.
(min)	Enter the length of **Blocking Period** in minutes.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 11
Content Filtering

This chapter provides a brief overview of content filtering using the embedded WebGUI.

Introduction to Content Filtering

Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URL keywords and should not be confused with packet filtering via SMT menu 21.1. To access these functions, from the **Main Menu**, click **Content Filter** to expand the Content Filter menus.

Restrict Web Features

The Contivity 221 can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

Days and Times

The Contivity 221 also allows you to define time periods and days during which the Contivity 221 performs content filtering.

Configure Content Filtering

Click **Content Filter** on the navigation panel, to open the following screen.

Figure 62 Content Filter

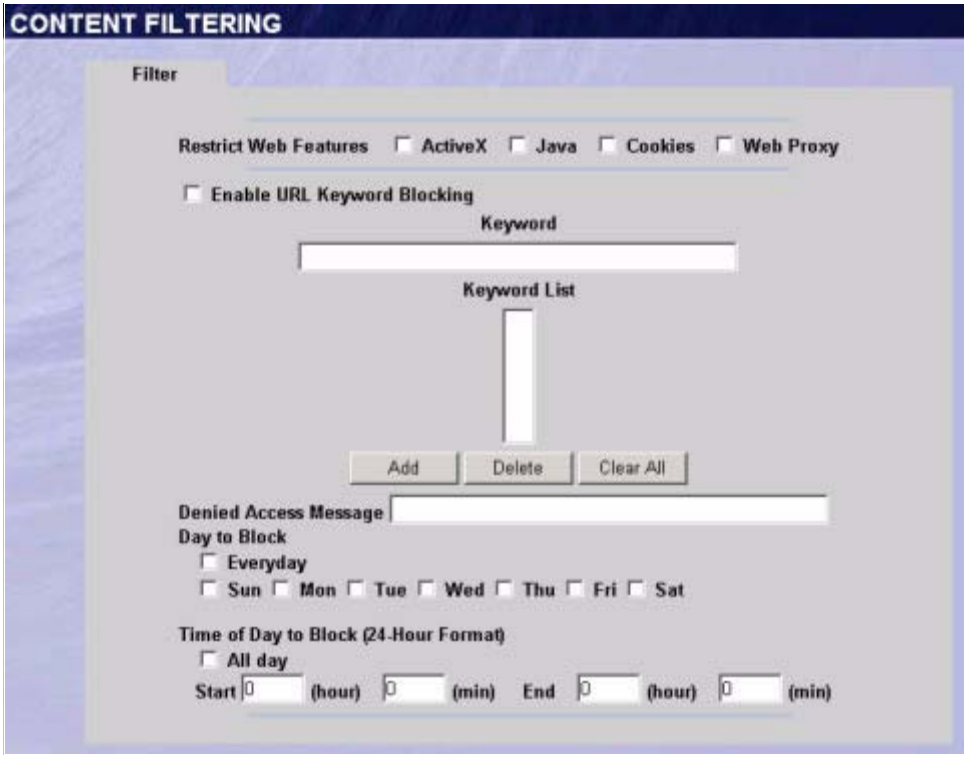


Table 45 Content Filter

Label	Description
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.

Table 45 Content Filter

Label	Description
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The Contivity 221 can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http:// www.website.com/bad.html would be blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Clear All	Click this button to remove all of the listed keywords.
Day to Block	Select check boxes for the days that you want the Contivity 221 to perform content filtering. Select the **Everyday** check box to have content filtering turned on all days of the week.
Time of Day to Block	Time of Day to Block allows the administrator to define during which time periods content filtering is enabled. Time of Day to Block restrictions only apply to the keywords (see above). Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. Enter the time period, in 24-hour format, during which content filtering will be enforced. Select the **All Day** check box to have content filtering always active on the days selected in **Day to Block** with time of day limitations not enforced.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh

Chapter 12
Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/ services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

Security Association

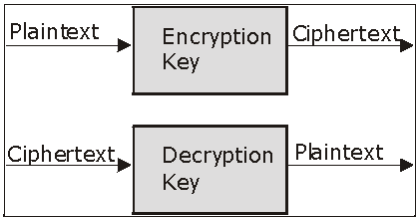
A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

Other Terminology

Encryption

Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms “ciphertext” to plaintext. Decryption also requires a key.

Figure 63 Encryption and Decryption



Data Confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

Data Integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

Data Origin Authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

VPN Applications

The Contivity 221 supports the following VPN applications.

- Linking Two or More Private Networks Together

Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

- Accessing Network Resources When NAT Is Enabled

When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

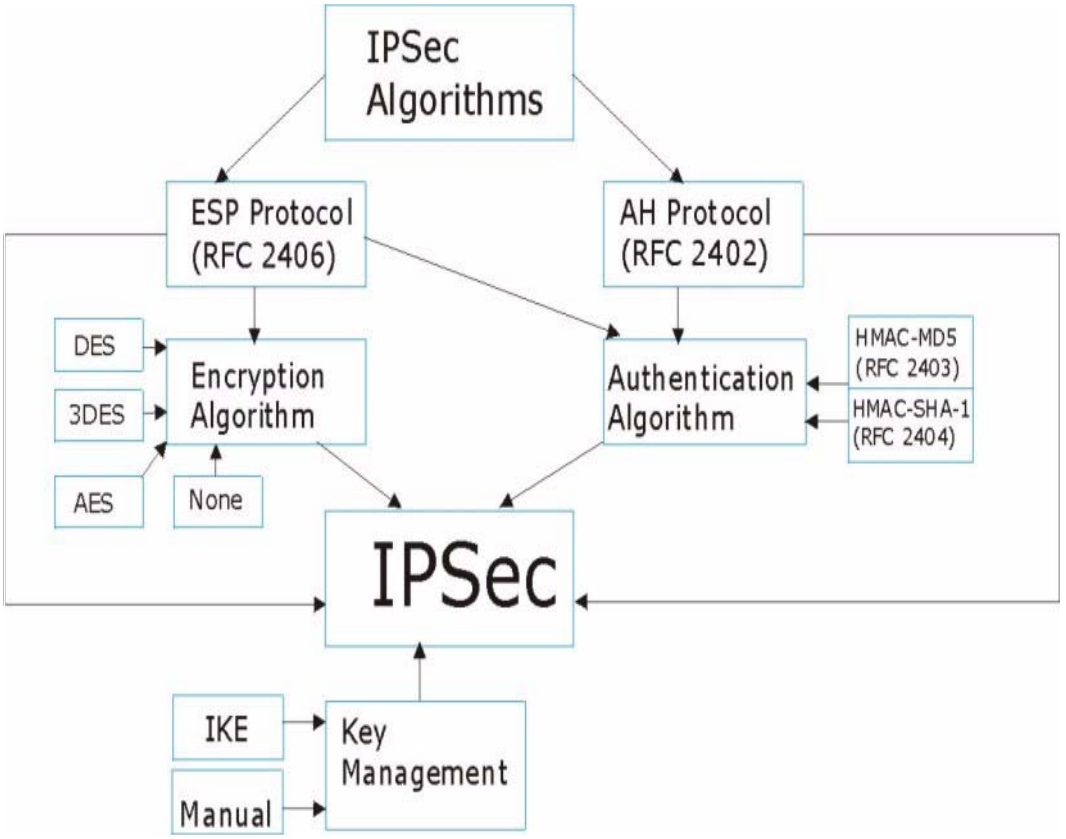
- Unsupported IP Applications

A VPN tunnel may be created to add support for unsupported emerging IP applications.

IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 64 IPSec Architecture



IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Please see IPSec Algorithms for more information.

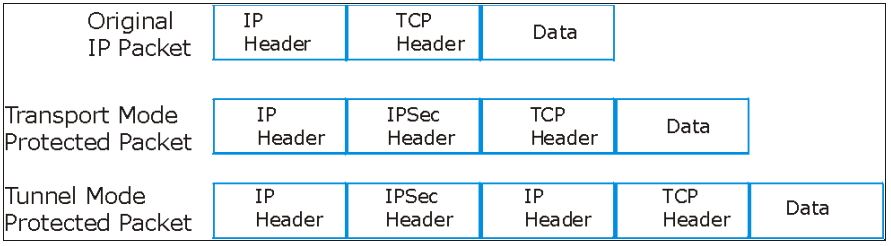
Key Management

Your Contivity 221 uses IKE (ISAKMP) key management in order to set up a VPN.

Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Figure 65 Transport and Tunnel Mode IPSec Encapsulation



Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for VPN switch to VPN switch and host to VPN switch communications. **Tunnel** mode communications have two sets of IP headers:

Outside header: The outside IP header contains the destination IP address of the VPN switch.

Inside header: The inside IP header contains the destination IP address of the final system behind the VPN switch. The security protocol appears after the outer IP header and before the inside IP header.

IPSec and NAT

Read this section if you are running IPSec on a host computer behind the Contivity 221.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN switch, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (see *section NAT Traversal* for details).

Table 46 VPN and NAT

Security Protocol	Mode	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

Chapter 13
VPN Screens

This chapter introduces the VPN WebGUI. See the Logs chapter for information on viewing logs and the appendices for IPSec log descriptions.

VPN/IPSec Overview

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 47 AH and ESP

	ESP	**AH**
Encryption	**DES** (default) Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data.	
	3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	
	AES Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data during phase 1. You can configure the device to use a 128-bit, 192-bit or 256-bit key for phase 2. AES is faster than 3DES.	
	Select **NULL** to set up a phase 2 tunnel without encryption.	

Table 47 AH and ESP

	ESP	**AH**
Authentication	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select **MD5** for minimal security and **SHA-1** for maximum security.	

My IP Address

My IP Address is the WAN IP address of the Contivity 221. The Contivity has to rebuild the VPN tunnel if the **My IP Address** changes after setup.

The following applies if this field is configured as 0.0.0.0:

- The Contivity 221 uses the current Contivity 221 WAN IP address (static or dynamic) to set up the VPN tunnel.
- If the WAN connection goes down, the Contivity 221 uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.

Secure Gateway Address

Secure Gateway Address is the WAN IP address or domain name of the remote VPN switch (secure gateway).

If the remote VPN switch has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote VPN switch's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote VPN switch's domain name in the **Secure Gateway Address** field if the remote VPN switch has a dynamic WAN IP address and is using DDNS. The Contivity 221 has to rebuild the VPN tunnel each time the remote VPN switch's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote VPN switch's new WAN IP address).

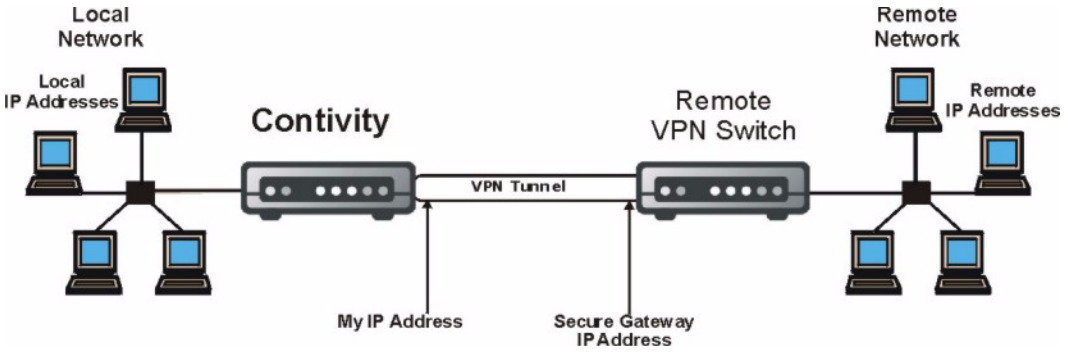
Dynamic Secure Gateway Address

If the remote VPN switch has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the remote VPN switch's address. In this case only the remote VPN switch can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network.

Summary Screen

The following figure helps explain the main fields in the WebGUI.

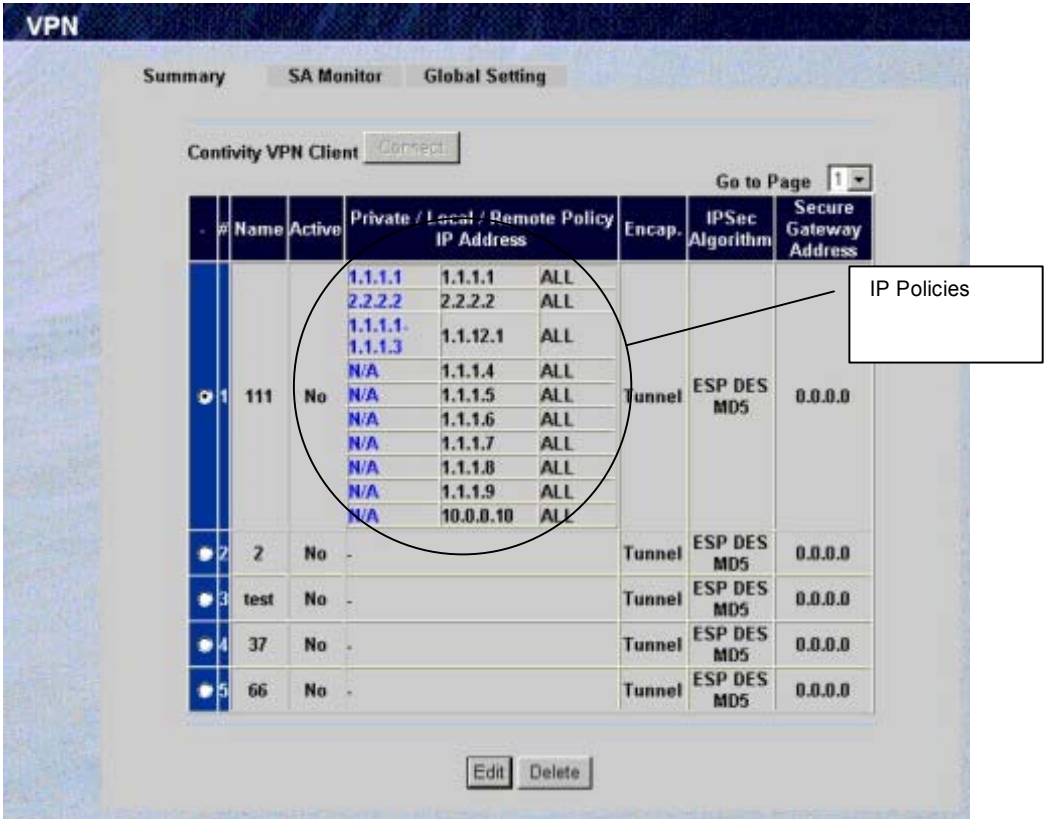
Figure 66 IPSec Summary Fields



Local and remote IP addresses must be static.

Click **VPN** to open the **Summary** screen. This is a read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then clicking **Edit** to configure the associated submenus.

Figure 67 Summary



The following table describes the fields in this screen.

Table 48 Summary

Label	Description
Contivity VPN Client	The Contivity VPN Client is a simple VPN rule that lets you define and store connection information for accessing your corporate network through a Contivity VPN switch. The Contivity VPN Client uses the IPSec protocol to establish a secure end-to-end connection. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive.
Connect	Create a VPN connection to remote Contivity switch.
Disconnect	Drop the Contivity VPN connection.

Table 48 Summary

Label	Description
Go to Page	This displays when the total number of the VPN rules' IP policies is more than ten. There can be a total of five VPN rules. The VPN rules can have a combined total of total of 60 IP policies. Each page can display up to ten IP policies. Therefore, it may take more than one page to display one VPN rule's IP policies. Each page always displays all of the configured VPN rules, although the rule's IP policies may not all display. You may need to select another page number from this **Go to Page** drop-down list box to view other IP policies.
#	This is the VPN rule index number.
Active	This field displays whether the VPN rule is active or not. A **Yes** signifies that this VPN rule is active. **No** signifies that this VPN rule is not active.
Private /Local / Remote Policy IP Address	This field displays private, local and remote IP addresses when you configure the VPN rule's IP policy to use branch tunnel NAT address mapping. This field displays only local and remote IP addresses when you configure the VPN rule's policy to not use branch tunnel NAT address mapping. See the following descriptions for more details about the private, local and remote IP addresses.
Private Policy IP Address	The **Private Policy IP Address** or **Local Policy IP Address** field displays the IP address (or range of IP addresses) of the computer (or computers) on your Contivity 221's local network, for which you have configured this VPN rule IP policy. A **Private Policy IP Address** displays in blue, this applies when you configure the IP policy to use branch tunnel NAT address mapping. The **Private Policy IP Address** field displays a single (static) IP address when the IP policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **One-to-One** in the **IP Policy** screen. The **Private Policy IP Address** field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **Many One-to-one** or **Many-to-One** in the **IP Policy** screen.

Table 48 Summary

Label	Description
Local Policy IP address	The **Local Policy IP Address** field displays the IP policy's virtual IP address (or range of addresses) when you enable branch tunnel NAT address mapping in the **IP Policy** screen. The **Local Policy IP Address** field displays a single (static) IP address when the IP policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **One-to-one** or **Many-to-One** in the **IP Policy** screen. The **Local Policy IP Address** field displays the beginning and ending (static) IP addresses of a range of computers when the policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **Many One-to-one** in the **IP Policy** screen. The **Local Policy IP Address** field displays the policy's local IP address (or range of addresses) when you disable branch tunnel NAT address mapping in the **IP Policy** screen. The **Local Policy IP Address** field displays a single (static) IP address when the IP policy's **Local Address Type** field is configured to **Single Address** in the **IP Policy** screen. The **Local Policy IP Address** field displays the beginning and ending (static) IP addresses of a range of computers when the policy's **Local Address Type** field is configured to **Range Address** in the **IP Policy** screen. The **Local Policy IP Address** field displays a (static) IP address and a subnet mask when the policy's **Local Address Type** field is configured to **Subnet Address** in the **IP Policy** screen.
Remote Policy IP Address	The **Remote Policy IP Address** field displays the IP address(es) of computer(s) on the remote network behind the remote VPN switch. A single (static) IP address displays for the **Remote Policy IP Address** when the IP policy's **Remote Address Type** field is configured to **Single Address** in the **IP Policy** screen. The beginning and ending (static) IP addresses of a range of computers display for the **Remote Policy IP Address** when the IP policy's **Remote Address Type** field is configured to **Range Address** in the **IP Policy** screen. A (static) IP address and a subnet mask display for the **Remote Policy IP Address** when the IP policy's **Remote Address Type** field is configured to **Subnet Address** in the **IP Policy** screen. The **Remote Policy IP Address** displays **ALL** whenever the **Secure Gateway Address** field is set to **0.0.0.0**. The **Remote Policy IP Address** also displays **ALL** whenever the IP policy's **Remote Starting IP Address** field is set to **0.0.0.0** in the **IP Policy** screen. When **ALL** displays, only the remote VPN switch can initiate the VPN.
Encap	This field displays **Tunnel** or **Transport** mode. You need to finish configuring the VPN policy if **???** is displayed.

Table 48 Summary

Label	Description
IPSec Algorithm	This field displays the security protocols used for an SA. Both **AH** and **ESP** increase Contivity 221 processing requirements and communications latency (delay).
Secure Gateway Address	This is the static WAN IP address or URL of the remote VPN switch. This field displays **0.0.0.0** when you configure the **Secure Gateway Address** field in the **VPN Branch Office** screen to **0.0.0.0.**
Edit	Click the radio button next to a VPN index number and then click **Edit** to edit a specific VPN policy. Click the radio button next to an empty VPN policy index number and then **Edit** to add a new VPN policy.
Delete	Click the radio button next to a VPN policy number you want to delete and then click **Delete**. When a VPN policy is deleted, subsequent policies do not move up in the page list.

Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the Contivity 221 automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see the *Configuring Advanced Branch Office Setup* section for more on the IPSec SA lifetime). The keep alive option is available with the Contivity Client rule. In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Both VPN switches must have a Contivity 221-compatible keep alive feature enabled in order for this feature to work.

If the Contivity 221 has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the Contivity 221 because the Contivity 221 never drops the tunnels that are already connected.



Note: No matter whether or not keep alive is set, when there is outbound traffic with no inbound traffic, the Contivity 221 automatically drops the tunnel after two minutes.

Nailed Up

The nailed up feature is similar to the keep alive feature. When you initiate an IPSec tunnel with nailed up enabled, the Contivity 221 automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see *section Configuring Advanced Branch Office Setup* for more on the IPSec SA lifetime). The nailed up option is available with the branch office rules. Unlike keep alive, anytime the Contivity 221 restarts, it also automatically renegotiates any nailed up tunnels. In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Also different from keep alive, the peer VPN switch does not have to have a Contivity 221-compatible nailed up feature enabled in order for this feature to work.

If the Contivity 221 has its maximum number of simultaneous IPSec tunnels connected to it and they all have nailed up enabled, then no other tunnels can take a turn connecting to the Contivity 221 because the Contivity 221 never drops the tunnels that are already connected.

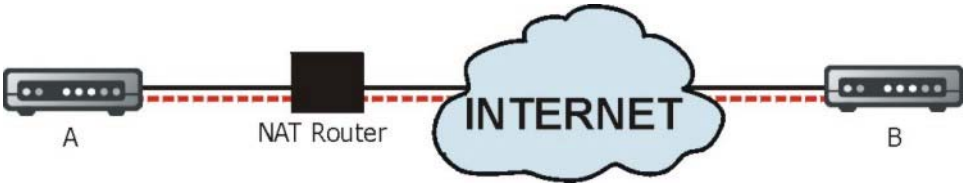


Note: No matter whether or not nailed up is set, when there is outbound traffic with no inbound traffic, the Contivity 221 automatically drops the tunnel after two minutes.

NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between the two VPN switches.

Figure 68 NAT Router Between VPN Switches



Normally you cannot set up a VPN connection with a NAT router between the two VPN switches because the NAT router changes the header of the IPSec packet. In the previous figure, VPN switch A sends an IPSec packet in an attempt to initiate a VPN. The NAT router changes the IPSec packet's header so it does not match the header for which VPN switch B is checking. Therefore, VPN switch B does not respond and the VPN connection cannot be built.

NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. VPN switch B checks the UDP port 500 header and responds. VPN switches A and B build a VPN connection.

NAT Traversal Configuration

For NAT traversal to work you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.

In order for VPN switch A (see the figure) to receive an initiating IPSec packet from VPN switch B, set the NAT router to forward UDP port 500 to VPN switch A.

ID Type and Content

With aggressive negotiation mode (see *section* Negotiation Mode), the Contivity 221 identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the Contivity 221 to distinguish between multiple rules for SAs that connect from remote VPN switches that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the Contivity 221 from VPN switches with dynamic IP addresses.



Note: Regardless of the ID type and content configuration, the Contivity 221 does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see *section* Negotiation Mode), the ID type and content are encrypted to provide identity protection. In this case the Contivity 221 can only distinguish between up to eight different incoming SAs that connect from remote VPN switches that have dynamic WAN IP addresses. The Contivity 221 can distinguish up to eight incoming SAs because you can select between two encryption algorithms (DES and 3DES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see *section Configuring Advanced Branch Office Setup*). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 49 Local ID Type and Content Fields

Local ID type=	**Content=**
IP	Type the IP address of your computer or leave the field blank to have the Contivity 221 automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this Contivity 221.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this Contivity 221.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.	

Table 50 Peer ID Type and Content Fields

Peer ID type=	**Content=**
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Contivity 221 automatically use the address in the **Secure Gateway** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote VPN switch.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote VPN switch.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote VPN switch's IP address or what you configure in the **Secure Gateway Address** field below.	

ID Type and Content Examples

Two VPN switches must have matching ID type and content configuration in order to set up a VPN tunnel.

The two Contivity 221s in this example can complete negotiation and establish a VPN tunnel.

Table 51 Matching ID Type and Content Configuration Example

Contivity 221 A	**Contivity 221 B**
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two Contivity 221s in this example cannot complete their negotiation because Contivity 221 B's **Local ID type** is **IP**, but Contivity 221 A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 52 Mismatching ID Type and Content Configuration Example

Contivity 221 A	**Contivity 221 B**
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see page 237 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

Configuring Contivity Client VPN Rule Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. If the **Branch Office** screen is displayed, select **Contivity Client** from the **Connection Type** list box. The **VPN Contivity Client Rule Setup** screen is shown next.

Figure 69 VPN Contivity Client Rule Setup



Table 53 VPN Contivity Client Rule Setup

Label	Description
Connection Type	Select **Branch Office** to manually configure a VPN rule. Select **Contivity Client** to use a simple VPN rule that lets you define and store connection information for accessing your corporate network through a Contivity VPN switch. You can only have one Contivity Client rule.
Active	Select this check box to turn on this rule. Clear this check box if you do not want to use this rule after you apply it. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive.
Keep Alive	Select this check box to turn on the Keep Alive feature for this SA. Turn on Keep Alive to have the Contivity 221 automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote VPN switch must also have keep alive enabled in order for this feature to work.
Description	Enter a brief description about this rule for identification purposes.

Table 53 VPN Contivity Client Rule Setup

Label	Description
Destination	This field specifies the IP address or the domain name (up to 31 case-sensitive characters) of the remote Contivity VPN switch. You can use alphanumeric characters, the underscore, dash, period and the "@" symbol in a domain name. No spaces are allowed.
User Name	Enter the user name exactly as the Contivity VPN switch administrator gives you.
Password	Enter the password exactly as the Contivity VPN switch administrator gives you.
Advanced	Click **Advanced** to configure group authentication and on demand client tunnel settings.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Cancel	Click **Cancel** to return to the **VPN Summary** screen without saving your changes.

Configuring Advanced Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. If the **Branch Office** screen is displayed, select **Contivity Client** from the **Connection Type** list box. Click **Advanced** to display the **VPN Contivity Client Advanced Rule Setup** screen as shown next.

Figure 70 VPN Contivity Client Advanced Rule Setup



The following table describes the fields in this screen.

Table 54 VPN Contivity Client Advanced Rule Setup

Label	Description
Group Authentication	Enable **Group Authentication** to have the Contivity 221 send a **Group ID** and **Group Password** to the remote Contivity VPN switch for initial authentication. After a successful initial authentication, a RADIUS server associated with the remote Contivity VPN switch uses the **User Name** and **Password** to authenticate the Contivity 221. You must also configure the **Group ID** and **Group Password** fields when you enable **Group Authentication**. When **Group Authentication** is not enabled, the remote Contivity VPN switch uses the **User Name** and **Password** to authenticate the Contivity 221.
Group ID	Enter the group ID exactly as the Contivity VPN switch administrator gives you. This field only applies when you enable **Group Authentication**.
Group Password	Enter the group password exactly as the Contivity VPN switch administrator gives you. This field only applies when you enable **Group Authentication**.

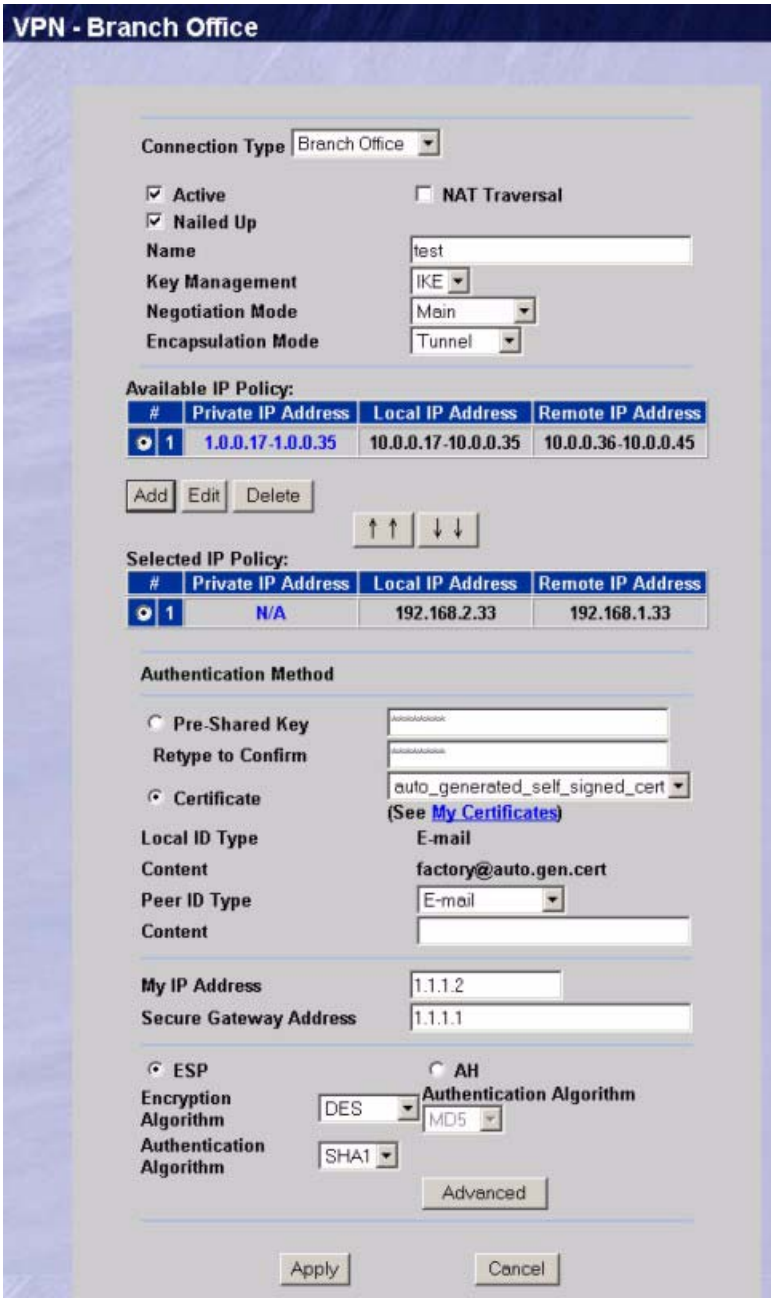
Table 54 VPN Contivity Client Advanced Rule Setup

Label	Description
On Demand Client Tunnel	Select this check box to have any outgoing packets automatically trigger a VPN connection to the remote Contivity VPN switch. When **On Demand Client Tunnel** is not enabled, you need to go to the **VPN Summary** screen and click the **Connect** button to create a VPN connection to the remote Contivity VPN switch.
Apply	Click **Apply** to temporarily save the settings and return to the **VPN - Contivity Client** screen. The **Group Authentication** settings will be saved if you click **Apply** in the **VPN - Contivity Client** screen.
Cancel	Click **Cancel** to return to the **VPN Contivity Client Rule Setup** screen without saving your changes.

Configuring Branch Office VPN Rule Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. The **VPN Branch Office Rule Setup** screen is shown next.

Figure 71 VPN Branch Office Rule Setup



The following table describes the fields in this screen.

Table 55 VPN Branch Office Rule Setup

Label	Description
Connection Type	Select **Branch Office** to manually configure a VPN rule. Select **Contivity Client** to use a simple VPN rule that lets you define and store connection information for accessing your corporate network through a Contivity VPN switch. You can only have one Contivity client rule. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive.
Active	Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied.
Nailed Up	Select this check box to turn on the nailed up feature for this SA. Turn on nailed up to have the Contivity 221 automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The Contivity 221 also reinitiates the SA when it restarts.
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two VPN switches. The remote VPN switch must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol. In order for a VPN switch behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the VPN switch behind the NAT router.
Name	Type a name to identify this VPN policy. You may use any character, including spaces, but the Contivity 221 drops trailing spaces.
Key Management	Your Contivity 221 uses IKE (ISAKMP) key management in order to set up a VPN.
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a VPN switch must have the same negotiation mode.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.

Table 55 VPN Branch Office Rule Setup

Label	Description
Available/ Selected IP Policy	The **Available IP Policy** table displays network routes. Use the **Add**, **Edit** and **Delete** buttons to configure this list. Move the network routes that you want to use the VPN tunnel down into the **Selected IP Policy** table. Select a network route's radio button in the **Available IP Policy** table, then click the down arrows to move it into the **Selected IP Policy** table. To remove a network route from the **Selected IP Policy** table, select its radio button in the **Selected IP Policy** table and click the up arrows. A network route that is already selected for a VPN tunnel does not display in the **Available IP Policy** table.
Go to Page	This displays when the total number of the VPN rules' IP policies is more than ten. There can be a total of five VPN rules. The VPN rules can have a combined total of total of 60 IP policies. Each page can display up to ten IP policies. Therefore, it may take more than one page to display one VPN rule's IP policies. Select another page number from this **Go to Page** drop-down list box to view more IP policies.
Private IP Address	This field displays the IP address of the computer (or a range of computers) on your Contivity 221's local network, for which you have configured this VPN rule. This field applies when you configure the IP policy to use a branch tunnel NAT address-mapping rule in the **IP Policy** screen. This field displays a single (static) IP address when the IP policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **One-to-One** in the **IP Policy** screen. This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **Many-to-One** or **Many One-to-one** in the **IP Policy** screen.

Table 55 VPN Branch Office Rule Setup

Label	Description
Local IP Address	This field displays the IP address (or range of IP addresses) of the computer (or computers) on your Contivity 221's local network, for which you have configured this IP policy. This field displays the IP policy's virtual IP address (or range of addresses) when you enable branch tunnel NAT address mapping in the **IP Policy** screen. This field displays a single (static) IP address when the IP policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **One-to-one** or **Many-to-One** in the **IP Policy** screen. This field displays the beginning and ending (static) IP addresses of a range of computers when the policy's **Branch Tunnel NAT Address Mapping Rule Type** field is configured to **Many One-to-one** in the **IP Policy** screen. This field displays the policy's local IP address (or range of addresses) when you disable branch tunnel NAT address mapping in the **IP Policy** screen. This field displays a single (static) IP address when the IP policy's **Local Address Type** field is configured to **Single Address** in the **IP Policy** screen. This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's **Local Address Type** field is configured to **Range Address** in the **IP Policy** screen. This field displays a (static) IP address and a subnet mask when the IP policy's **Local Address Type** field is configured to **Subnet Address** in the **IP Policy** screen.

Table 55 VPN Branch Office Rule Setup

Label	Description
Remote IP Address	This field displays the IP address(es) of computer(s) on the remote network behind the remote VPN switch. This field displays a single (static) IP address when the IP policy's **Remote Address Type** field is configured to **Single Address** in the **IP Policy** screen. This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's **Remote Address Type** field is configured to **Range Address** in the **IP Policy** screen. This field displays a (static) IP address and a subnet mask when the IP policy's **Remote Address Type** field is configured to **Subnet Address** in the **IP Policy** screen. This field displays **ALL** whenever the **Secure Gateway Address** field is set to **0.0.0.0**. This field also displays **ALL** whenever the IP policy's **Remote Starting IP Address** field is set to **0.0.0.0** in the **IP Policy** screen. When **ALL** displays, only the remote VPN switch can initiate the VPN.
Add	Select **Add** to open a screen where you can configure an IP policy.
Edit	Select the radio button next to an IP policy and then click **Edit** to edit that IP policy.
Delete	Select the radio button next to an IP policy that you want to remove and then click **Delete**.
Authentication Method	Select the **Pre-Shared Key** radio button to use a pre-shared secret key to identify the Contivity 221. Select the **Certificate** radio button to identify the Contivity 221 by a certificate.
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 32 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a “PYLD_MALFORMED” (payload malformed) packet if the same pre-shared key is not used on both ends.

Table 55 VPN Branch Office Rule Setup

Label	Description
Retype to Confirm	Type your pre-shared key again in this field.
Certificate	Use the drop-down list box to select the certificate to use for this VPN tunnel. You must have certificates already configured in the **My Certificates** screen. Click **My Certificates** to go to the **My Certificates** screen where you can view the Contivity 221's list of certificates.
Local ID Type	Select **IP** to identify this Contivity 221 by its IP address. Select **DNS** to identify this Contivity 221 by a domain name. Select **E-mail** to identify this Contivity 221 by an e-mail address.
Local Content	When you select **IP** in the **Local ID Type** field, type an IP address or leave the field blank to have the Contivity 221 automatically use its own IP address. When you select **DNS** in the **Local ID Type** field, type a domain name (up to 31 characters) by which to identify this Contivity 221. When you select **E-mail** in the **Local ID Type** field, type an e-mail address (up to 31 characters) by which to identify this Contivity 221. The IP address, domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.
Peer ID Type	Select **IP** to identify the remote VPN switch by its IP address. Select **DNS** to identify the remote VPN switch by a domain name. Select **E-mail** to identify the remote VPN switch by an e-mail address.
Peer Content	When you select **IP** in the **Peer ID Type** field, type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Contivity 221 automatically use the address in the **Secure Gateway Address** field. When you select **DNS** in the **Peer ID Type** field, type a domain name (up to 31 characters) by which to identify the remote VPN switch. When you select **E-mail** in the **Peer ID Type** field, type an e-mail address (up to 31 characters) by which to identify the remote VPN switch. The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Address** field. Regardless of how you configure the **ID Type** and **Content** fields, two active SAs cannot have both the local and remote IP address ranges overlap between rules.

Table 55 VPN Branch Office Rule Setup

Label	Description
My IP Address	Enter the WAN IP address of your Contivity 221. The VPN tunnel has to be rebuilt if this IP address changes. The following applies if this field is configured as **0.0.0.0**: • The Contivity 221 uses the current Contivity 221 WAN IP address (static or dynamic) to set up the VPN tunnel. • If the WAN connection goes down, the Contivity 221 uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.
Secure Gateway Address	Type the WAN IP address or the domain name (up to 31 characters) of the VPN switch with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote VPN switch has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**). The remote address fields do not apply when the **Secure Gateway Address** field is configured to **0.0.0.0**. In this case only the remote VPN switch can initiate the VPN. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
ESP	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as the services offered by AH. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next).
AH	Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field.

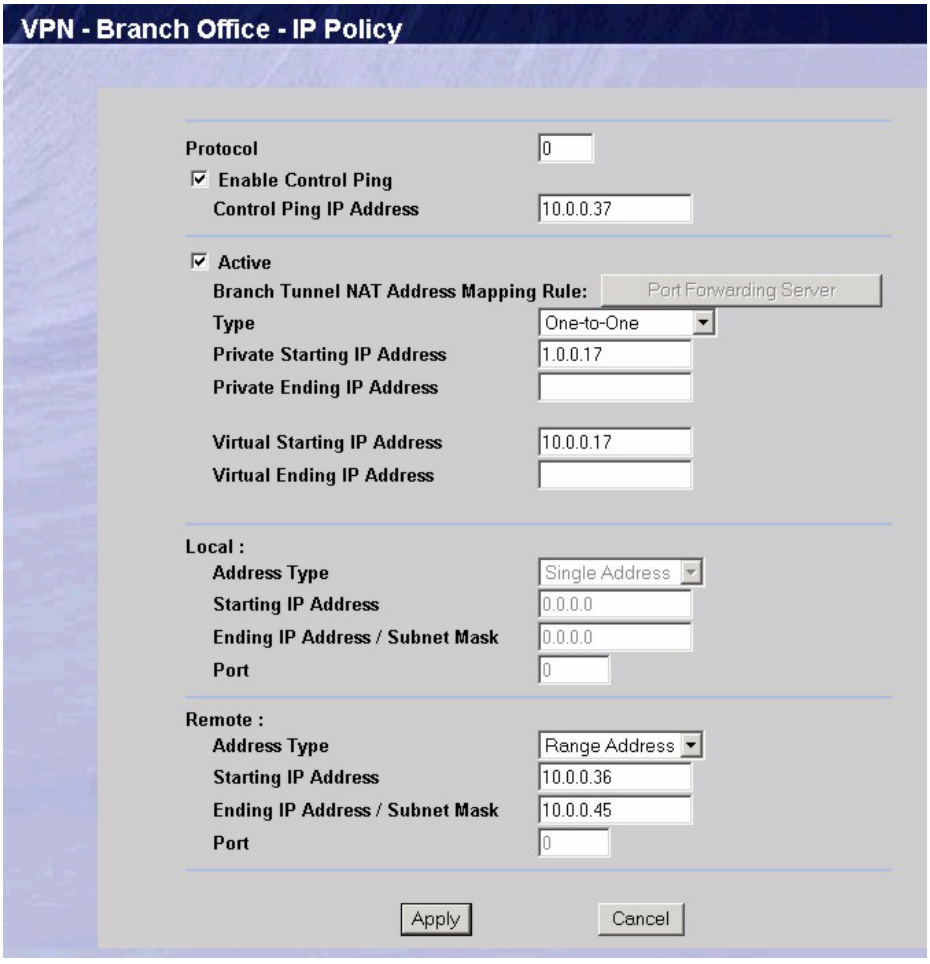
Table 55 VPN Branch Office Rule Setup

Label	Description
Encryption Algorithm	Select **DES**, **3DES**, **AES 128**, **AES 192**, **AES 256** or **NULL** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit, 192-bit, or 256-bit key with this implementation of **AES**. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Apply	Click **Apply** to save your changes back to the Contivity 221
Cancel	Click **Cancel** to return to the **VPN Summary** screen without saving your changes.

Configuring an IP Policy

Select one of the IP policies in the **VPN Branch Office** screen and click **Add** or **Edit** to configure the policy's settings. The **Branch Office – IP Policy** setup screen is shown next.

Figure 72 VPN Branch Office - IP Policy



The following table describes the fields in this screen.

Table 56 VPN Branch Office - IP Policy

Label	Description
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Enable Control Ping	Select the check box and configure an IP address in the **Control Ping IP Address** field to have the Contivity 221 periodically test the VPN tunnel to the branch office. The Contivity 221 pings the IP address every minute. The Contivity 221 starts the IPSec connection idle timeout timer when it sends the ping packet. If there is no traffic from the remote Contivity VPN switch by the time the timeout period expires, the Contivity 221 disconnects the VPN tunnel.
Control Ping IP Address	If you select **Enable Control Ping**, enter the IP address of a computer at the branch office. The computer's IP address must be in this IP policy's remote range (see the **Remote** fields).
Branch Tunnel NAT Address Mapping Rule	
Port Forwarding Server	Click **Port Forwarding Server** to configure a list of inside (behind NAT on the LAN) servers, for example, web or FTP. The Contivity 221 makes these servers visible to the devices using the VPN branch NAT tunnel (from behind the remote Contivity VPN switch) even though NAT makes your inside network appear as a single machine. This option applies when the **Type** field is configured to **Many-to-One**.
Active	Enable this feature to have the Contivity 221 use a different (virtual) IP address for the VPN connection. When you enable branch tunnel NAT address mapping, you do not configure the local section.
Type	Select one of the following port mapping types. 1. **One-to-One**: One-to-one mode maps one private IP address to one virtual IP address. Port numbers do not change with one-to-one NAT mapping. 2. **Many-to-One**: Many-to-One mode maps multiple private IP addresses to one virtual IP address. This is equivalent to SUA (i.e., PAT, port address translation), Contivity 221's Single User Account feature. 3. **Many One-to-one**: Many One-to-one mode maps each private IP address to a unique virtual IP address. Port numbers do not change with many one-to-one NAT mapping.

Table 56 VPN Branch Office - IP Policy

Label	Description
Private Starting IP Address	When the **Type** field is configured to **One-to-one**, enter the (static) IP address of the computer on your Contivity 221's LAN that is to use the VPN tunnel. When the **Type** field is configured to **Many-to-One** or **Many One-to-one**, enter the beginning (static) IP address of the range of computers on your Contivity 221's LAN that are to use the VPN tunnel.
Private Ending IP Address	When the **Type** field is configured to **One-to-one**, this field is N/A. When the **Type** field is configured to **Many-to-One** or **Many One-to-one**, enter the ending (static) IP address of the range of computers on your Contivity 221's LAN that are to use the VPN tunnel.
Virtual Starting IP Address	Virtual addresses must be static and correspond to the remote VPN switch's configured remote IP addresses. The computers on the Contivity 221's LAN and the remote network can function as if they were on the same subnet when the virtual IP address(es) is on the same subnet as the remote IP address(es). Two active SAs can have the same virtual or remote IP address, but not both. You can configure multiple SAs between the same virtual and remote IP addresses, as long as only one is active at any time. When the **Type** field is configured to **One-to-one** or **Many-to-One**, enter the (static) IP address that you want to use for the VPN tunnel. When the **Type** field is configured to **Many One-to-one**, enter the beginning (static) IP address of the range of IP addresses that you want to use for the VPN tunnel.
Virtual Ending IP Address	When the **Type** field is configured to **One-to-one** or **Many-to-One**, this field is N/A. When the **Type** field is configured to **Many One-to-one**, enter the ending (static) IP address of the range of IP addresses that you want to use for the VPN tunnel.

Table 56 VPN Branch Office - IP Policy

Label	Description
Local	Local IP addresses must be static and correspond to the remote VPN switch's configured remote IP addresses. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. Two IP policies can have the same local or remote IP address, but not both. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Address Type	Use the drop-down menu to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your Contivity 221. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on your LAN behind your Contivity 221. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your Contivity 221.
Ending IP Address / Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your Contivity 221. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your Contivity 221.
Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3

Table 56 VPN Branch Office - IP Policy

Label	Description
Remote	Remote IP addresses must be static and correspond to the remote VPN switch's configured local IP addresses. The remote fields do not apply when the **Secure Gateway Address** field is configured to **0.0.0.0**. In this case only the remote VPN switch can initiate the VPN. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. Two IP policies can have the same local or remote IP address, but not both.
Address Type	Use the drop-down menu to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your Contivity 221. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on your LAN behind your Contivity 221. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your Contivity 221.
Ending IP Address / Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your Contivity 221. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your Contivity 221.
Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return to the **VPN Branch Office** screen without saving your changes.

Port Forwarding Server

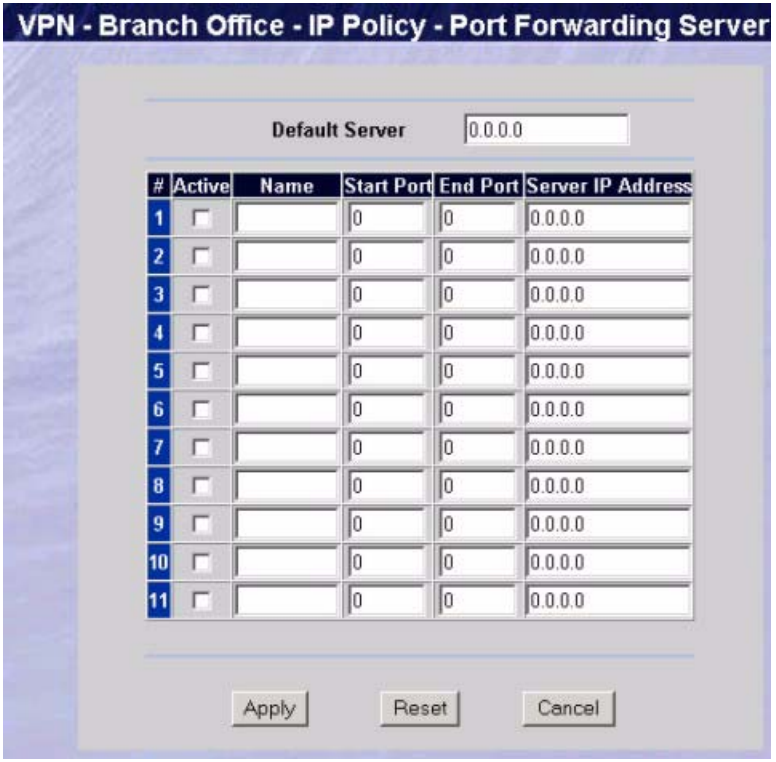
A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the devices using the VPN branch NAT tunnel (from behind the remote Contivity VPN switch) even though NAT makes your inside network appear as a single machine. The servers must be using the VPN branch NAT tunnel (from behind the Contivity 221).

You may enter a single port or a range of ports to be forwarded and then the local IP address of the desired inside server(s).

Configuring a Port Forwarding Server

Select one of the IP Policies in the **VPN Branch Office** screen and click **Edit** to display the **Branch Office – IP Policy** setup screen. Then click the **Port Forwarding Server** button to display the screen shown next.

Figure 73 VPN Branch Office - IP Policy - Port Forwarding Server



The following table describes the fields in this screen.

Table 57 VPN Branch Office - IP Policy - Port Forwarding Server

Label	Description
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen will be discarded.
#	Number of an individual port forwarding server entry.
Active	Select this check box to activate the port forwarding server entry.
Name	Enter a descriptive name for identifying purposes.

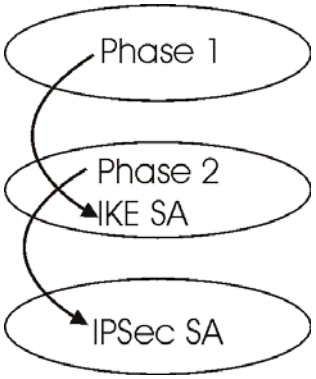
Table 57 VPN Branch Office - IP Policy - Port Forwarding Server

Label	Description
Start Port	Type a port number in this field. To forward only one port, type the port number again in the **End Port** field. To forward a series of ports, type the start port number here and the end port number in the **End Port** field.
End Port	Type a port number in this field. To forward only one port, type the port number in the **Start Port** field above and then type it again in this field. To forward a series of ports, type the last port number in a series that begins with the port number in the **Start Port** field above.
Server IP Address	Type your server IP address in this field.
Apply	Click this button to save these settings and return to the **VPN Branch Office - IP Policy** screen.
Reset	Click this button to begin configuring this screen afresh.
Cancel	Click this button to return to the **VPN Branch Office - IP Policy** screen without saving your changes.

IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 74 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see *section Perfect Forward Secrecy (PFS)*. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.

- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The Contivity 221 automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The Contivity 221 also automatically renegotiates the IPSec SA if both VPN switches have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the VPN switch must renegotiate the SA the next time someone attempts to send traffic.

Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

Main Mode ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).

Aggressive Mode is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection.

Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

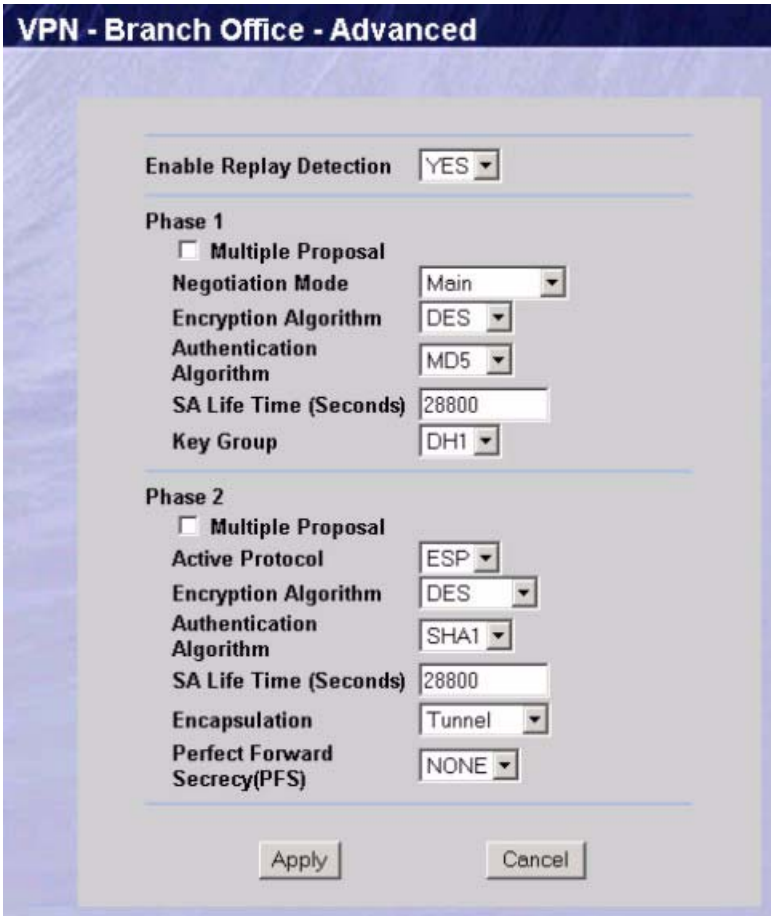
This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the Contivity 221. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

Configuring Advanced Branch Office Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. The basic IKE rule setup screen opens

In the **VPN Branch Office Rule Setup** screen, click the **Advanced** button to display the **VPN Branch Office Advanced Rule Setup** screen.

Figure 75 VPN Branch Office Advanced Rule Setup



The following table describes the fields in this screen.

Table 58 VPN Branch Office Advanced Rule Setup

Label	Description
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to **YES**.
Phase 1	A phase 1 exchange establishes an IKE SA (Security Association).

Table 58 VPN Branch Office Advanced Rule Setup

Label	Description
Multiple Proposal	Select this check box to allow the Contivity 221 to use any of its phase 1 encryption and authentication algorithms when negotiating an IKE SA. Clear this check box to have the Contivity 221 use only the phase 1 encryption and authentication algorithms configured below when negotiating an IKE SA.
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. The Contivity 221's negotiation mode should be identical to that on the remote VPN switch.
Encryption Algorithm	Select **DES**, **3DES** or **AES** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit, 192-bit, or 256-bit key with this implementation of **AES**. **AES** is faster than **3DES**.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. The Contivity 221's authentication algorithm should be identical to the remote VPN switch. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate the source and integrity of packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select **SHA-1** for maximum security.
SA Life Time	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA life time increases security by forcing the two VPN switches to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	A phase 2 exchange uses the IKE SA established in phase 1 to negotiate the SA for IPSec.
Multiple Proposal	Select this check box to allow the Contivity 221 to use any of its phase 2 encryption and authentication algorithms when negotiating an IPSec SA. Clear this check box to have the Contivity 221 use only the phase 2 encryption and authentication algorithms configured below when negotiating an IPSec SA.

Table 58 VPN Branch Office Advanced Rule Setup

Label	Description
Active Protocol	Select **ESP** or **AH** from the drop-down list box. The Contivity 221's IPSec Protocol should be identical to the remote VPN switch. The ESP (Encapsulation Security Payload) protocol (RFC 2406) provides encryption as well as the authentication offered by AH. If you select **ESP** here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described below). The AH protocol (Authentication Header Protocol) (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field.
Encryption Algorithm	Select **DES**, **3DES**, **AES** or **NULL** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit, 192-bit, or 256-bit key with this implementation of **AES**. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select MD5 for minimal security and SHA-1 for maximum security.
SA Life Time	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA life time increases security by forcing the two VPN switches to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Encapsulation	Select **Tunnel** mode or **Transport** mode from the drop down list-box. The Contivity 221's encapsulation mode should be identical to the remote VPN switch.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (None) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose from **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1, a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2, a 1024 bit (1Kb) random number (more secure, yet slower).

Table 58 VPN Branch Office Advanced Rule Setup

Label	Description
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return to the **VPN Branch Office** screen without saving your changes.

SA Monitor

In the WebGUI, click **VPN** and the **SA Monitor** tab. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.



Note: When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See the section on keep alive to have the Contivity 221 renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 76 VPN SA Monitor



The following table describes the fields in this screen.

Table 59 VPN SA Monitor

Label	Description
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Local IP Address	This field displays the IP address of the computer using the VPN IPSec feature of your Contivity 221.
Remote IP Address	This field displays IP address (in a range) of computers on the remote network behind the remote VPN switch.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase Contivity 221 processing requirements and communications latency (delay).
Refresh	Click **Refresh** to display the current active VPN connection(s). This button is available when you have active VPN connections.
Disconnect	Select a security association index number that you want to disconnect and then click **Disconnect**. This button is available when you have active VPN connections.
Next Page (if applicable)	Click **Next Page** to view more items in the summary (if you have a summary list that exceeds this page)

Global Settings

In the WebGUI, click **VPN** on the navigation panel and the **Global Setting** tab.

Figure 77 VPN Global Setting

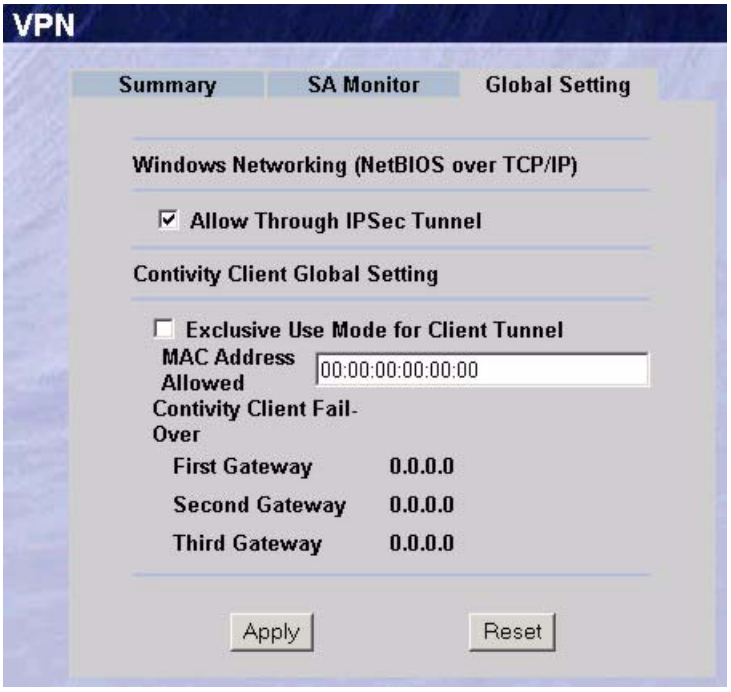


Table 60 VPN Global Setting

Label	Description
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow Through IPSec Tunnel	Select this check box to send NetBIOS packets through the VPN connection.

Table 60 VPN Global Setting

Label	Description
Exclusive Use Mode for Client Tunnel	Select this check box to permit only the computer with the MAC address that you specify to set up a VPN connection to the remote Contivity VPN switch.
MAC Address Allowed	Enter the MAC address of the computer you want to allow to use the VPN tunnel.
Contivity Client Fail-Over	The Contivity Client fail-over feature allows a Contivity client to establish a VPN connection to a backup Contivity VPN switch when the default remote Contivity VPN switch (specified in the Destination field) is not accessible. The VPN fail-over feature must also be set up in the remote Contivity VPN switch.
First Gateway Second Gateway Third Gateway	These read-only fields display the IP addresses of the backup Contivity VPN switches. The Contivity 221 automatically gets this information from the default remote Contivity VPN switch. When the remote Contivity VPN switch is unreachable or fails to respond to IKE negotiation, the Contivity 221 tries to establish a VPN connection to a backup Contivity VPN switch.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 14
Certificates

This chapter gives background information about public-key certificates and explains how to use them.

Certificates Overview

The Contivity 221 can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the Contivity 221 to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The Contivity 221 uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The Contivity 221 does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The Contivity 221 can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The Contivity 221 only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

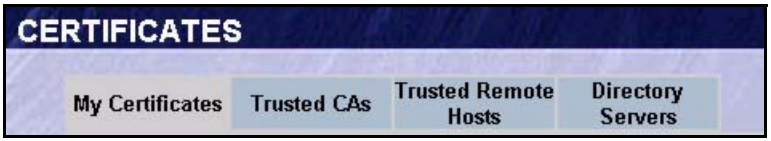
Self-signed Certificates

Until public-key infrastructure becomes more mature, it may not be available in some areas. You can have the Contivity 221 act as a certification authority and sign its own certificates.

Configuration Summary

This section summarizes how to manage certificates on the Contivity 221.

Figure 78 Certificate Configuration Overview



Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the Contivity 221s' CA-signed certificates.

Use the **Trusted CA** screens to save CA certificates to the Contivity 221.

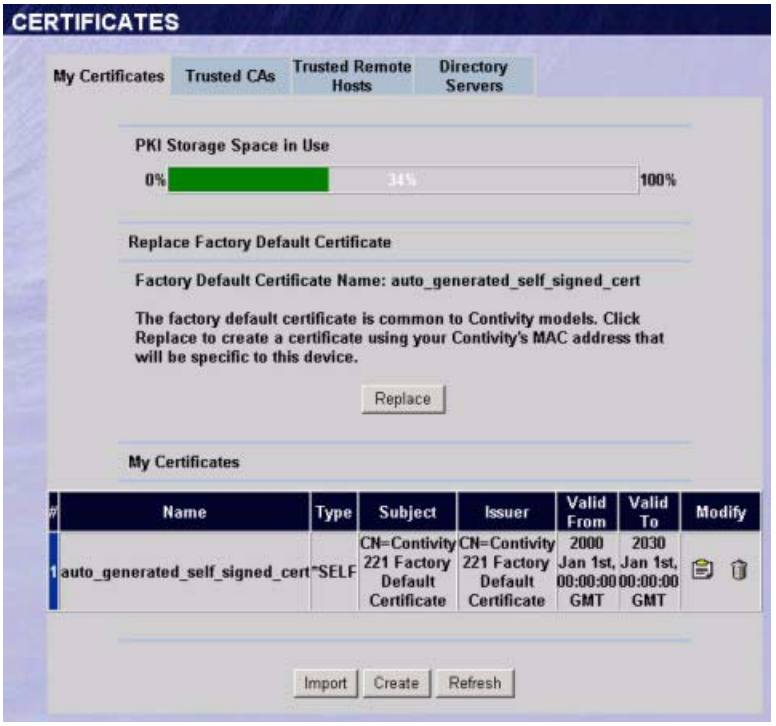
Use the **Trusted Remote Hosts** screens to import self-signed certificates.

Use the **Directory Servers** screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

My Certificates

Click **CERTIFICATES**, **My Certificates** to open the Contivity 221's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. See the following figure.

Figure 79 My Certificates



The following table describes the labels in this screen.

Table 61 My Certificates

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the Contivity 221's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the Contivity 221 has the factory default certificate. The factory default certificate is common to all Contivity 221s that use certificates. It is recommended that you use this button to replace the factory default certificate with one that uses your Contivity 221's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.

Table 61 My Certificates

Label	Description
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the Contivity 221 uses to sign imported trusted remote host certificates. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

Table 61 My Certificates

Label	Description
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. You cannot delete a certificate that one or more features is configured to use. Do the following to delete a certificate that shows ***SELF** in the **Type** field. 1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the ***SELF** certificate. 2. Click the details icon next to another self-signed certificate (see the description on the **Create** button if you need to create a self-signed certificate). 3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box. 4. Click **Apply** to save the changes and return to the **My Certificates** screen. 5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now. Note that subsequent certificates move up by one when you take this action
Import	Click **Import** to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the Contivity 221.
Create	Click **Create** to go to the screen where you can have the Contivity 221 generate a certificate or a certification request.
Refresh	Click **Refresh** to display the current validity status of the certificates.

Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The Contivity 221 currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

Importing a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the Contivity 221, see the following figure.

Note: 1. You can only import a certificate that matches a corresponding certification request that was generated by the Contivity 221.
2. The certificate you import replaces the corresponding request in the My Certificates screen.
3. You must remove any spaces from the certificate's filename before you can import it.

Figure 80 My Certificate Import



The following table describes the labels in this screen.

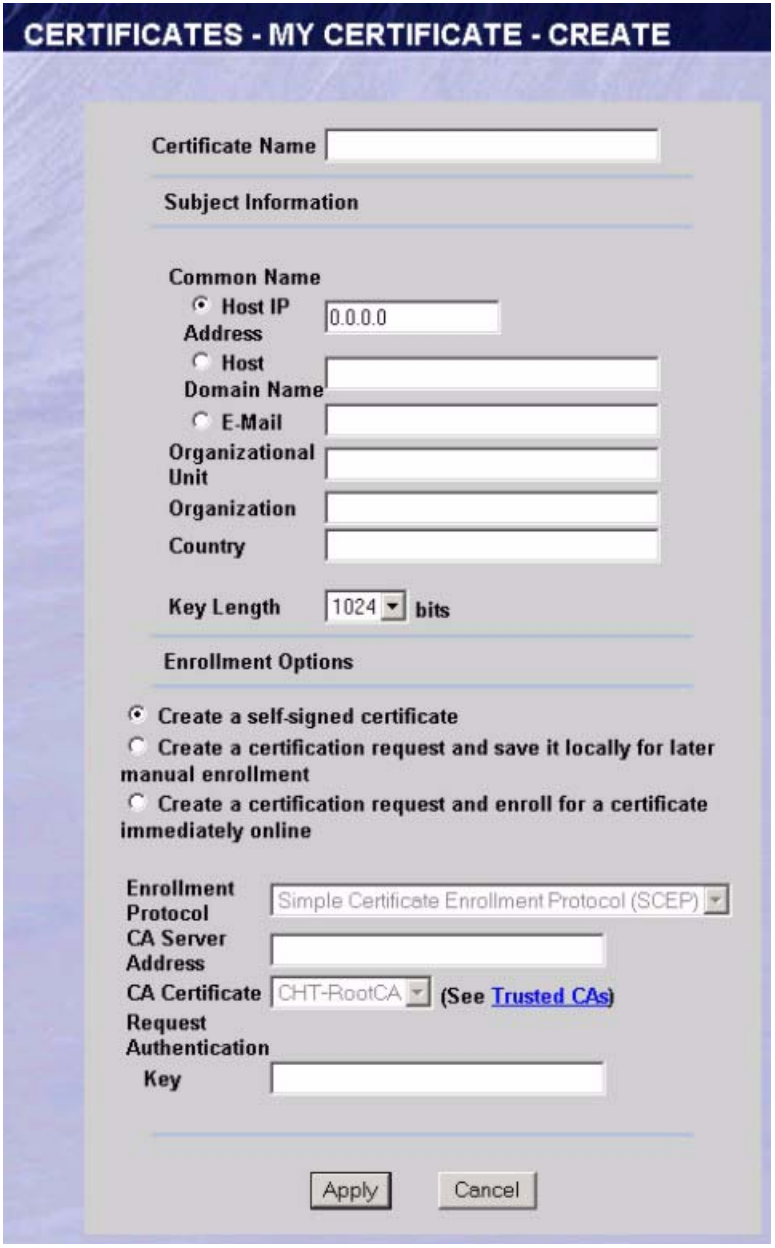
Table 62 My Certificate Import

Label	Description
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the Contivity 221.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

Creating a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Create** to open the **My Certificate Create** screen. Use this screen to have the Contivity 221 create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request, see the following figure.

Figure 81 My Certificate Create



The following table describes the labels in this screen.

Table 63 My Certificate Create

Label	Description
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the **Common Name** is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the Contivity 221 drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the Contivity 221 drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the Contivity 221 drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select **Create a self-signed certificate** to have the Contivity 221 generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.

Table 63 My Certificate Create

Label	Description
Create a certification request and save it locally for later manual enrollment	Select **Create a certification request and save it locally for later manual enrollment** to have the Contivity 221 generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see the My Certificate Details section) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select **Create a certification request and enroll for a certificate immediately online** to have the Contivity 221 generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the Contivity 221's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SECP enrollment protocol.
Key	Type the key that the certification authority gave you.

Table 63 My Certificate Create

Label	Description
Apply	Click **Apply** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the Contivity 221 is generating the self-signed certificate or certification request.

After the Contivity 221 successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the Contivity 221 enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the Contivity 221 to enroll a certificate online.

My Certificate Details

Click **CERTIFICATES**, and then **My Certificates** to open the **My Certificates** screen (see Figure 79). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the Contivity 221 uses to sign the trusted remote host certificates that you import to the Contivity 221.

Figure 82 My Certificate Details



The following table describes the labels in this screen.

Table 64 My Certificate Details

Label	Description
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the Contivity 221 use this certificate to sign the trusted remote host certificates that you import to the Contivity 221. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.
Certification Path	Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The Contivity 221 does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the Contivity 221.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).

Table 64 My Certificate Details

Label	Description
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The Contivity 221 uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Contivity 221 uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the Contivity 221 calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the Contivity 221 calculated using the SHA1 algorithm.

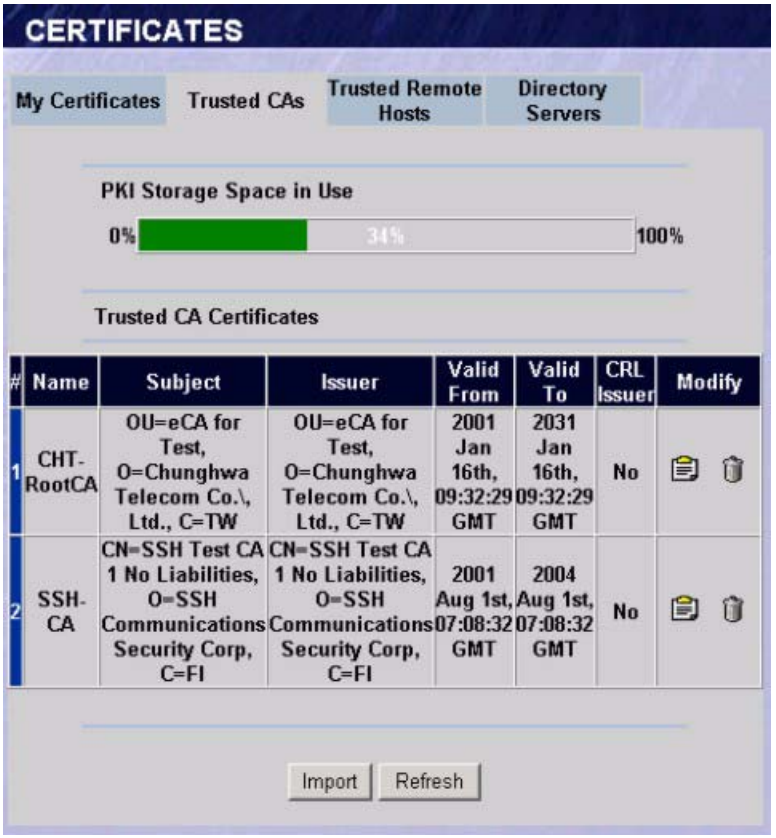
Table 64 My Certificate Details

Label	Description
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes back to the Contivity 221. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

Trusted CAs

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the Contivity 221 to accept as trusted. The Contivity 221 accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities. See the following figure.

Figure 83 Trusted CAs



The following table describes the labels in this screen.

Table 65 Trusted CAs

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the Contivity 221's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.

Table 65 Trusted CAs

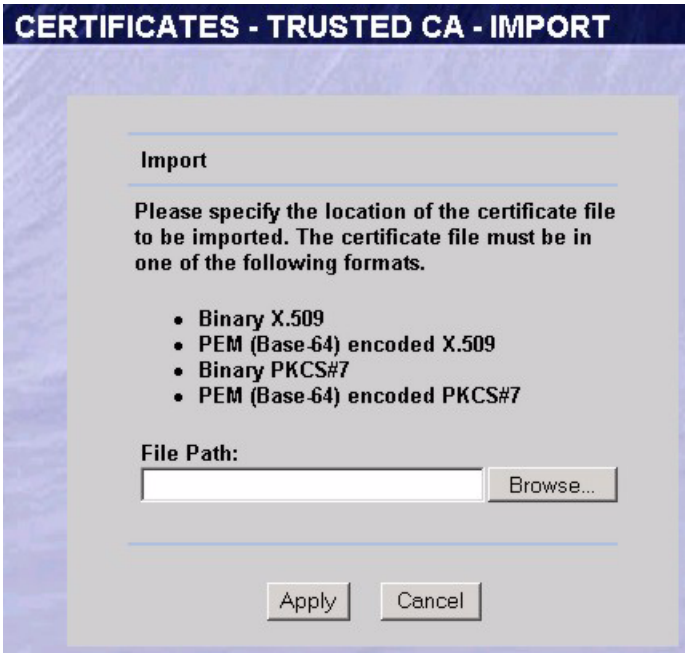
Label	Description
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the **Issues certificate revocation lists (CRL)** check box in the certificate's details screen to have the Contivity 221 check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the Contivity 221.
Refresh	Click this button to display the current validity status of the certificates.

Importing a Trusted CA's Certificate

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the Contivity 221, see the following figure.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 84 Trusted CA Import



The following table describes the labels in this screen.

Table 66 Trusted CA Import

Label	Description
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.

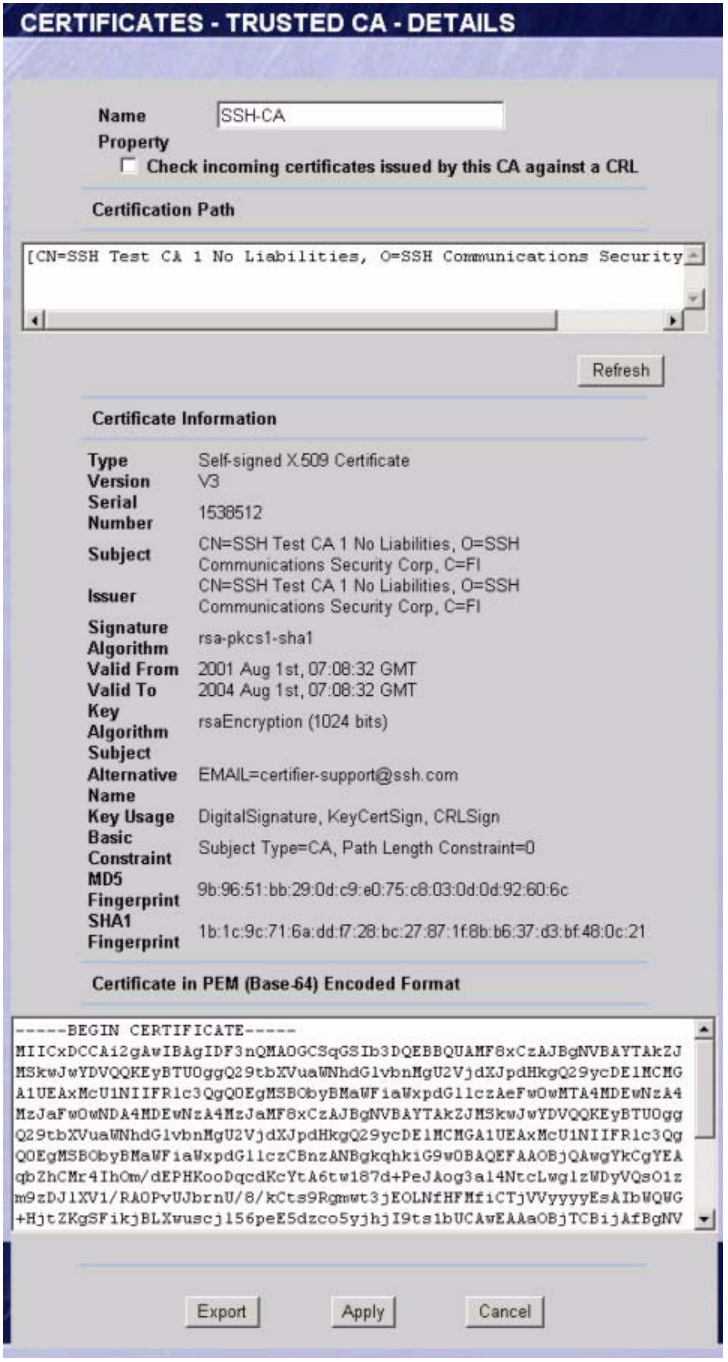
Table 66 Trusted CA Import

Label	Description
Apply	Click **Apply** to save the certificate on the Contivity 221.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

Trusted CA Certificate Details

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the Contivity 221 to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 85 Trusted CA Details



The following table describes the labels in this screen.

Table 67 Trusted CA Details

Label	Description
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Check incoming certificates issued by this CA against a CRL	Select this check box to have the Contivity 221 check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the Contivity 221 not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The Contivity 221 does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.

Table 67 Trusted CA Details

Label	Description
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Contivity 221 uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the Contivity 221 calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the Contivity 221 calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.

Table 67 Trusted CA Details

Label	Description
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes back to the Contivity 221. You can only change the name and/or set whether or not you want the Contivity 221 to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

Trusted Remote Hosts

Click **CERTIFICATES**, **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen (see the following figure). This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the Contivity 221 automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

Figure 86 Trusted Remote Hosts



The following table describes the labels in this screen.

Table 68 Trusted Remote Hosts

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the Contivity 221's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Issuer (My Default Self-signed Certificate)	This field displays identifying information about the default self-signed certificate on the Contivity 221 that the Contivity 221 uses to sign the trusted remote host certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.

Table 68 Trusted Remote Hosts

Label	Description
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Import	Click **Import** to open a screen where you can save the certificate of a remote host (which you trust) from your computer to the Contivity 221.
Refresh	Click this button to display the current validity status of the certificates.

Verifying a Trusted Remote Host's Certificate

Certificates issued by certification authorities have the certification authority's signature for you to check. Self-signed certificates only have the signature of the host itself. This means that you must be very careful when deciding to import (and thereby trust) a remote host's self-signed certificate.

Trusted Remote Host Certificate Fingerprints

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to use a certificate's fingerprint to verify that you have the remote host's actual certificate.

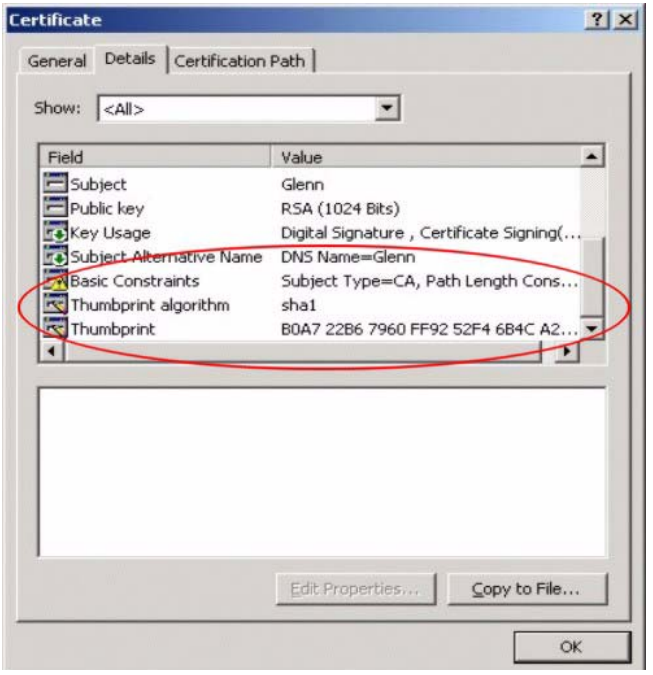
1. Browse to where you have the remote host's certificate saved on your computer.
2. Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 87 Remote Host Certificates



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 88 Certificate Details



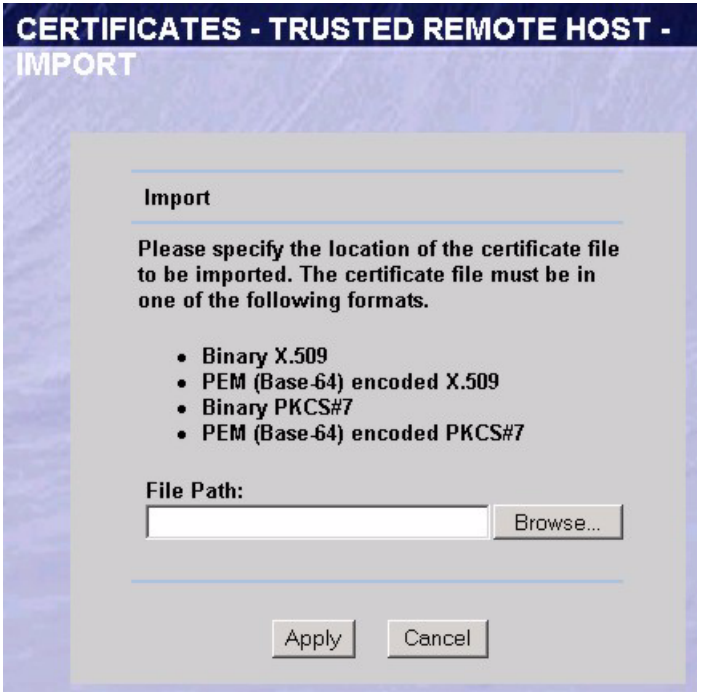
Verify (over the phone for example) that the remote host has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields.

Importing a Trusted Remote Host's Certificate

Click **CERTIFICATES**, **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen. Follow the instructions in this screen to save a trusted host's certificate to the Contivity 221, see the following figure.

Note: The trusted remote host certificate must be a self-signed certificate; and you must remove any spaces from its filename before you can import it.

Figure 89 Trusted Remote Host Import



The following table describes the labels in this screen.

Table 69 Trusted Remote Host Import

Label	Description
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the Contivity 221.
Cancel	Click **Cancel** to quit and return to the **Trusted Remote Hosts** screen.

Trusted Remote Host Certificate Details

Click **CERTIFICATES**, **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen. You can use this screen to view in-depth information about the trusted remote host's certificate and/or change the certificate's name.

Figure 90 Trusted Remote Host Details



The following table describes the labels in this screen.

Table 70 Trusted Remote Host Details

Label	Description
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a certificate's issuing certification authority. For a trusted host, the list consists of the end entity's own certificate and the default self-signed certificate that the Contivity 221 uses to sign remote host certificates.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The Contivity 221 is the Certification Authority that signed the certificate. X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the device that created the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the default self-signed certificate on the Contivity 221 that the Contivity 221 uses to sign the trusted remote host certificates.
Signature Algorithm	This field displays the type of algorithm that the Contivity 221 used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Contivity 221 uses RSA encryption) and the length of the key set in bits (1024 bits for example).

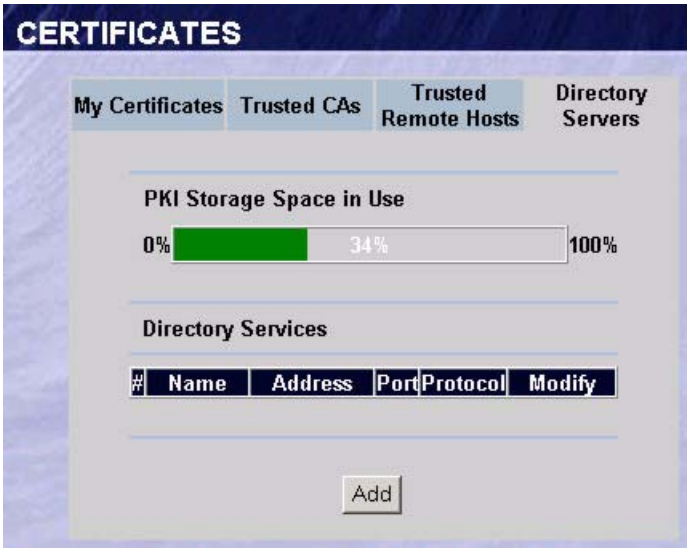
Table 70 Trusted Remote Host Details

Label	Description
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the Contivity 221 calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the Contivity 221 has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See the Verifying a Trusted Remote Host's Certificate section for how to verify a remote host's certificate.
SHA1 Fingerprint	This is the certificate's message digest that the Contivity 221 calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the Contivity 221 has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See the Verifying a Trusted Remote Host's Certificate section for how to verify a remote host's certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes back to the Contivity 221. You can only change the name of the certificate.
Cancel	Click **Cancel** to quit configuring this screen and return to the **Trusted Remote Hosts** screen.

Directory Servers

Click **CERTIFICATES**, **Directory Servers** to open the **Directory Servers** screen. This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the Contivity 221. If you decide to have the Contivity 221 check incoming certificates against the issuing certification authority's list of revoked certificates, the Contivity 221 first checks the server(s) listed in the **CRL Distribution Points** field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the Contivity 221 checks the servers listed here.

Figure 91 Directory Servers



The following table describes the labels in this screen.

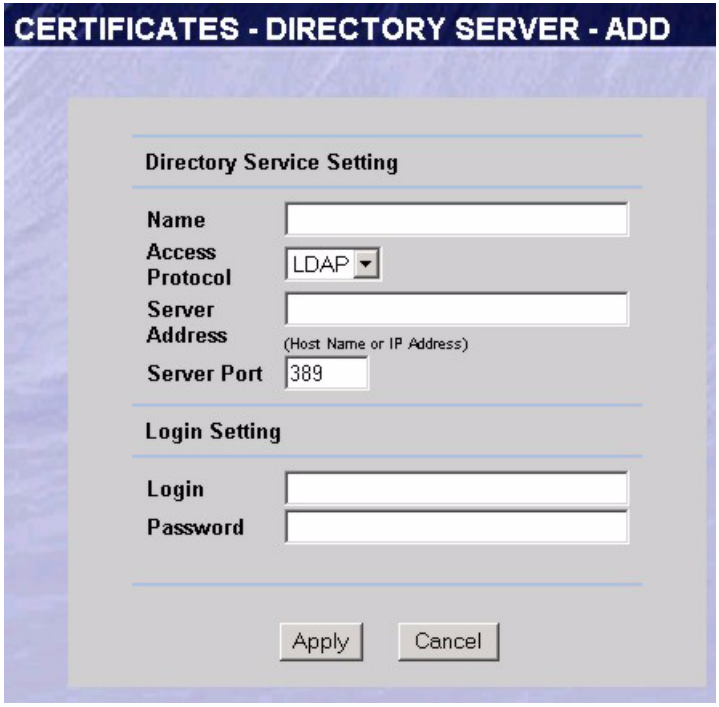
Table 71 Directory Servers

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the Contivity 221's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	The index number of the directory server. The servers are listed in alphabetical order.
Name	This field displays the name used to identify this directory server.
Address	This field displays the IP address or domain name of the directory server.
Port	This field displays the port number that the directory server uses.
Protocol	This field displays the protocol that the directory server uses.
Modify	Click the details icon to open a screen where you can change the information about the directory server. Click the delete icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action.
Add	Click **Add** to open a screen where you can configure information about a directory server so that the Contivity 221 can access it.

Add or Edit a Directory Server

Click **CERTIFICATES**, **Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to open the following screen. Use this screen to configure information about a directory server that the Contivity 221 can access.

Figure 92 Directory Server Add



The following table describes the labels in this screen.

Table 72 Directory Server Add

Label	Description
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.
Access Protocol	Use the drop-down list box to select the access protocol used by the directory server. **LDAP** (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories certificates and lists of revoked certificates.[1]
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.

Table 72 Directory Server Add

Label	Description
Server Port	This field displays the default server port number of the protocol that you select in the **Access Protocol** field. You may change the server port number if needed, however you must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
Login Setting	
Login	The Contivity 221 may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Apply	Click **Apply** to save your changes back to the Contivity 221.
Cancel	Click **Cancel** to quit configuring this screen and return to the **Directory Servers** screen.

1 At the time of writing, LDAP is the only choice of directory server access protocol.

Chapter 15
Bandwidth Management

This chapter describes the functions and configuration of bandwidth management.

Bandwidth Management Overview

Bandwidth management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the Contivity 221 forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- Which traffic must have guaranteed delivery?
- How much bandwidth should be allotted to guarantee delivery?

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1024 kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1024 kbps.

Bandwidth Classes and Filters

Use bandwidth sub-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth sub-class based on a specific application and/or subnet. Use the **Class Setup** tab (see the Bandwidth Manager Class Configuration section) to set up a bandwidth class's name, bandwidth allotment, and filter specifics. Each bandwidth sub-class consists of a single filter you can define by editing the sub-class.

Unallocated bandwidth, that is bandwidth that is not controlled by a sub-class you specify, is allocated to traffic that is not controlled by any sub-class. View your configured bandwidth sub-classes for a given interface in the **Class Setup** tab (see the Configuring Class Setup section for details). The total of the configured bandwidth budgets cannot exceed the configured bandwidth budget for the interface, as specified on the **Summary** page.

Proportional Bandwidth Allocation

Bandwidth management allows you to define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

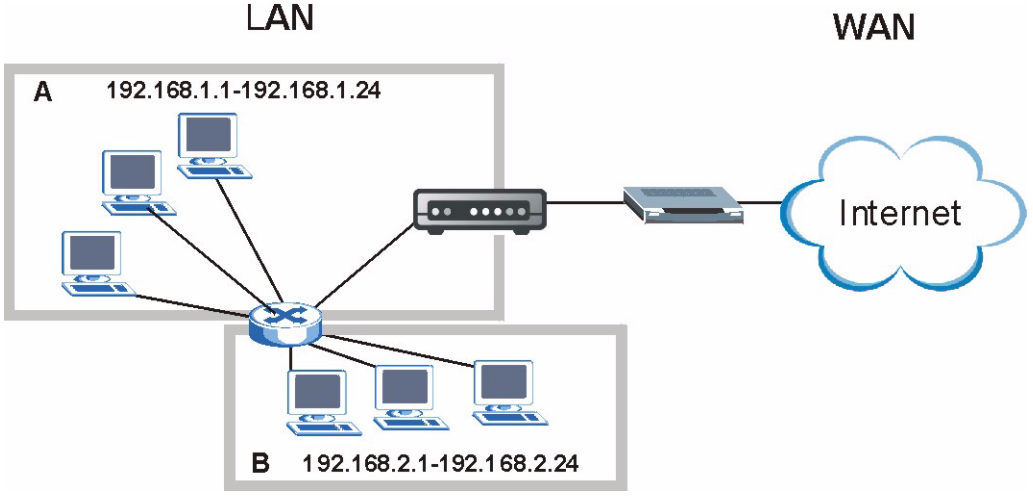
Application-based Bandwidth Management

You can create bandwidth classes based on individual applications (like FTP, H.323 and SIP).

Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets. The following figure shows LAN subnets. You could configure one bandwidth class for subnet A and another for subnet B.

Figure 93 Subnet-based Bandwidth Management Example



Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

Table 73 Application and Subnet-based Bandwidth Management Example

Traffic Type	From Subnet A	From Subnet B
FTP	64 Kbps	64 Kbps
H.323	64 Kbps	64 Kbps
SIP	64 Kbps	64 Kbps

Reserving Bandwidth for Non-Bandwidth Class Traffic

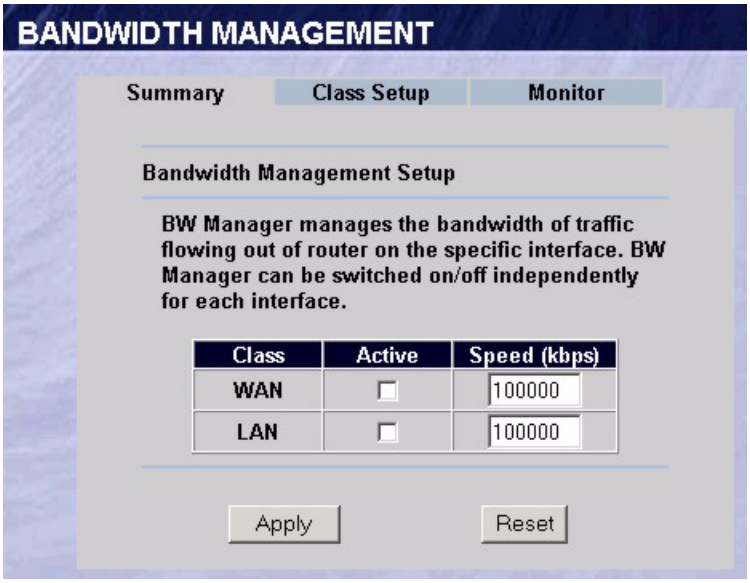
If you want to allow bandwidth for traffic that is not defined in a bandwidth filter, leave some of the interface's bandwidth unbudgeted.

Configuring Summary

Click **BW MGMT** to open the **Summary** screen.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

Figure 94 Bandwidth Manager: Summary



The following table describes the labels in this screen.

Table 74 Bandwidth Manager: Summary

Label	Description
WAN LAN	These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the Contivity 221 and be managed by bandwidth management.
Active	Select an interface's check box to enable bandwidth management on that interface.

Table 74 Bandwidth Manager: Summary

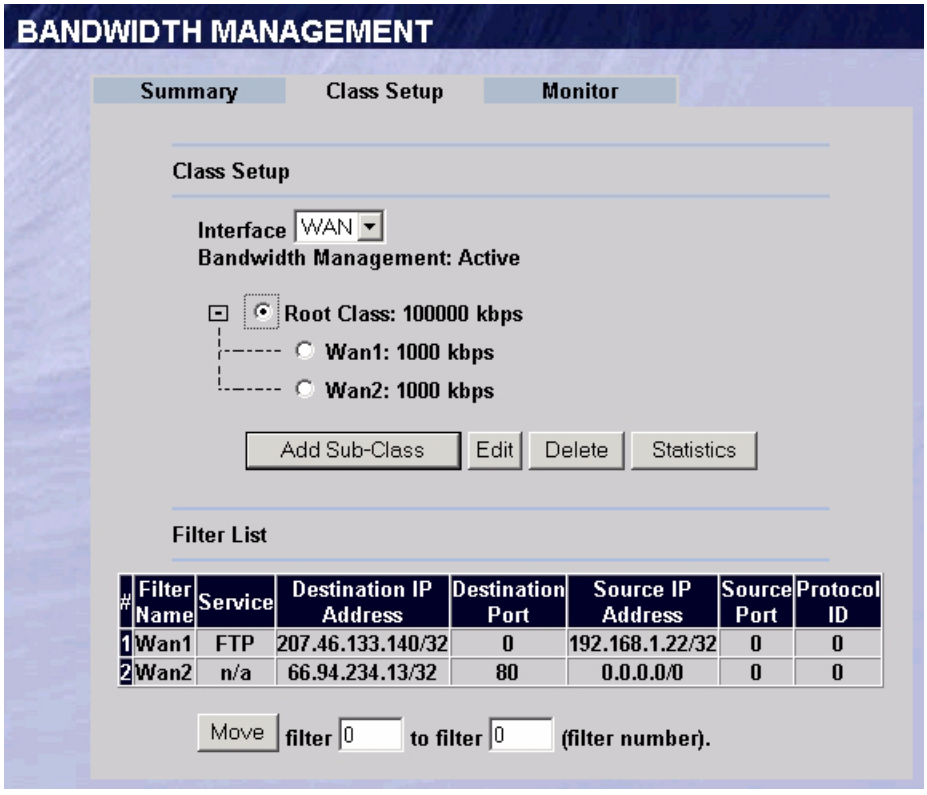
Label	Description
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class (see the Configuring Class Setup section). The recommendation is to set this speed to match what the device connected to the port can handle. For example, set the WAN interface speed to 1000 kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1000 kbps.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring Class Setup

The class setup screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click "+" to expand the class tree or click "-" to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see the Configuring Summary section to configure the speed of the interface). Configure sub-class layers for the root class.

To add or delete child classes on an interface, click **BW MGMT**, then the **Class Setup** tab. The screen appears as shown (with example classes).

Figure 95 Bandwidth Manager: Class Setup



The following table describes the labels in this screen.

Table 75 Bandwidth Manager: Class Setup

Label	Description
Interface	Select an interface from the drop-down list box for which you wish to set up classes.
Bandwidth Management	This field displays whether bandwidth management on the interface you selected in the field above is enabled (**Active**) or not (**Inactive**).
Add Sub-Class	Click **Add Sub-class** to add a sub-class.
Edit	Click **Edit** to go to a screen where you can configure the selected sub-class. You cannot edit the root class.
Delete	Click **Delete** to remove the selected sub-class. You cannot delete the root class.
Statistics	Click **Statistics** to display the status of the selected class.

Table 75 Bandwidth Manager: Class Setup

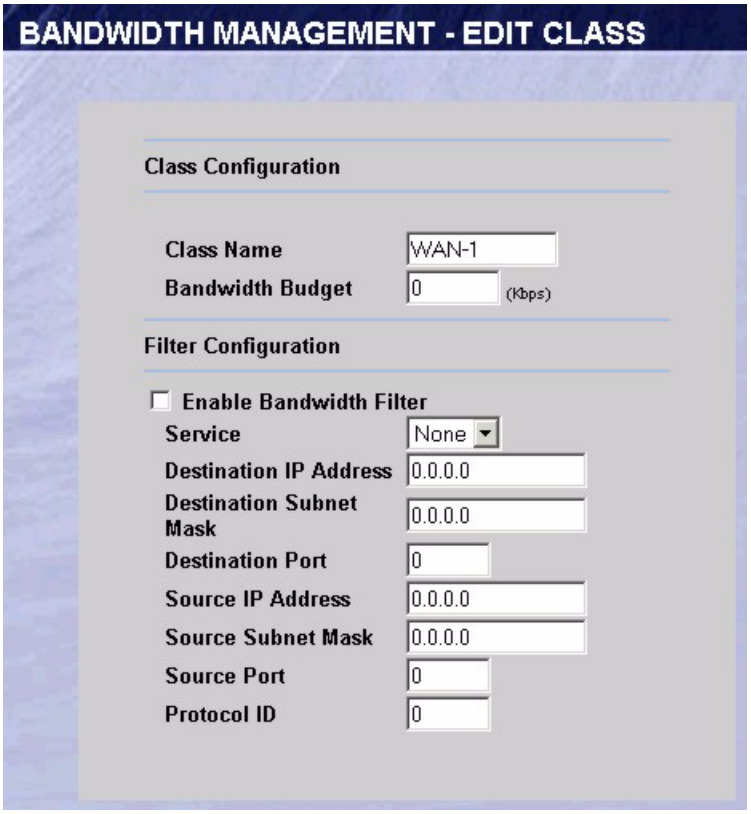
Label	Description
#	This is the number of a filter entry. The ordering of your filters is important as they are applied in turn. The **Move** button below allows you to reorder your filters.
Filter Name	This is the **Class Name** that you configured in the **Edit Class** screen.
Service	If you selected a predefined application (FTP, H.323 or SIP), it displays here.
Destination IP Address	This field displays the destination IP address in dotted decimal notation followed by the subnet mask. 0.0.0.0/0 means all.
Destination Port	This field displays the port number of the destination. 0 means all ports.
Source IP Address	This field displays the source IP address in dotted decimal notation followed by the subnet mask. 0.0.0.0/0 means all.
Source Port	This field displays the port number of the source. 0 means all ports.
Protocol ID	This field displays the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP. 0 means all protocols.
Move	Type the number of a filter entry and the number for where you want to put it. Click **Move** to move the filter to the number that you typed. The ordering of your filters is important as they are applied in order of their numbering. The filter entry numbers are not static names for the entries. A filter entry's number changes as you move the filter entry up or down in the list. Also, only the existing filter entries are counted, you cannot have any blank filter entries. For example, if you have only three filters and try to move number one to seven, it will become filter three.

Bandwidth Manager Class Configuration

Configure a bandwidth management class in the **Class Setup** screen. You must use the **Summary** screen to enable bandwidth management on an interface before you can configure sub-classes for that interface.

To add a sub-class, click **BW MGMT**, then the **Class Setup** tab. Click the **Add Sub-Class** button to open the following screen.

Figure 96 Bandwidth Manager: Edit Class



The following table describes the labels in this screen.

Table 76 Bandwidth Manager: Edit Class

Label	Description
Class Configuration	
Class Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
Bandwidth Budget (kbps)	Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class. The bandwidth you specify cannot cause the total allocated bandwidths of this and all other sub-classes to exceed the bandwidth for the interface.
Filter Configuration	

Table 76 Bandwidth Manager: Edit Class

Label	Description
Enable Bandwidth Filter	Select **Enable Bandwidth Filter** to have the Contivity 221 use this bandwidth filter when it performs bandwidth management. You must enter a value in at least one of the following fields (other than the **Subnet Mask** fields which are only available when you enter the destination or source IP address).
Service	This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not need to configure the rest of the bandwidth filter fields (other than the **Active** check box). **FTP** (File Transfer Program) is a program to enable fast transfer of files, including large files that may not be possible by e-mail. Select FTP from the drop-down list box to configure the bandwidth filter for FTP traffic. **H.323** is a protocol standard used for multimedia communications over networks, for example NetMeeting. Select H.323 from the drop-down list box to configure the bandwidth filter for H.323 traffic. If you select **H.323**, make sure you also turn on the H.323 ALG. See “ALG” on page 94. **SIP** (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging, events notification and conferencing. The Contivity 221 supports SIP traffic pass-through. Select SIP from the drop-down list box to configure this bandwidth filter for SIP traffic. This option makes it easier to manage bandwidth for SIP traffic and is useful for example when there is a VoIP (Voice over Internet Protocol) device on your LAN. If you select **SIP**, make sure you also turn on the SIP ALG. See “ALG” on page 94. Select **All** from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select **All**, you need to configure at least one of the following fields (other than the **Subnet Mask** fields which you only enter if you also enter a corresponding destination or source IP address).
Destination IP Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a **Destination IP Address**. Refer to Appendix H, “IP Subnetting for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See the Predefined Services section in Chapter 10 Firewall Screens for a table of services and port numbers.
Source IP Address	Enter the source IP address.

Table 76 Bandwidth Manager: Edit Class

Label	Description
Source Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a **Source IP Address**. Refer to Appendix H, "IP Subnetting for more information on IP subnetting.
Source Port	Enter the port number of the source. See the following table for some common services and port numbers.
Protocol ID	Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Cancel	Click **Cancel** to exit this screen without saving.

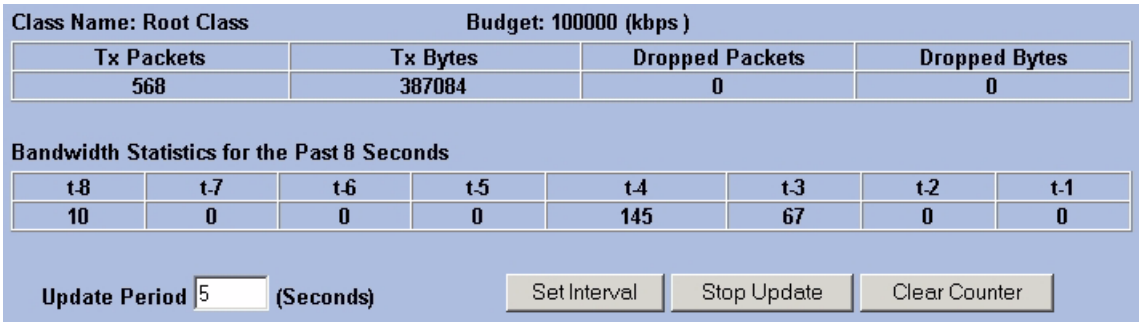
Table 77 Services and Port Numbers

Services	Port Number
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Bandwidth Management Statistics

Use the **Bandwidth Management Statistics** screen to view network performance for the interface (root class) or a specific sub-class. Select the root or sub-class from the **Class Setup** screen and then click **Statistics** to see how it is performing.

Figure 97 Bandwidth Management Statistics



The following table describes the labels in this screen.

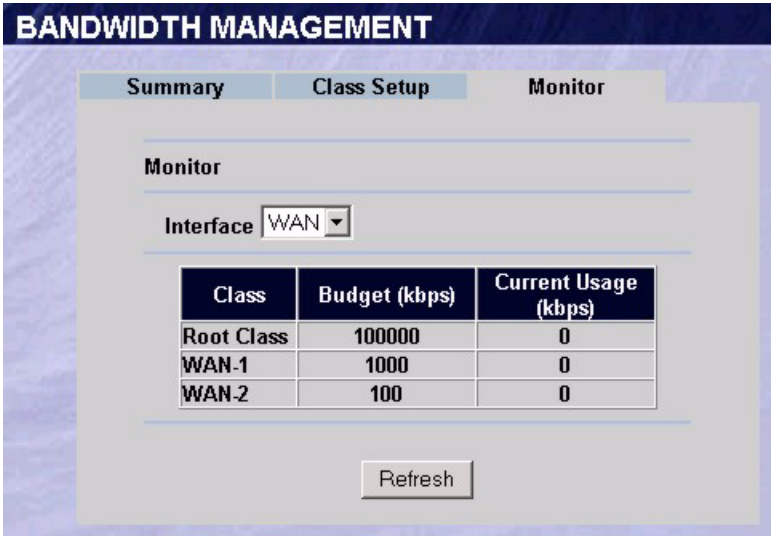
Table 78 Bandwidth Management Statistics

Label	Description
Class Name	This field displays the name of the class the statistics page is showing.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Tx Packets	This field displays the total number of packets transmitted.
Tx Bytes	This field displays the total number of bytes transmitted.
Dropped Packets	This field displays the total number of packets dropped.
Dropped Bytes	This field displays the total number of bytes dropped.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1)	
This field displays the bandwidth statistics (in bps) for the past one to eight seconds. For example, t-1 means one second ago.	
Update Period (Seconds)	Enter the time interval in seconds to define how often the information should be refreshed.
Set Interval	Click **Set Interval** to apply the new update period you entered in the **Update Period** field above.
Stop Update	Click **Stop Update** to stop the browser from refreshing bandwidth management statistics.
Clear Counter	Click **Clear Counter** to clear all of the bandwidth management statistics.

Monitor

To view the device's bandwidth usage and allotments, click **BW MGMT**, then the **Monitor** tab. The screen appears as shown.

Figure 98 Bandwidth Manager Monitor



The following table describes the labels in this screen.

Table 79 Bandwidth Manager Monitor

Label	Description
Interface	Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes.
Class	This field displays the name of the class.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Current Usage (kbps)	This field displays the amount of bandwidth that each class is using.
Refresh	Click **Refresh** to update the page.

Chapter 16
IEEE 802.1x

IEEE 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of users and encryption key management. Authentication can be done using the local user database internal to the Contivity 221 (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

RADIUS

RADIUS is based on a client-sever model that supports authentication and accounting, where users are the clients and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- Authentication

  Determines the identity of the users.

- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your Contivity 221 acts as a message relay between the user and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the Contivity 221 and the RADIUS server for user authentication:

- Access-Request

  Sent by the Contivity 221 requesting authentication.

- Access-Reject

  Sent by a RADIUS server rejecting access.

- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The Contivity 221 sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the Contivity 221 and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the Contivity 221 requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the Contivity 221 and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

EAP Authentication Overview

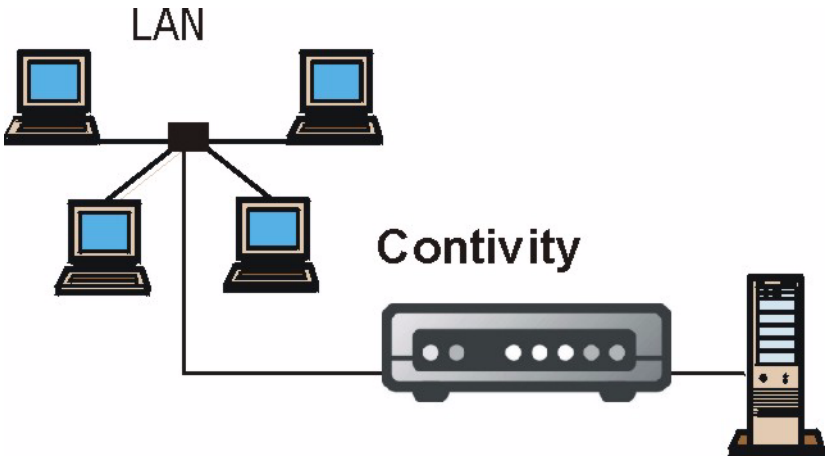
EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the Contivity 221 helps a user's computer and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP.

Your Contivity 221 supports EAP-MD5 (Message-Digest Algorithm 5) with the local user database.

The following figure shows an overview of authentication when you specify a RADIUS server on your Contivity 221.

Figure 99 EAP Authentication



The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the appendix on the IEEE 802.1x.

- The user sends a start message to the Contivity 221.
- The Contivity 221 sends a request identity message to the user for identity information.
- The user replies with identity information, including username and password.
- The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the user.

Configuring 802.1X

To change your Contivity 221's Authentication settings, click **802.1X**. The screen appears as shown.

Figure 100 802.1X



The following table describes the labels in this screen.

Table 80 802.1X

Label	Description
Authentication Type	Select **Authentication Required**, **No Access** or **No Authentication Required** from the drop-down list box. Select **Authentication Required** to authenticate all users before they can access the network. Select **No Authentication Required** to allow all users to access your network without authentication. Select **No Access** to deny all users access to your wired network.
Reauthentication Period	Specify the time interval between the RADIUS server's authentication checks of users connected to the network. This field is active only when you select **Authentication Required** in the **Authentication Type** field.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 17
Authentication Server

The Contivity 221 can use either the local user database internal to the Contivity 221 or an external RADIUS server for an unlimited number of users.

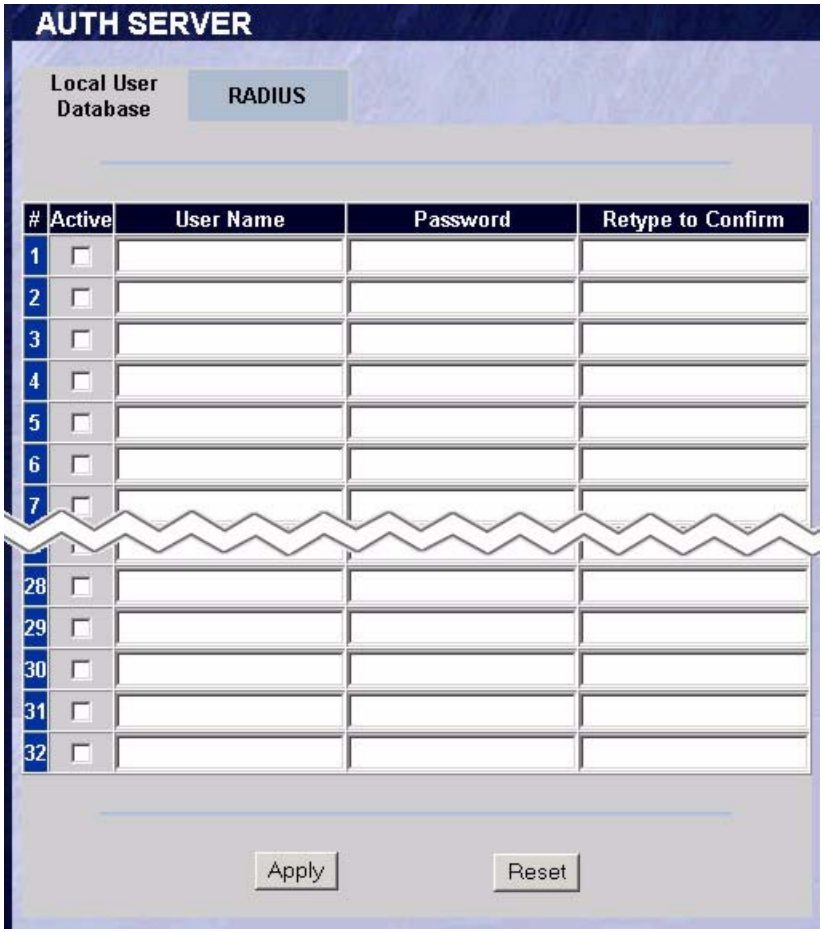
Introduction to Local User Database

By storing user profiles locally on the Contivity 221, your Contivity 221 is able to authenticate users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

Configuring Local User Database

To change your Contivity 221's local user list, click **AUTH SERVER**. The **Local User Database** screen appears as shown.

Figure 101 Local User Database



The following table describes the labels in this screen.

Table 81 Local User Database

Label	Description
Active	Select this check box to enable the user profile.
User Name	Enter the user name of the user profile.
Password	Enter a password up to 31 characters long for this user profile. Note that as you type a password, the screen displays a (*) for each character you type.

Table 81 Local User Database

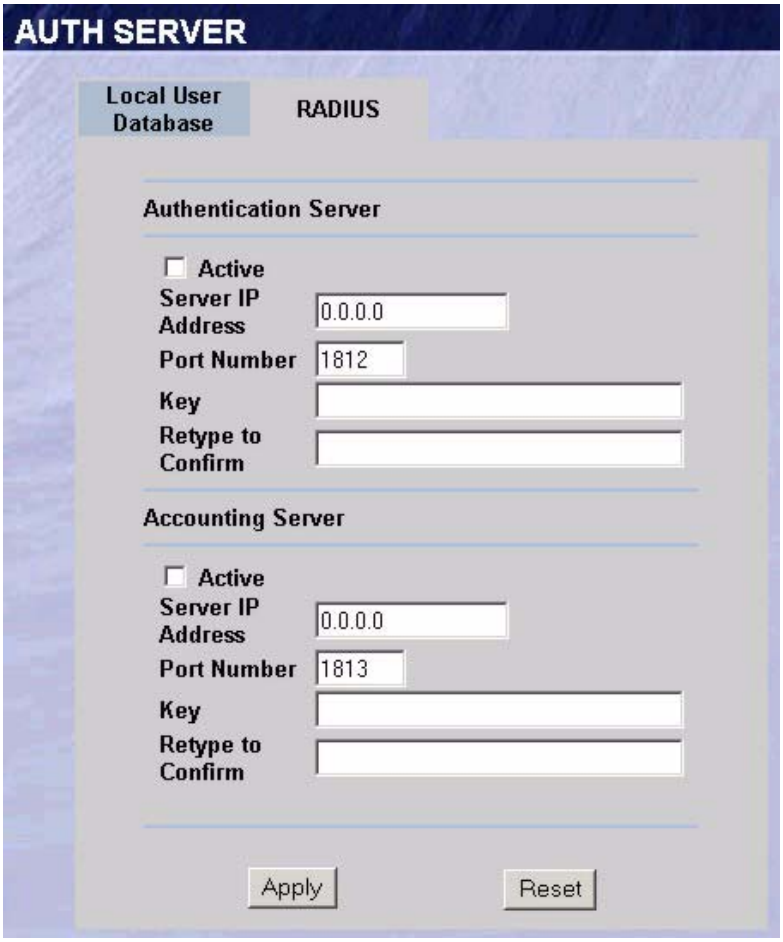
Label	Description
Retype to Confirm	Enter the password again to make sure that you have entered it correctly.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring RADIUS

Use RADIUS if you want to authenticate users using an external server.

To set up your Contivity 221's RADIUS Server settings, click **AUTH SERVER,** then the **RADIUS** tab. The screen appears as shown.

Figure 102 RADIUS



The following table describes the labels in this screen.

Table 82 RADIUS

Label	Description
Authentication Server	
Active	Select the check box to enable user authentication through an external authentication server. Clear the check box to enable user authentication using the local user profile on the Contivity 221.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Contivity 221. Note that as you type a password, the screen displays a (*) for each character you type. The key is not sent over the network. This key must be the same on the external authentication server and Contivity 221.
Retype to Confirm	Enter the password again to make sure that you have entered it correctly.
Accounting Server	
Active	Select the check box to enable user accounting through an external authentication server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the Contivity 221. Note that as you type a password, the screen displays a (*) for each character you type. The key is not sent over the network. This key must be the same on the external accounting server and Contivity 221.
Retype to Confirm	Enter the password again to make sure that you have entered it correctly.

Table 82 RADIUS

Label	Description
Apply	Click **Apply** to save your changes back to the Contivity 221.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 18
Remote Management Screens

This chapter provides information on the **Remote Management** screens.

Remote Management Overview

Remote management allows you to determine which services/protocols can access which Contivity 221 interface (if any) from which computers.



Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

You may manage your Contivity 221 from a remote location via:

Internet (WAN only)	ALL (LAN and WAN)
LAN only,	Neither (Disable).



Note: When you Choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in SMT menu 3.1 (LAN) or in menu 11.1.4 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in one of the remote management screens.
3. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the Contivity 221 will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
6. There is a web remote management session running with a Telnet session. A web session will be disconnected if you begin a Telnet session; it will not begin if there already is a Telnet session.
7. There is a firewall rule that blocks it.

Remote Management and NAT

When NAT is enabled:

- Use the Contivity 221's WAN IP address when configuring from the WAN.
- Use the Contivity 221's LAN IP address when configuring from the LAN.

System Timeout

There is a system timeout of five minutes (three hundred seconds) for either the console port or telnet/web/FTP connections. Your Contivity 221 automatically logs you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line. Use the **System** screen to change the timeout period in the **Administrator Inactivity Timer** field.

Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

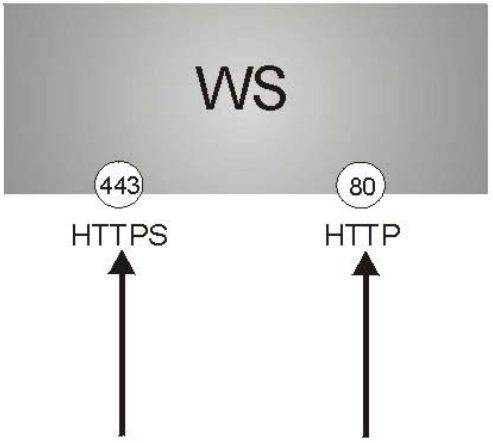
It relies upon certificates, public keys, and private keys (see Chapter 14 Certificates for more information).

HTTPS on the Contivity 221 is used so that you may securely access the Contivity 221 using the WebGUI. The SSL protocol specifies that the SSL server (the Contivity 221) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Contivity 221), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT**, **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-client must send the Contivity 221 a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the Contivity 221.

Please refer to the following figure.

1. HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Contivity 221's WS (web server).
2. HTTP connection requests from a web browser go to port 80 (by default) on the Contivity 221's WS (web server).

Figure 103 HTTPS Implementation

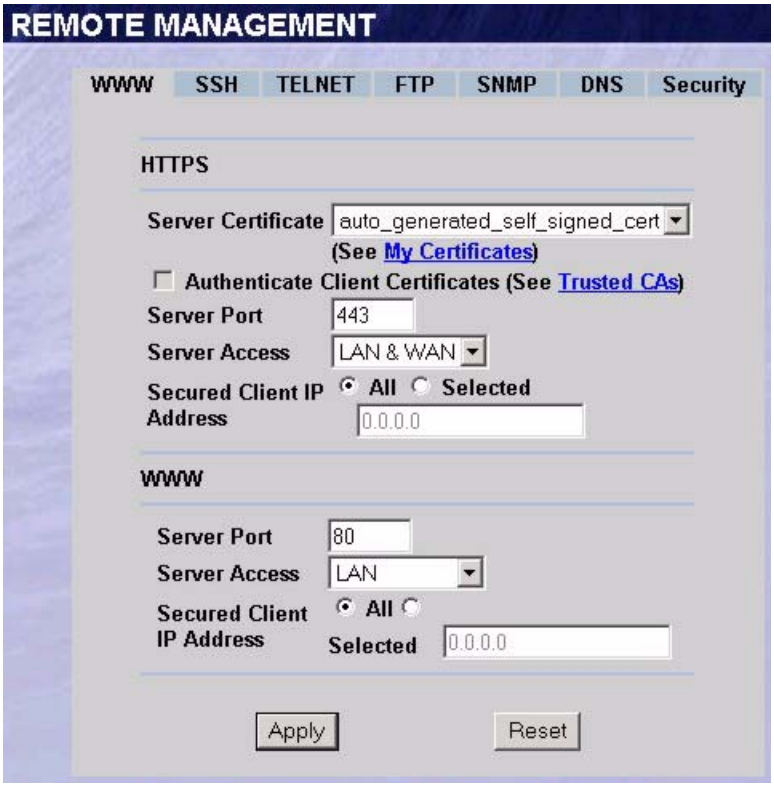


Note: If you disable **HTTP Server Access** (**Disable**) in the **REMOTE MGMT WWW** screen, then the Contivity 221 blocks all HTTP connection attempts.

Configuring WWW

To change your Contivity 221's web settings, click **REMOTE MGMT** to open the **WWW** screen.

Figure 104 WWW



The following table describes the labels in this screen.

Table 83 WWW

Label	Description
HTTPS	
Server Certificate	Select the **Server Certificate** that the Contivity 221 will use to identify itself. The Contivity 221 is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Contivity 221).
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the Contivity 221 by sending the Contivity 221 a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the Contivity 221 (see the appendix on importing certificates for details).

Table 83 WWW

Label	Description
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the Contivity 221, for example 8443, then you must notify people who need to access the Contivity 221 WebGUI to use “https://Contivity 221 IP Address:**8443**” as the URL.
Server Access	Select a Contivity 221 interface from **Server Access** on which incoming HTTPS access is allowed. You can allow only secure WebGUI access by setting the **HTTP Server Access** field to **Disable** and setting the **HTTPS Server Access** field to an interface(s).
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the Contivity 221 using this service. Select **All** to allow any computer to access the Contivity 221 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Contivity 221 using this service.
HTTP	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the Contivity 221 using this service.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the Contivity 221 using this service. Select **All** to allow any computer to access the Contivity 221 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Contivity 221 using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

HTTPS Example

If you haven’t changed the default HTTPS port on the Contivity 221, then in your browser enter “https://Contivity 221 IP Address/” as the web site address where “Contivity 221 IP Address” is the IP address or domain name of the Contivity 221 you wish to access.

Internet Explorer Warning Messages

When you attempt to access the Contivity 221 HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the Contivity 221.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the WebGUI login screen; if you select **No**, then WebGUI access is blocked.

Figure 105 Security Alert Dialog Box (Internet Explorer)



Netscape Navigator Warning Messages

When you attempt to access the Contivity 221 HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the Contivity 221.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the Contivity 221's certificate into the SSL client.

Figure 106 Figure 18-4 Security Certificate 1 (Netscape)



Figure 107 Security Certificate 2 (Netscape)



Avoiding the Browser Warning Messages

The following describes the main reasons that your browser displays warnings about the Contivity 221's HTTPS server certificate and what you can do to avoid

seeing the warnings.

- The issuing certificate authority of the Contivity 221's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the Contivity 221's factory default certificate is the Contivity 221 itself since the certificate is a self-signed certificate.
  - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
  - To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to the appendix on importing certificates for details.
- The actual IP address of the HTTPS server (the IP address of the Contivity 221's port that you are trying to access) does not match the common name specified in the Contivity 221's HTTPS server certificate that your browser received. Do the following to check the common name specified in the certificate that your Contivity 221 sends to HTTPS clients.

  a Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.

  b Click **CERTIFICATES**. Find the certificate and check its **Subject** column. **CN** stands for certificate's common name (see Figure 111 for an example).

Use this procedure to have the Contivity 221 use a certificate with a common name that matches the Contivity 221's actual IP address. You cannot use this procedure if you need to access the WAN port and it uses a dynamically assigned IP address.

a Create a new certificate for the Contivity 221 that uses the IP address (of the Contivity 221's port that you are trying to access) as the certificate's common name. For example, to use HTTPS to access a LAN port with IP address 192.168.1.1, create a certificate that uses 192.168.1.1 as the common name.

b Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

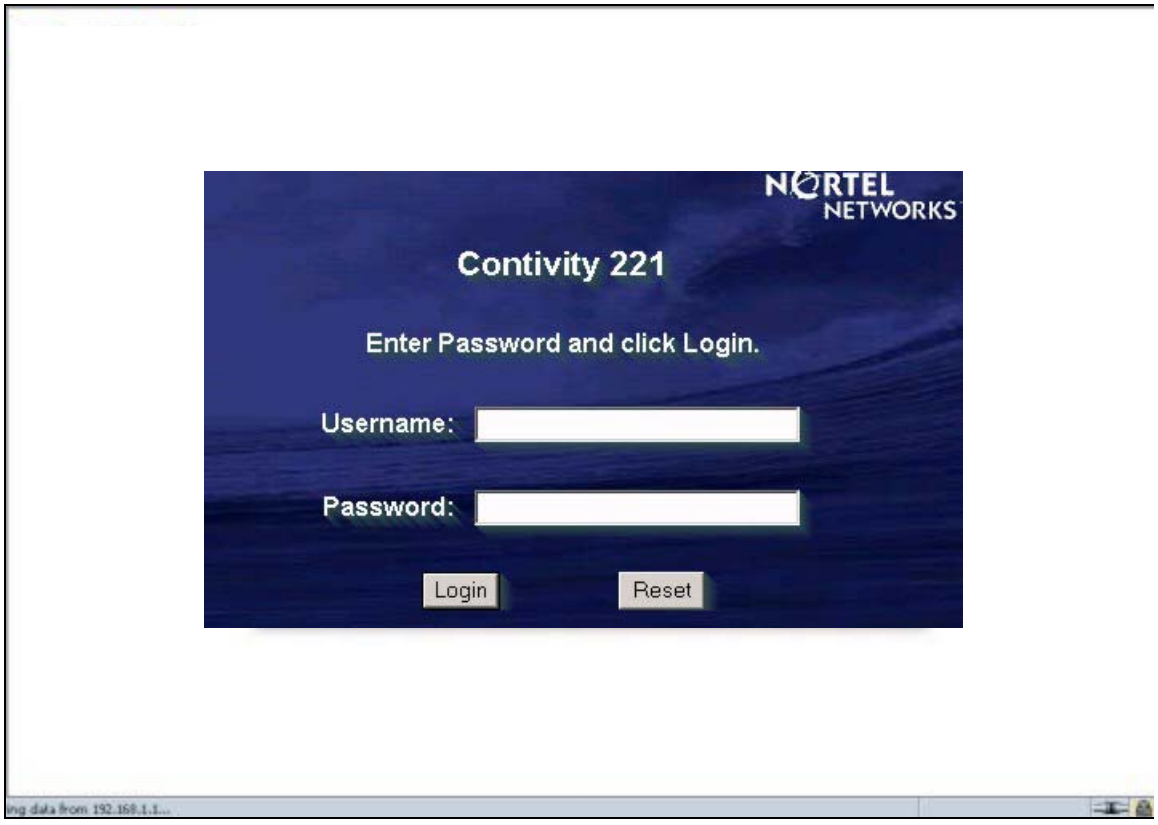
Login Screen

After you accept the certificate, the Contivity 221 login screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

Figure 108 Login Screen (Internet Explorer)



Figure 109 Login Screen (Netscape)



Click **Login** and you then see the next screen.

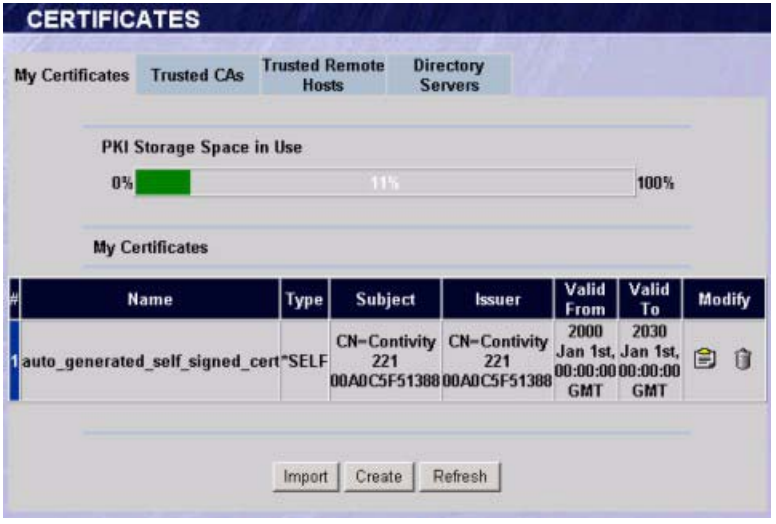
The factory default certificate is a common default certificate for all Contivity 221 models.

Figure 110 Replace Certificate



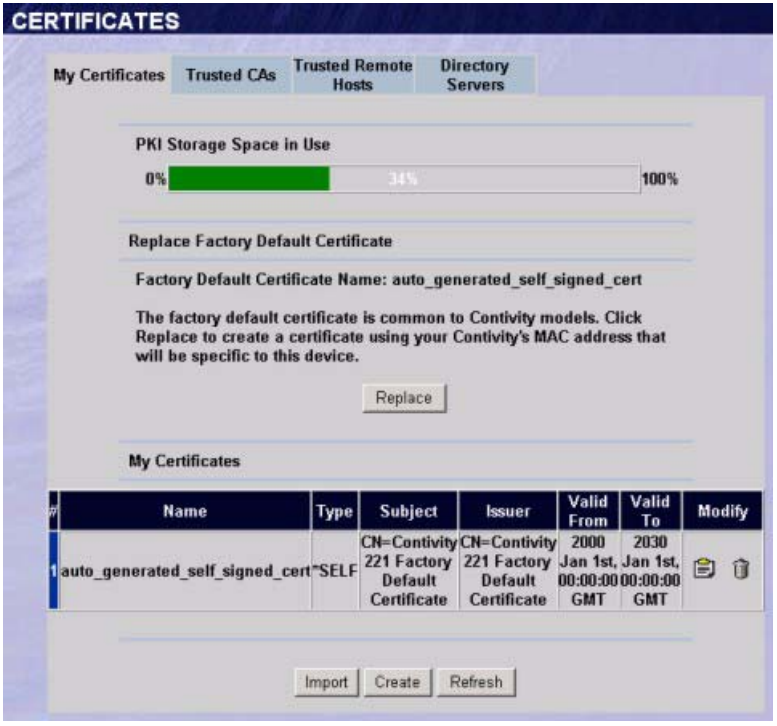
Click **Apply** in the **Replace Certificate** screen to create a certificate using your Contivity 221's MAC address that will be specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You will see information similar to that shown in the following figure.

Figure 111 Device-specific Certificate



Click **Ignore** in the **Replace Certificate** screen to use the common Contivity 221 certificate. You will then see this information in the **My Certificates** screen.

Figure 112 Common Contivity 221 Certificate



SSH Overview

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

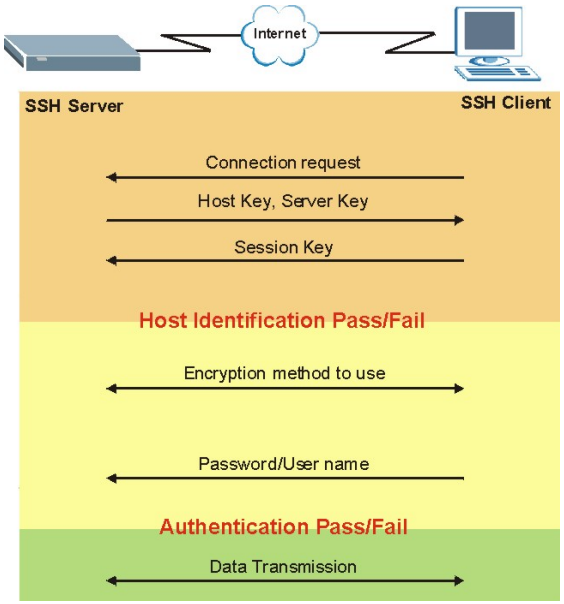
Figure 113 SSH Communication Example



How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 114 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

SSH Implementation on the Contivity 221

Your Contivity 221 supports SSH version 1.5 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the Contivity 221 for remote SMT management and file transfer on port 22. Only one SSH connection is allowed at a time.

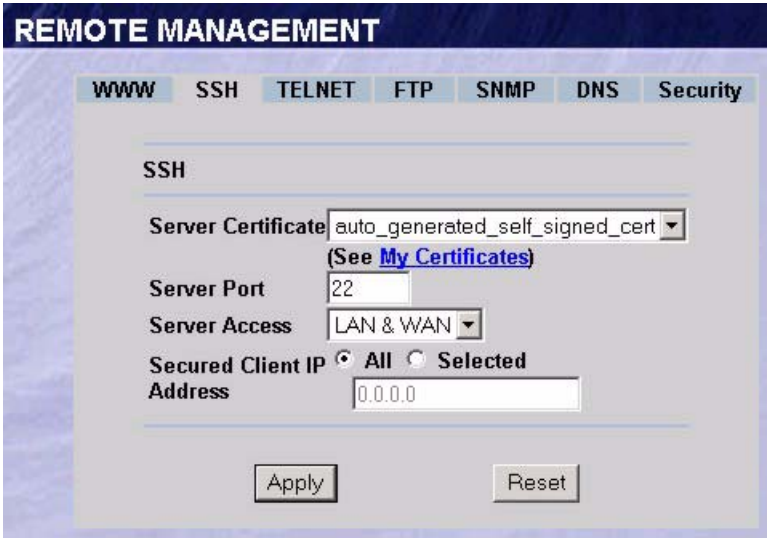
Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Contivity 221 over SSH.

Configuring SSH

To change your Contivity 221's Secure Shell settings, click **REMOTE MGMT**, then the **SSH** tab. The screen appears as shown.

Figure 115 SSH



The following table describes the labels in this screen.

Table 84 SSH

Label	Description
Server Host Key	Select the certificate whose corresponding private key is to be used to identify the Contivity 221 for SSH connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 14 Certificates for details).
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the Contivity 221 using this service.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the Contivity 221 using this service. Select **All** to allow any computer to access the Contivity 221 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Contivity 221 using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Note: It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Secure Telnet Using SSH Examples

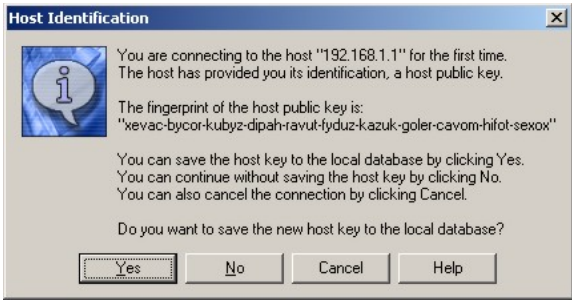
This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the Contivity 221. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

Example 1: Microsoft Windows

This section describes how to access the Contivity 221 using the Secure Shell Client program.

1. Launch the SSH client and specify the connection information (IP address, port number or device name) for the Contivity 221.
2. Configure the SSH client to accept connection using SSH version 1.
3. A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 116 SSH Example 1: Store Host Key



Enter the password to log in to the Contivity 221. The SMT main menu displays next.

Example 2: Linux

This section describes how to access the Contivity 221 using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the Contivity 221.

Enter "`telnet 192.168.1.1 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the Contivity 221 (using the default IP address of 192.168.1.1).

A message displays indicating the SSH protocol version supported by the Contivity 221.

Figure 117 SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "`ssh -1 192.168.1.1`". This command forces your computer to connect to the Contivity 221 using SSH version 1. If this is the first time you are connecting to the Contivity 221 using SSH, a message displays prompting you to save the host information of the Contivity 221. Type "`yes`" and press [ENTER].

Then enter the password to log in to the Contivity 221.

Figure 118 SSH Example 2: Log in

```
$ ssh -1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of known hosts.
Administrator@192.168.1.1's password:
```

3 The SMT main menu displays next.

Secure FTP Using SSH Example

This section shows an example on file transfer using the OpenSSH client program. The configuration and connection steps are similar for other SSH client programs. Refer to your SSH client program user's guide.

1. Enter "`sftp -1 192.168.1.1`". This command forces your computer to connect to the Contivity 221 for secure file transfer using SSH version 1. If this is the first time you are connecting to the Contivity 221 using SSH, a message displays prompting you to save the host information of the Contivity 221. Type "`yes`" and press [ENTER].
2. Enter the password to login to the Contivity 221.
3. Use the "`put`" command to upload a new firmware to the Contivity 221.

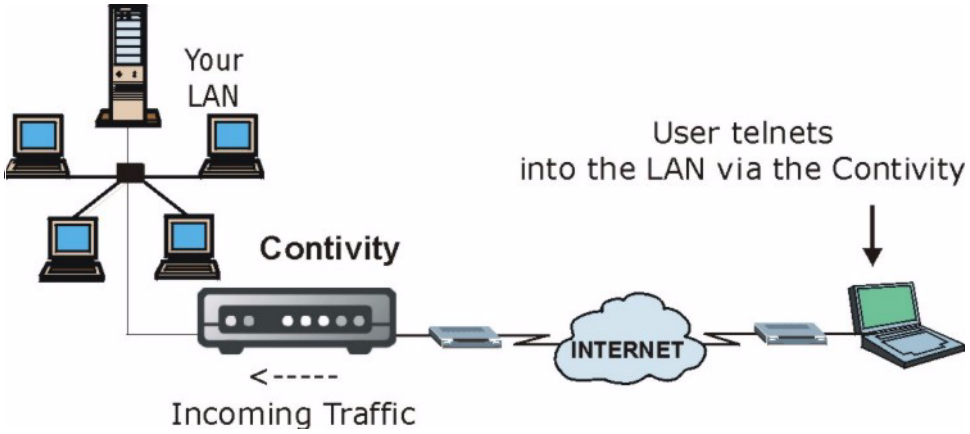
Figure 119 Secure FTP: Firmware Upload Example

```
$ sftp -1 192.168.1.1
Connecting to 192.168.1.1...
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of known hosts.
Administrator@192.168.1.1's password:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.1.1: Connection reset by peer
Connection closed
$
```

Telnet

You can configure your Contivity 221 for remote Telnet access as shown next.

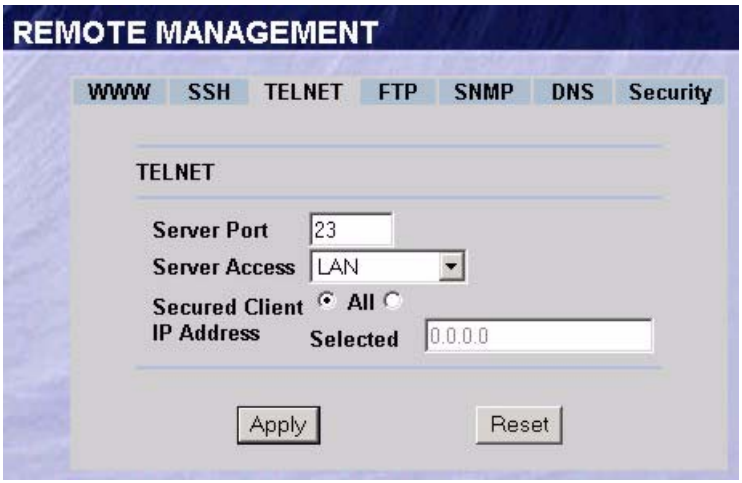
Figure 120 Telnet Configuration on a TCP/IP Network



Configuring TELNET

Click **REMOTE MANAGEMENT** to open the **TELNET** screen.

Figure 121 Telnet



The following table describes the fields in this screen.

Table 85 Telnet

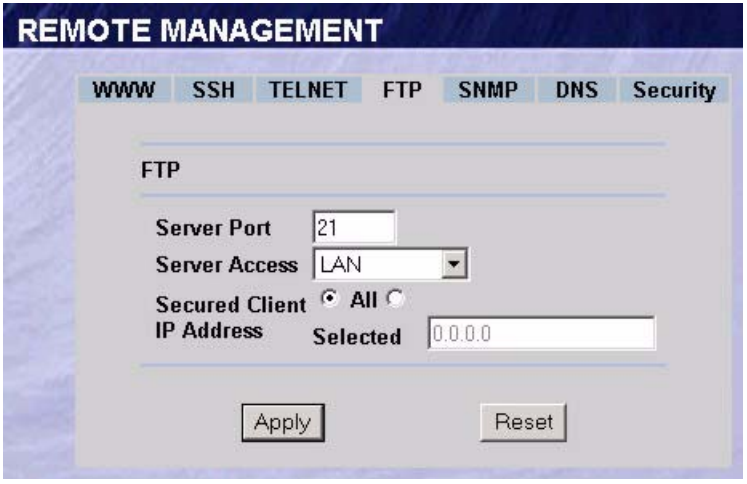
Label	Description
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the Contivity 221 using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the Contivity 221 using this service. Select **All** to allow any computer to access the Contivity 221 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Contivity 221 using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring FTP

You can upload and download the Contivity 221’s firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

To change your Contivity 221's FTP settings, click **REMOTE MANAGEMENT**, then the **FTP** tab. The screen appears as shown.

Figure 122 FTP



The following table describes the fields in this screen.

Table 86 FTP

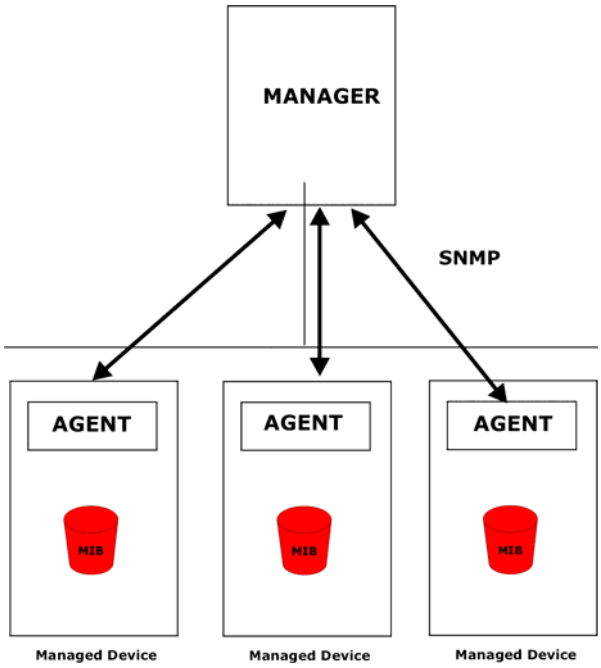
Label	Description
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the Contivity 221 using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the Contivity 221 using this service. Select **All** to allow any computer to access the Contivity 221 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Contivity 221 using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Contivity 221 supports SNMP agent functionality, which allows a manager station to manage and monitor the Contivity 221 through the network. The Contivity 221 supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured. The default get and set communities are “public”.

Note: SNMP is only available if TCP/IP is configured.

Figure 123 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the Contivity 221). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

Supported MIBs

The Contivity 221 supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

SNMP Traps

The Contivity 221 will send traps to the SNMP manager when any one of the following events occurs:

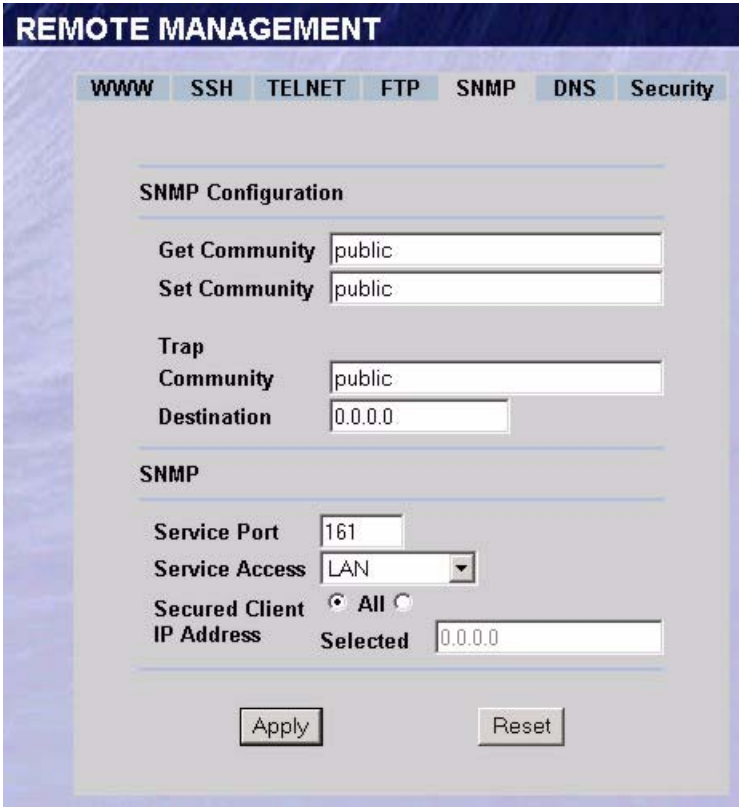
Table 87 SNMP Traps

Trap #	Trap Name	Description
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

REMOTE MANAGEMENT: SNMP

To change your Contivity 221's SNMP settings, click **REMOTE MANAGEMENT**, then the **SNMP** tab. The screen appears as shown.

Figure 124 SNMP



The following table describes the fields in this screen.

Table 88 SNMP

Label	Description
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trusted Host	If you enter a trusted host, your Contivity 221 will only respond to SNMP messages from this address. 0.0.0.0 (default) means your Contivity 221 will respond to all SNMP messages it receives, regardless of source.

Table 88 SNMP

Label	Description
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the Contivity 221 using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the Contivity 221 using this service. Select **All** to allow any computer to access the Contivity 221 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Contivity 221 using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for example, the IP address of www.nortelnetworks.com is 47.249.48.20.

To change your Contivity 221’s DNS settings, click **REMOTE MANAGEMENT**, then the **DNS** tab. The screen appears as shown.

Figure 125 DNS



The following table describes the fields in this screen.

Table 89 DNS

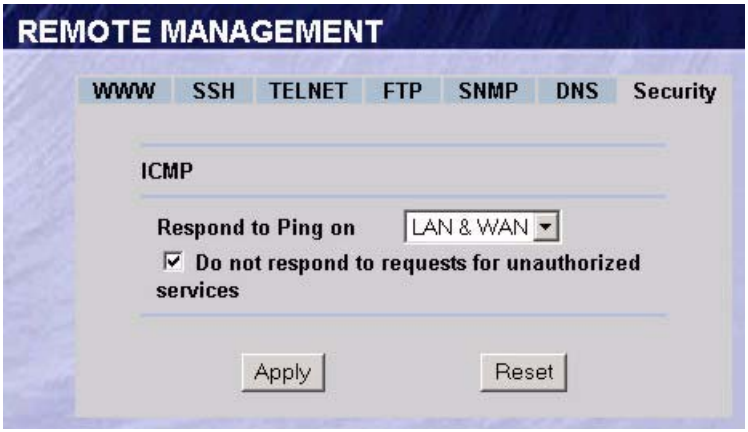
Label	Description
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the Contivity 221.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to send DNS queries to the Contivity 221. Select **All** to allow any computer to send DNS queries to the Contivity 221. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the Contivity 221.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring Security

To change your Contivity 221’s Security settings, click **REMOTE MANAGEMENT**, then the **Security** tab. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your Contivity 221, an ICMP response packet is automatically returned. This allows the outside user to know the Contivity 221 exists. The Contivity 221 series support anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your Contivity 221 when unsupported ports are probed.

Figure 126 Security



The following table describes the fields in this screen.

Table 90 Security

Label	Description
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The Contivity 221 will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests**.** Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests.

Table 90 Security

Label	Description
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the Contivity 221 by probing for unused ports. If you select this option, the Contivity 221 will not send ICMP response packets to port request(s) for unused ports, thus leaving the unused ports and the Contivity 221 unseen. If the firewall blocks a packet from the WAN, the Contivity 221 sends a TCP reset packet. Use the "sys firewall tcprst rst off" command in the command interpreter if you want to stop the Contivity 221 from sending TCP reset packets.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 19
UPnP

This chapter introduces the Universal Plug and Play feature.

Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP Implementation

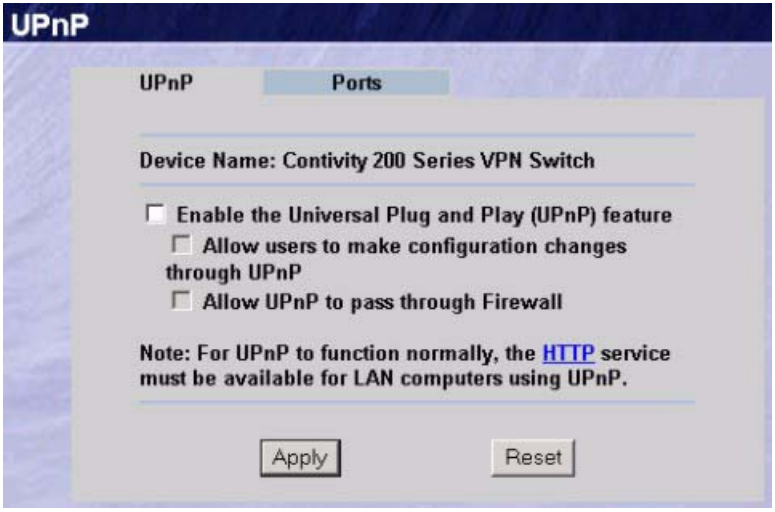
The device has UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). This UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing the UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

The Contivity 221 only sends UPnP multicasts to the LAN.

Configuring UPnP

Click **UPnP** to display the screen shown next.

Figure 127 Configuring UPnP



The following table describes the fields in this screen.

Table 91 Configuring UPnP

Label	Description
Device Name	This identifies the device in UPnP applications.
Enable the Universal Plug and Play (UPnP) feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the WebGUI's login screen without entering the Contivity 221's IP address (although you must still enter the password to access the WebGUI).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the Contivity 221 so that they can communicate through the Contivity 221, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Displaying UPnP Port Mapping

Click **UPnP** and then **Ports** to display the screen as shown next. Use this screen to view the NAT port mapping rules that UPnP creates on the Contivity 221.

Figure 128 UPnP Ports



The following table describes the labels in this screen.

Table 92 UPnP Ports

Label	Description
Retain UPnP port forwarding	Select this check box to have the Contivity 221 retain UPnP created NAT rules even after restarting. If you use UPnP and you set a port on your computer to be fixed for a specific service (for example FTP for file transfers), this option allows the Contivity 221 to keep a record when your computer uses UPnP to create a NAT forwarding rule for that service.
The following read-only table displays information about the UPnP-created NAT mapping rule entries in the Contivity 221's NAT routing table.	
#	This is the index number of the UPnP-created NAT mapping rule entry.
Remote Host	This field displays the source IP address (on the WAN) of inbound IP packets. Since this is often a wildcard, the field may be blank. When the field is blank, the Contivity 221 forwards all traffic sent to the **External Port** on the WAN interface to the **Internal Client** on the **Internal Port**. When this field displays an external IP address, the NAT rule has the Contivity 221 forward inbound packets to the **Internal Client** from that IP address only.

Table 92 UPnP Ports

Label	Description
External Port	This field displays the port number that the Contivity 221 “listens” on (on the WAN port) for connection requests destined for the NAT rule’s **Internal Port** and **Internal Client**. The Contivity 221 forwards incoming packets (from the WAN) with this port number to the **Internal Client** on the **Internal Port** (on the LAN). If the field displays “0”, the Contivity 221 ignores the **Internal Port** value and forwards requests on all external port numbers (that are otherwise unmapped) to the **Internal Client**.
Protocol	This field displays the protocol of the NAT mapping rule (TCP or UDP).
Internal Port	This field displays the port number on the **Internal Client** to which the Contivity 221 should forward incoming connection requests.
Internal Client	This field displays the DNS host name or IP address of a client on the LAN. Multiple NAT clients can use a single port simultaneously if the internal client field is set to 255.255.255.255 for UDP mappings.
Enabled	This field displays whether or not this UPnP-created NAT mapping rule is turned on. The UPnP-enabled device that connected to the Contivity 221 and configured the UPnP-created NAT mapping rule on the Contivity 221 determines whether or not the rule is enabled.
Description	This field displays a text explanation of the NAT mapping rule.
Lease Duration	This field displays a dynamic port-mapping rule’s time to live (in seconds). It displays “0” if the port mapping is static.
Apply	Click **Apply** to save your changes back to the Contivity 221.
Refresh	Click **Refresh** update the screen’s table.

Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

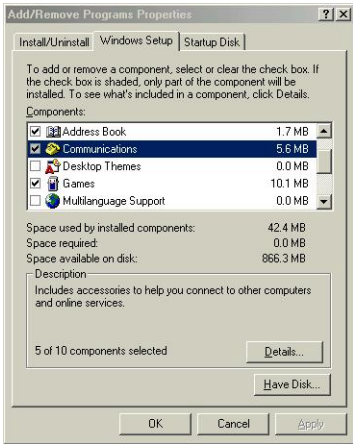
Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 129 Add/Remove Programs: Windows Setup

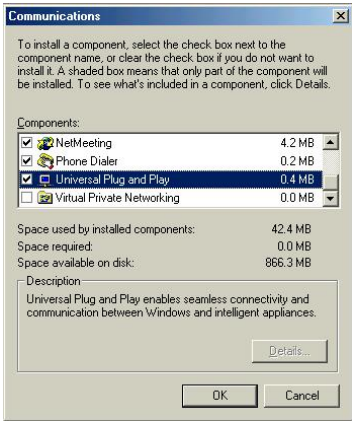


3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Figure 130 Communications



Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

1 Click **start** and **Control Panel**.

2 Double-click Network Connections.

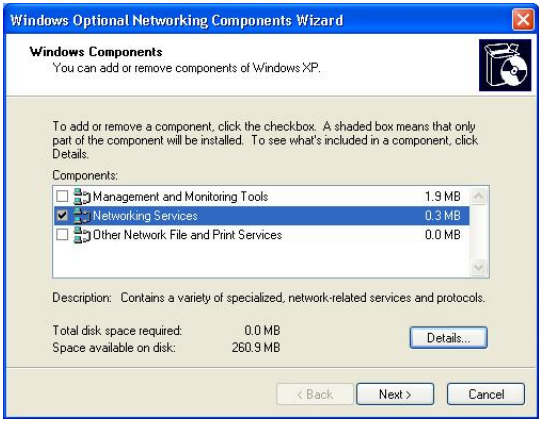
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**
The **Windows Optional Networking Components Wizard** window displays.

Figure 131 Network Connections



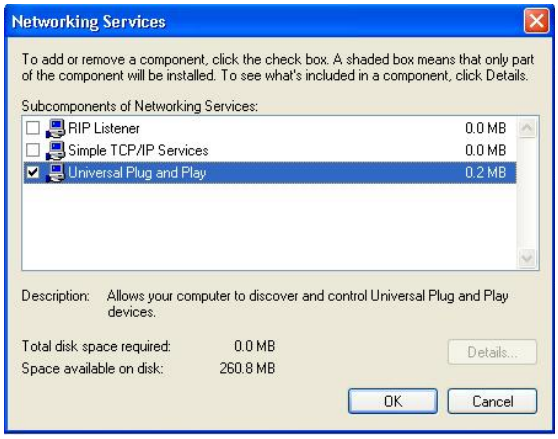
4 Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 132 Windows Optional Networking Components Wizard



5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 133 Windows XP Networking Services



6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the device.

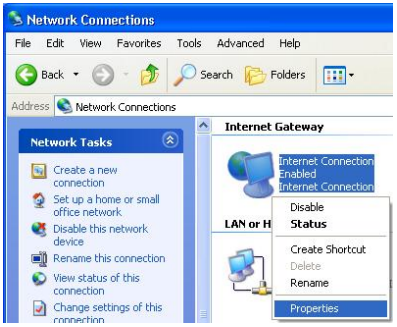
Make sure the computer is connected to a LAN port of the device. Turn on your computer and the Contivity 221.

Auto-discover Your UPnP-enabled Network Device

1 Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.

Figure 134 Internet Gateway Icon



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.

Figure 135 Internet Connection Properties



4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 136 Internet Connection Properties Advanced Setup

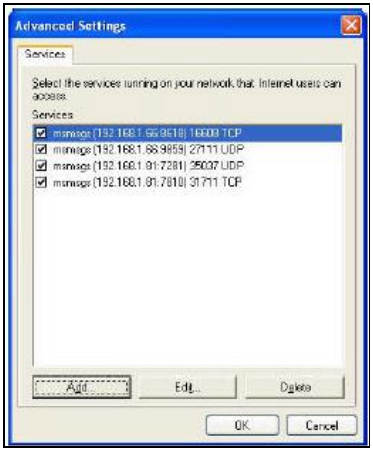
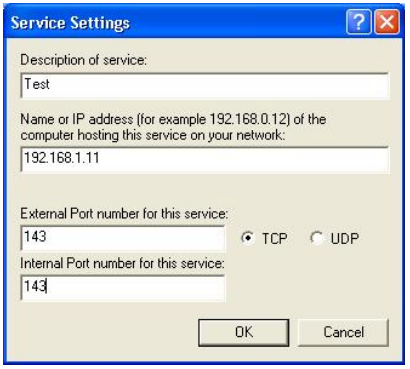


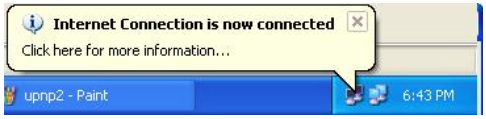
Figure 137 Service Settings



Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

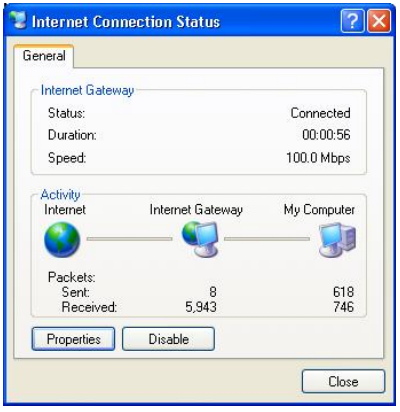
5 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray.

Figure 138 Internet Connection Icon



6 Double-click the icon to display your current Internet connection status.

Figure 139 Internet Connection Status



WebGUI Easy Access

With UPnP, you can access the WebGUI without first finding out its IP address. This is helpful if you do not know the IP address of your Contivity 221.

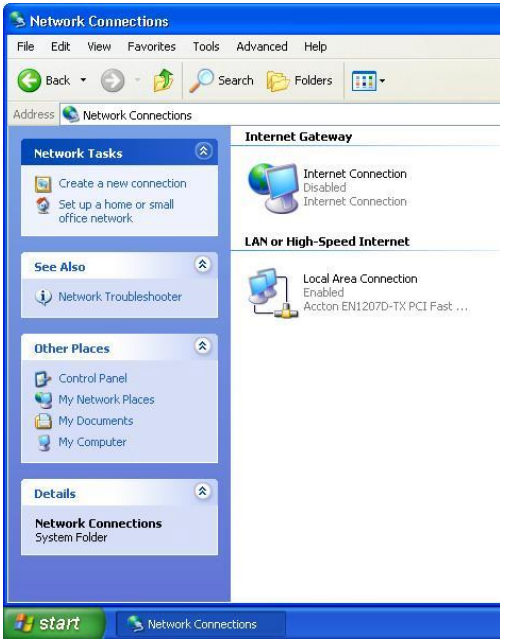
Follow the steps below to access the WebGUI.

1 Click **start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**

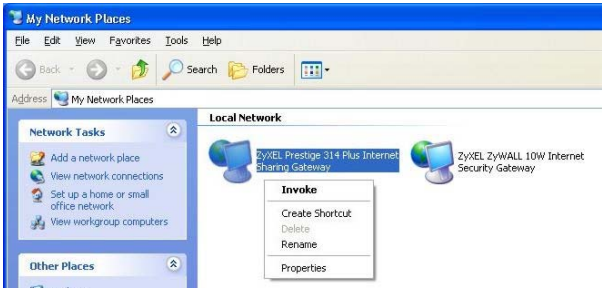
Figure 140 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click the icon for your Contivity 221 and select **Invoke**. The WebGUI login screen displays.

Figure 141 My Network Places: Local Network



Chapter 20
Logs Screens

This chapter contains information about configuring general log settings and viewing the Contivity 221's logs. Refer to the Appendices for example log message explanations.

Configuring View Log

The WebGUI allows you to look at all of the Contivity 221's logs in one location.

Click **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see *page 351*). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 142 View Log



#	Time	Message	Source	Destination	Note
1	01/01/2000 08:38:45	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
2	01/01/2000 08:38:45	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
3	01/01/2000 08:38:45	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
4	01/01/2000 08:38:39	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
5	01/01/2000 08:38:39	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
6	01/01/2000 08:38:39	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
7	01/01/2000 08:38:36	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
8	01/01/2000 08:38:36	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
9	01/01/2000 08:38:36	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
10	01/01/2000 08:37:37	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
11	01/01/2000 08:37:37	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
12	01/01/2000 08:37:37	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
13	01/01/2000 08:37:30	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD

The following table describes the fields in this screen.

Table 93 View Log

Label	Description
Display	The categories that you select in the **Log Settings** page display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the Contivity 221's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.

Table 93 View Log

Label	Description
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

Configuring Log Settings

To change your Contivity 221's log settings, click **Logs**, then the **Log Settings** tab. The screen appears as shown.

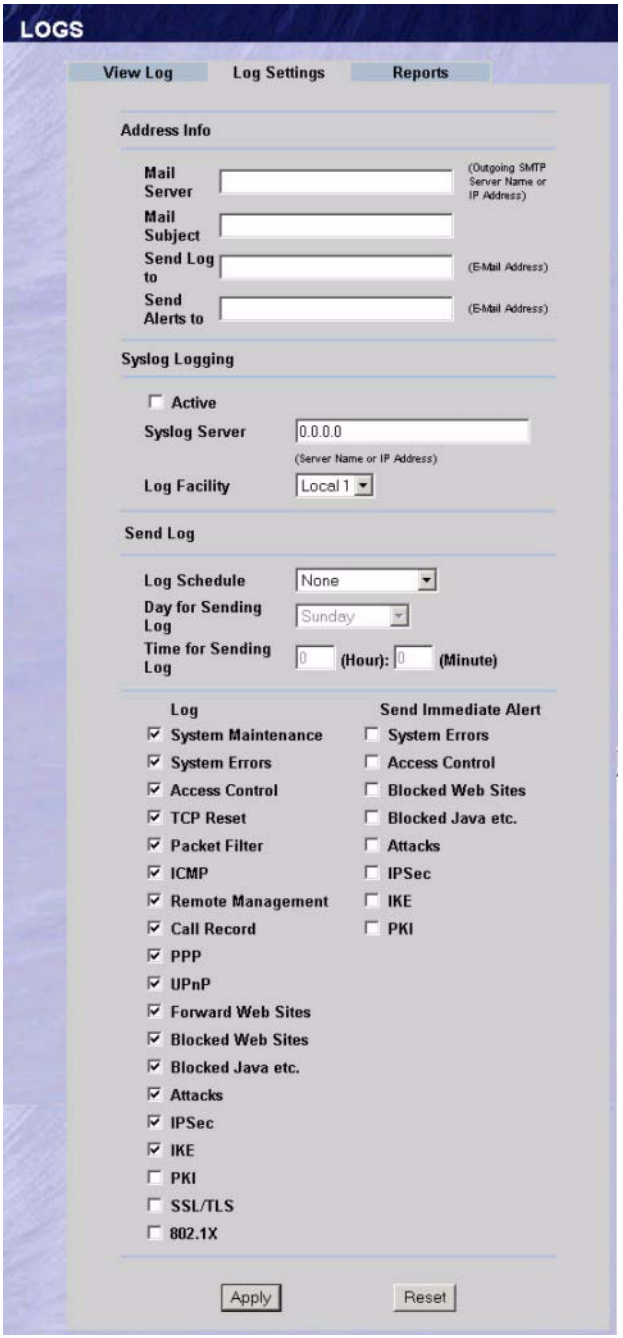
Use the **Log Settings** screen to configure to where the Contivity 221 is to send logs; the schedule for when the Contivity 221 is to send the logs and which logs and/or immediate alerts the Contivity 221 is to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.



Note: Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full. Selecting many alert and/or log categories (especially Access Control) may result in many e-mails being sent.

Figure 143 Log Settings



The following table describes the fields in this screen.

Table 94 Log Settings

Label	Description
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the Contivity 221 sends.
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: Daily Weekly Hourly When the Log is Full None. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.

Table 94 Log Settings

Label	Description
Log	Select the categories of logs that you want to record. Logs include alerts.
Send Immediate Alert	Select the categories of alerts for which you want the Contivity 221 to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Configuring Reports

To change your Contivity 221's log reports, click **Logs**, then the **Reports** tab. The screen appears as shown.

The **Reports** page displays which computers on the LAN send and receive the most traffic, what kinds of traffic are used the most and which web sites are visited the most often. Use the **Reports** screen to have the Contivity 221 record and display the following network usage details:

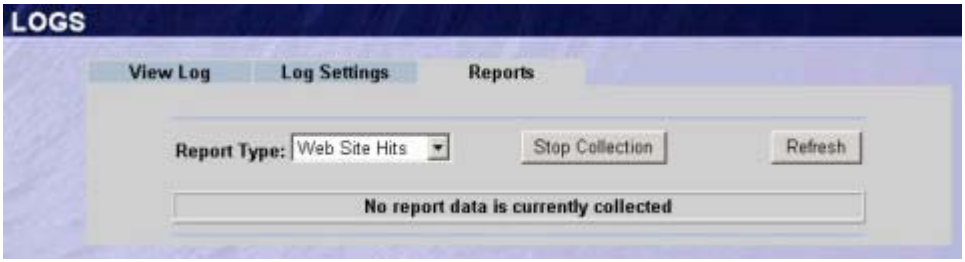
- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN IP addresses to and/or from which the most traffic has been sent
- How much traffic has been sent to and from the LAN IP addresses to and/or from which the most traffic has been sent



Note: The web site hit count may not be 100% accurate because sometimes when an individual web page loads, it may contain references to other web sites that also get counted as hits.

The Contivity 221 records web site hits by counting the HTTP GET packets. Many web sites include HTTP GET references to other web sites and the Contivity 221 may count these as hits, thus the web hit count is not (yet) 100% accurate.

Figure 144 Reports



Note: Enabling the Contivity 221's reporting function decreases the overall throughput by about 1 Mbps.

The following table describes the fields in this screen.

Table 95 Reports

Label	Description
Report Type	Use the drop-down list box to select the type of reports to display. **Web Site Hits** displays the web sites that have been visited the most often from the LAN and how many times they have been visited. **Protocol/Port** displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports. **LAN IP Address** displays the LAN IP addresses to and /or from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses.

Table 95 Reports

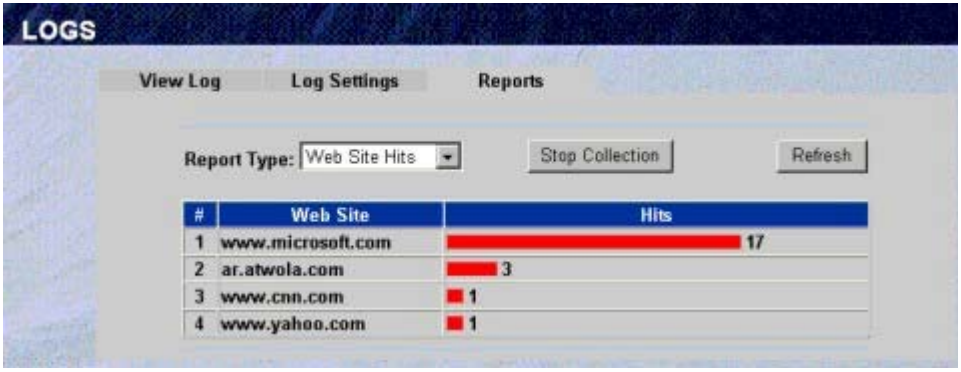
Label	Description
Start Collection/ Stop Collection	The button text shows **Start Collection** when the Contivity 221 is not recording report data and **Stop Collection** when the Contivity 221 is recording report data. Click **Start Collection** to have the Contivity 221 record report data. Click **Stop Collection** to halt the Contivity 221 from recording more data.
Refresh	Click **Refresh** to update the report display. The report also refreshes automatically when you close and reopen the screen.

Note: All of the recorded reports data is erased when you turn off the Contivity 221.

Viewing Web Site Hits

In the Reports screen, select **Web Site Hits** from the **Report Type** drop-down list box to have the Contivity 221 record and display which web sites have been visited the most often and how many times they have been visited.

Figure 145 Web Site Hits Report Example



The following table describes the fields in this screen.

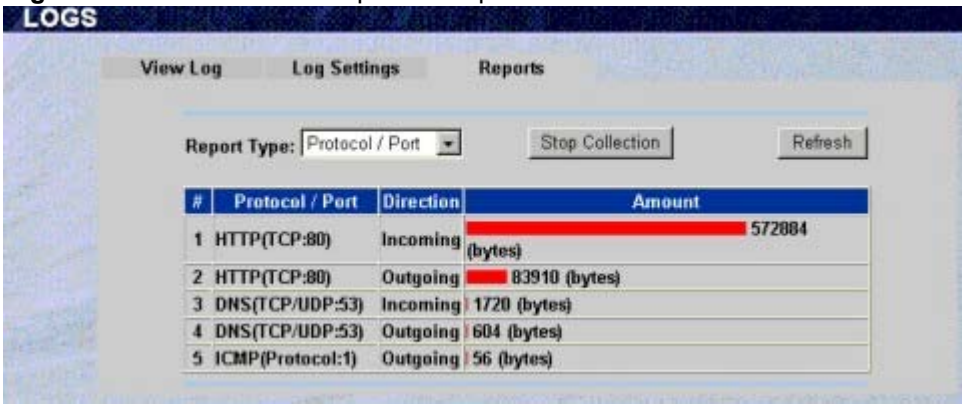
Table 96 Web Site Hits Report

Label	Description
Web Site	This column lists the domain names of the web sites visited most often from computers on the LAN. The names are ranked by the number of visits to each web site and listed in descending order with the most visited web site listed first. The Contivity 221 counts each page viewed in a web site as another hit on the web site.
Hits	This column lists how many times each web site has been visited. The count starts over at 0 if a web site passes the hit count limit.

Viewing Protocol/Port

In the **Reports** screen, select **Protocol/Port** from the **Report Type** drop-down list box to have the Contivity 221 record and display which protocols or service ports have been used the most and the amount of traffic for the most used protocols or service ports.

Figure 146 Protocol/Port Report Example



The following table describes the fields in this screen.

Table 97 Protocol/ Port Report

Label	Description
Protocol/Port	This column lists the protocols or service ports for which the most traffic has gone through the Contivity 221. The protocols or service ports are listed in descending order with the most used protocol or service port listed first.
Direction	This column lists the direction of travel of the traffic belonging to each protocol or service port listed. **Incoming** refers to traffic that is coming into the Contivity 221's LAN from the WAN. **Outgoing** refers to traffic that is going out from the Contivity 221's LAN to the WAN.
Amount	This column lists how much traffic has been sent and/or received for each protocol or service port. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see Table 99 on page 361).

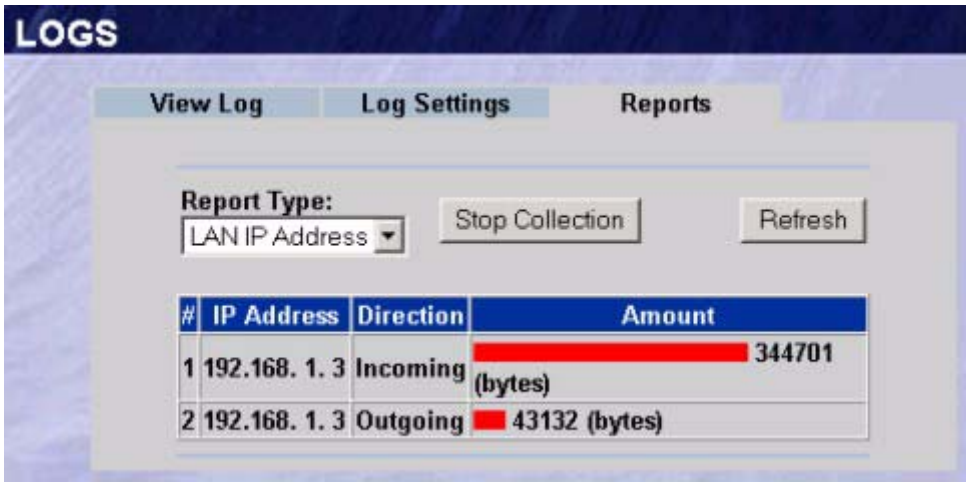
Viewing LAN IP Address

In the **Reports** screen, select **LAN IP Address** from the **Report Type** drop-down list box to have the Contivity 221 record and display the LAN IP addresses that the most traffic has been sent to and/or from and how much traffic has been sent to and/or from those IP addresses.



Note: Computers take turns using dynamically assigned LAN IP addresses. The Contivity 221 continues recording the bytes sent to or from a LAN IP address when it is assigned to a different computer.

Figure 147 LAN IP Address Report Example



The following table describes the fields in this screen.

Table 98 LAN IP Address Report

Label	Description
IP Address	This column lists the LAN IP addresses to and/or from which the most traffic has been sent. The LAN IP addresses are listed in descending order with the LAN IP address to and/or from which the most traffic was sent listed first.
Amount	This column displays how much traffic has gone to and from the listed LAN IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the LAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN IP passes the bytes count limit (see Table 99 on page 361).

Reports Specifications

The following table lists detailed specifications on the reports feature.

Table 99 Report Specifications

Label	Description
Number of web sites/protocols or ports/IP addresses listed:	20
Hit count limit:	Up to 2^{32} hits can be counted per web site. The count starts over at 0 if it passes four billion.
Bytes count limit:	Up to 2^{64} bytes can be counted per protocol/port or LAN IP address. The count starts over at 0 if it passes 2^{64} bytes.

Chapter 21
Call Scheduling Screens

Call scheduling (applicable for PPPoA or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

Call Scheduling Introduction

The call scheduling feature allows the Contivity 221 to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a video cassette recorder (you can specify a time period for the VCR to record). Apply schedule sets in the **WAN IP** screen or the **WAN Dial Backup** screen.

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Contivity 221, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets. You can apply up to four schedule sets for a remote node.

Call Schedule Summary

Click **CALL SCHEDULE** to open the **Call Schedule Summary** screen.

Figure 148 Call Schedule Summary



Table 100 Call Schedule Summary

Label	Description
#	This is the call schedule set number.
Name	This field displays the name of the call schedule set.
Active	This field shows whether the call schedule set is turned on (Yes) or off (No).
Start Date	This is the date (in year-month-day format) that the call schedule set takes effect.
Duration Date	This is the date (in year-month-day format) that the call schedule set ends.

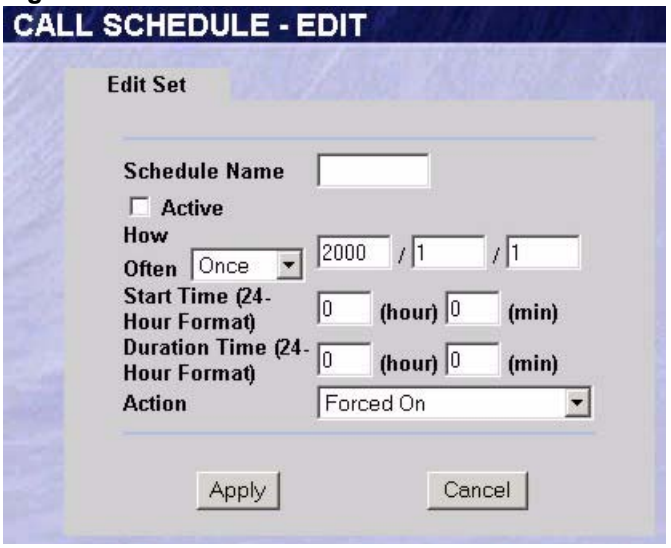
Table 100 Call Schedule Summary

Label	Description
Start Time	This is the time (in hour-minute format) when the schedule set takes effect.
Duration Time	This is the maximum length of time (in hour-minute format) that the schedule set applies the action displayed in the Action field.
Action	Forced On means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the Duration field. Forced Down means that the connection is blocked whether or not there is a demand call on the line. Enable Dial-On-Demand means that this schedule permits a demand call on the line. Disable Dial-On-Demand means that this schedule prevents a demand call on the line.
Edit	Click Edit to change a call schedule set.
Delete	Select the a call schedule set's radio button and click Delete to remove that call schedule set.

Call Scheduling Edit

To configure a schedule set, click the **Edit** button to display the screen shown next.

Figure 149 Call Schedule Edit



If a connection has been already established, your Contivity 221 will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 101 Call Schedule Edit

Label	Description
Schedule Name	Enter a name (up to 16 characters) for the call schedule set. You can use numbers, the letters A-Z (upper or lower case) and the underscore (_) and "@" symbols.
Active	Select this check box to turn on this call schedule set. Clear this check box to turn this call schedule set off.
Start Date	Set the date (in year-month-day format) when you want this call schedule set to take effect.
How Often	Select **Once** to use this schedule set only one time. Select **Weekly** to use this schedule every week. If you select **Once**, then enter the date the set should activate in year-month-day format. If you selected **Weekly** in the **How Often** field, then select the day(s) of the week when the set should activate.
Start Time (24-Hour Format)	Enter the start time (in hour-minute format) when you want the schedule set to take effect.

Table 101 Call Schedule Edit

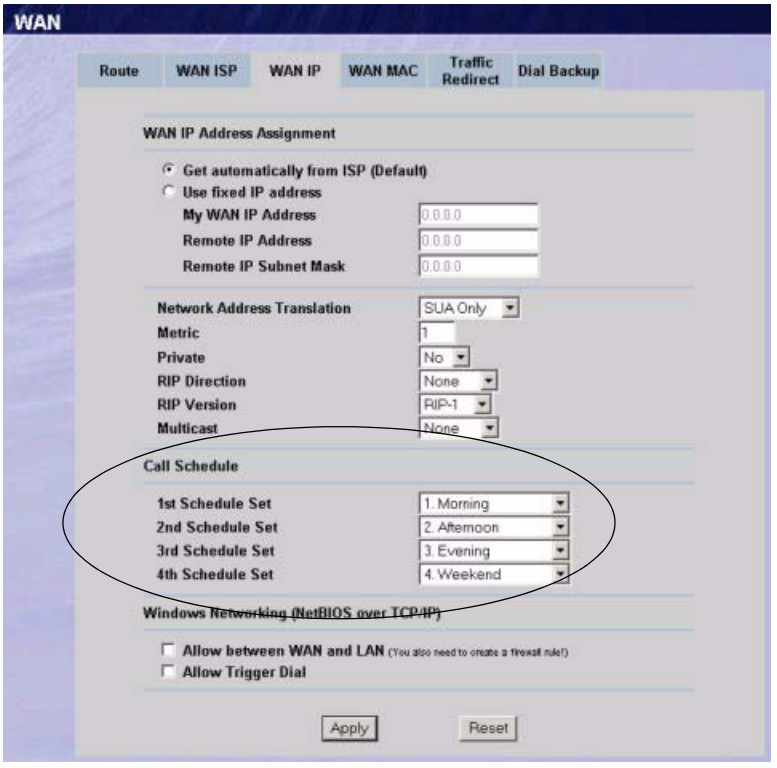
Label	Description
Duration Time (24-Hour Format)	Enter the maximum length of time (in hour-minute format) that the schedule set is to apply the action configured in the Action field. The limit is 24 hours.
Action	Select an action for the schedule set to take. **Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the Duration field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.
Apply	Click **Apply** to save your changes to the Contivity 221.
Cancel	Click **Cancel** to exit this screen without saving.

Applying Schedule Set(s) to a Remote Node

Once your schedule sets are configured, you must then apply them to the remote node. You can apply schedule sets when the Contivity 221 is set to use PPPoE or PPTP encapsulation (see the **WAN ISP** screen).

Click **WAN**, **WAN IP** to display the **WAN IP** screen as shown next. Use the screen to apply up to four schedule sets.

Figure 150 Applying Schedule Set(s) to a Remote Node



Chapter 22
Maintenance

This chapter displays system information such as firmware, port IP addresses and port traffic statistics.

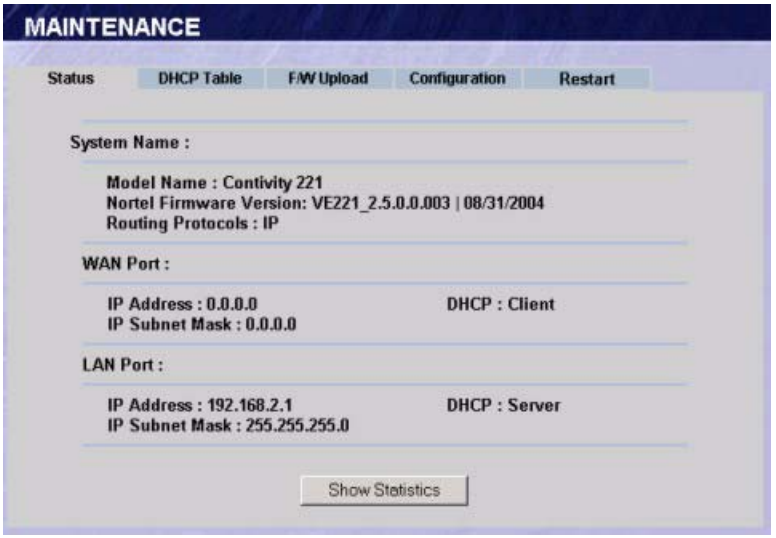
Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your Contivity 221.

Status Screen

Click **MAINTENANCE** to open the **Status** screen, where you can monitor your Contivity 221. Note that these fields are READ-ONLY and only used for diagnostic purposes.

Figure 151 System Status



The following table describes the fields in this screen.

Table 102 System Status

Label	Description
System Name	This is the **System Name** you chose in the first Internet Access Wizard screen. It is for identification purposes
Model Name	The model name identifies your device type. The model name should also be on a sticker on your device. If you are uploading firmware, be sure to upload firmware for this exact model name.
Nortel Firmware Version:	This is the Nortel Networks Firmware version and the date created.
Routing Protocols	This shows the routing protocol - **IP** for which the Contivity 221 is configured.
WAN Port	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port subnet mask.
DHCP	This is the WAN port DHCP role - **Client** or **None**.
LAN Port	
IP Address	This is the LAN port IP address.

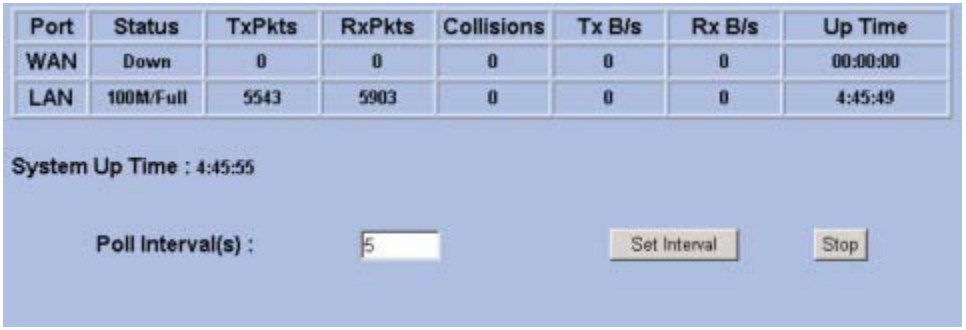
Table 102 System Status

Label	Description
IP Subnet Mask	This is the LAN port subnet mask.
DHCP	This is the LAN port DHCP role – **Server** or **None**.

System Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 152 System Status: Show Statistics



The following table describes the fields in this screen.

Table 103 System Status: Show Statistics

Label	Description
Port	This is the WAN or LAN port.
Status	This displays the port speed and duplex setting if you're using Ethernet encapsulation and **down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.

Table 103 System Status: Show Statistics

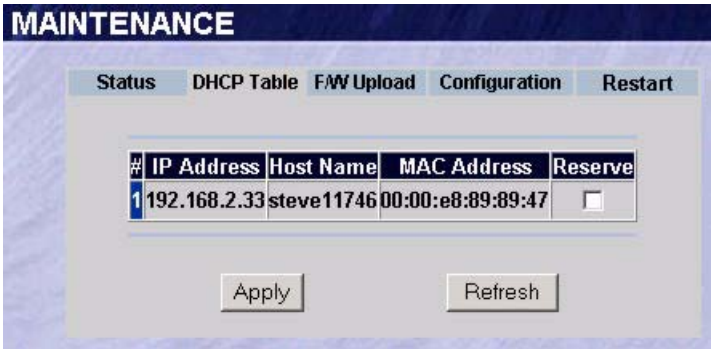
Label	Description
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the Contivity 221 has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics, click **Stop**.

DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Contivity 221 as a DHCP server or disable it. When configured as a server, the Contivity 221 provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **MAINTENANCE**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.

Figure 153 DHCP Table



The following table describes the fields in this screen.

Table 104 DHCP Table

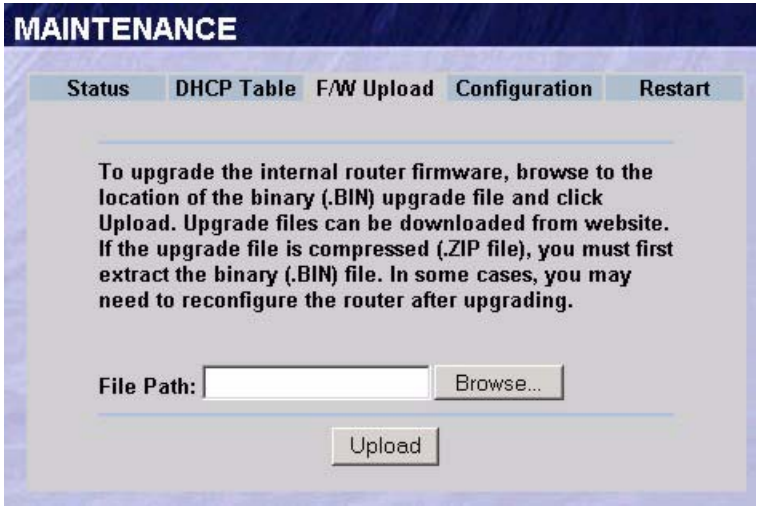
Label	Description
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click **Refresh** to renew the screen.

F/W Upload Screen

Find firmware at www.nortelnetworks.com/index.html in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "contivity221.bin". The upload process uses FTP (File Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **MAINTENANCE**, and then the **F/W UPLOAD** tab. Follow the instructions in this screen to upload firmware to your Contivity 221.

Figure 154 Firmware Upload



The following table describes the fields in this screen.

Table 105 Firmware Upload

Label	Description
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Note: Do not turn off the device while firmware upload is in progress!

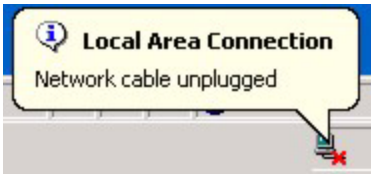
After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the device again.

Figure 155 Firmware Upload In Process



The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 156 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

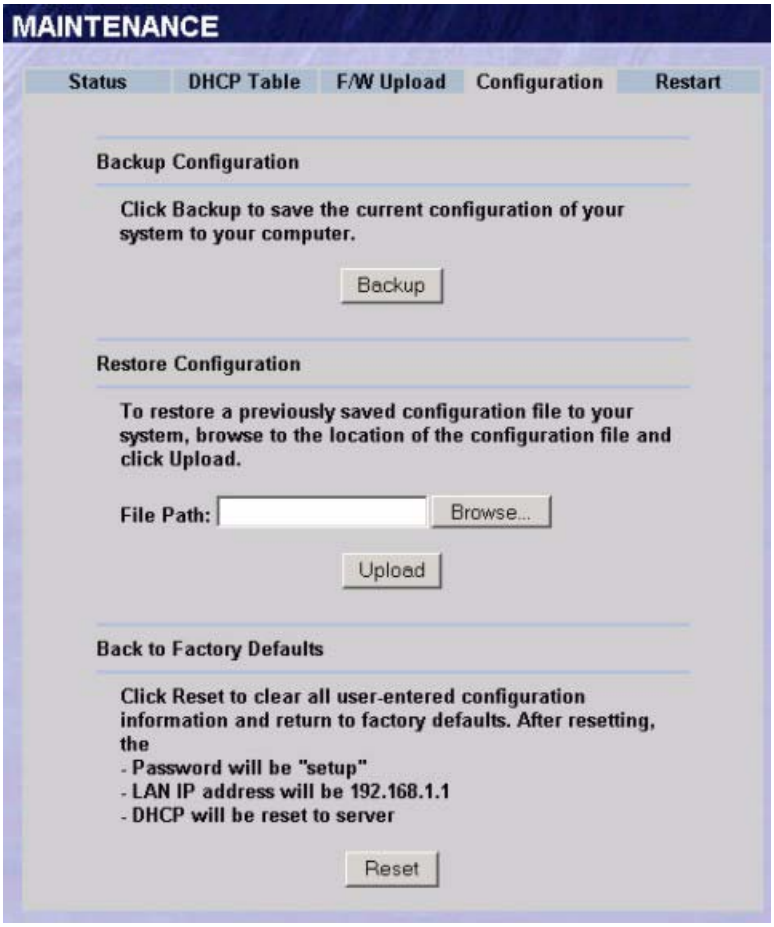
Figure 157 Firmware Upload Error



Configuration Screen

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

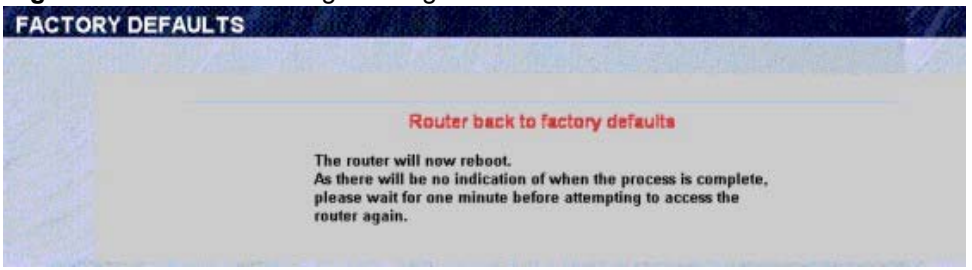
Figure 158 Configuration



Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the Contivity 221 to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 159 Reset Warning Message



You can also press the **RESET** button on the rear panel to reset the factory defaults of your Contivity 221.

Backup Configuration

Backup Configuration allows you to back up (save) the device's current configuration to a 104KB file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the device's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your Contivity 221.

Table 106 Restore Configuration

Label	Description
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Note: Do not turn off the device while configuration file upload is in progress.

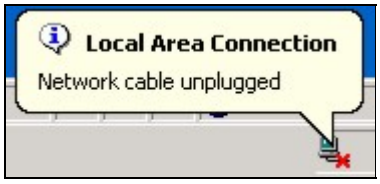
After you see a “configuration upload successful” screen, you must then wait one minute before logging into the device again.

Figure 160 Configuration Upload Successful



The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 161 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See your *Quick Start Guide* for details on how to set up your computer’s IP address.

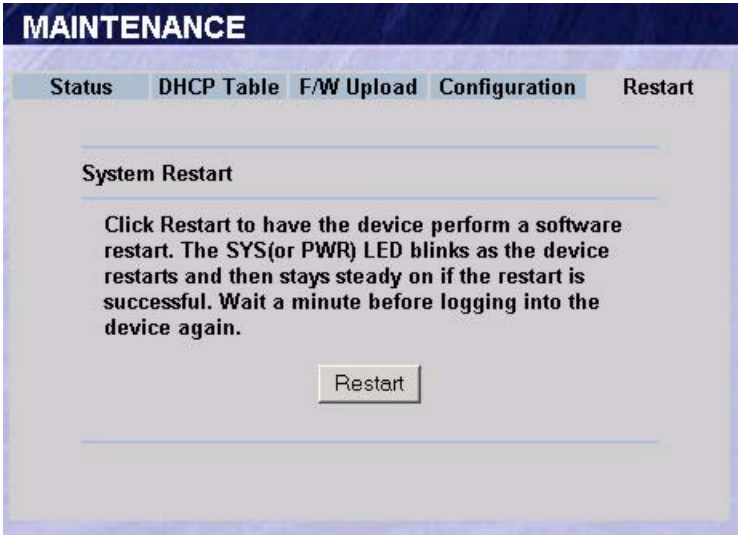
If the upload was not successful, click **Return** to go back to the **Configuration** screen.

Restart Screen

System restart allows you to reboot the Contivity 221 without turning the power off.

Click **MAINTENANCE**, and then **Restart**. Click **Restart** to have the Contivity 221 reboot. This does not affect the Contivity 221's configuration.

Figure 162 Restart Screen



Chapter 23
Introducing the SMT

This chapter explains how to access the System Management Terminal and gives an overview of its menus.

Introduction to the SMT

The Contivity 221's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus via console port, how to navigate the SMT and how to configure SMT menus.

Accessing the SMT via the Console Port

Make sure you have the physical connection properly set up as described in the hardware installation chapter.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

Initial Screen

When you turn on your Contivity 221, it performs several internal tests as well as line initialization.

After the tests, the Contivity 221 asks you to press [ENTER] to continue, as shown next.

Figure 163 Initial Screen

```
initialize ch =0, ethernet address: 00:A0:C5:22:1A:03
initialize ch =1, ethernet address: 00:A0:C5:22:1A:04
Press ENTER to continue...
```

Logging Into the SMT

The login screen appears after you press [ENTER], prompting you to enter the username, as shown below.

Type the user name (“admin” is the default) and press [ENTER].

The login screen next prompts you to enter the password

Type the password (“setup” is the default) and press [ENTER]. As you type the password, the screen displays an “X” for each character you type.

Figure 164 SMT Login

```
Enter Username : XXXX

Enter Password : XXXX
```

Please note that if there is no activity for longer than five minutes after you log in, your Contivity 221 will automatically log you out and display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

Navigating the SMT Interface

The SMT is an interface that you use to configure your Contivity 221.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 107 Main Menu Commands

Operations	Keystrokes	Descriptions
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press the [ESC] key to move back to the previous menu.
Move to a “hidden” menu	Press [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with “Edit” lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] to change **No** to **Yes**, and then press [ENTER] to go to a “hidden” menu.
Move the cursor	[ENTER] or [UP]/ [DOWN] arrow keys	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively. When you are at the top of a menu, press the [UP] arrow key to move to the bottom of a menu.
Entering information	Fill in, or press [SPACE BAR], then press [ENTER] to select from choices.	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? >	All fields with the symbol <?> must be filled in order be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message “Press ENTER to confirm or ESC to cancel”. Saving the data on the screen will take you, in most cases to the previous menu. Make sure you save your settings in each screen that you configure.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

Main Menu

After you enter the password, the SMT displays the **Contivity 221 Main Menu**, as shown next. Not all models have all the features shown.

Figure 165 Main Menu

```
Contivity 221 Main Menu

Getting Started                    Advanced Management

     1. General Setup                21. Filter and Firewall Setup
     2. WAN Setup                    22. SNMP Configuration
     3. LAN Setup                    23. System Security
     4. Internet Access Setup        24. System Maintenance
                                     26. Schedule Setup

     Advanced Applications
     11. Remote Node Setup
     12. Static Routing Setup
     14. Dial-in User Setup
     15. NAT Setup                   99.Exit

Enter Menu Selection Number:
```

The following table describes the fields in this screen.

Table 108 Main Menu Summary

No.	Menu Title	Function
1	General Setup	Use this menu to set up dynamic DNS and administrative information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN and configure the backup WAN dial-up connection.
3	LAN Setup	Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway IP address, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Configure IP static routes in this menu.
14	Dial-in User Setup	

Table 108 Main Menu Summary

No.	Menu Title	Function
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter and Firewall Setup	Configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.
23	System Security	Use this menu to change your password and enable network user authentication.
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this menu to exit (necessary for remote configuration).

Changing the System Password

Change the Contivity 221's administrator password by following the steps shown next.

1. From the main menu, enter 23 to display **Menu 23 – System Security**.
2. Enter 1 to display **Menu 23.1 – System Security – Change Password** as shown next.
3. Type your existing system password in the **Old Password** field, and press [ENTER].

Figure 166 Menu 23.1 System Security: Change Password

```
Menu 23.1 - System Security - Change Password
   Old Password= ****
   New Password= ?
   Retype to confirm= ?
    Enter here to CONFIRM or ESC to CANCEL:
```

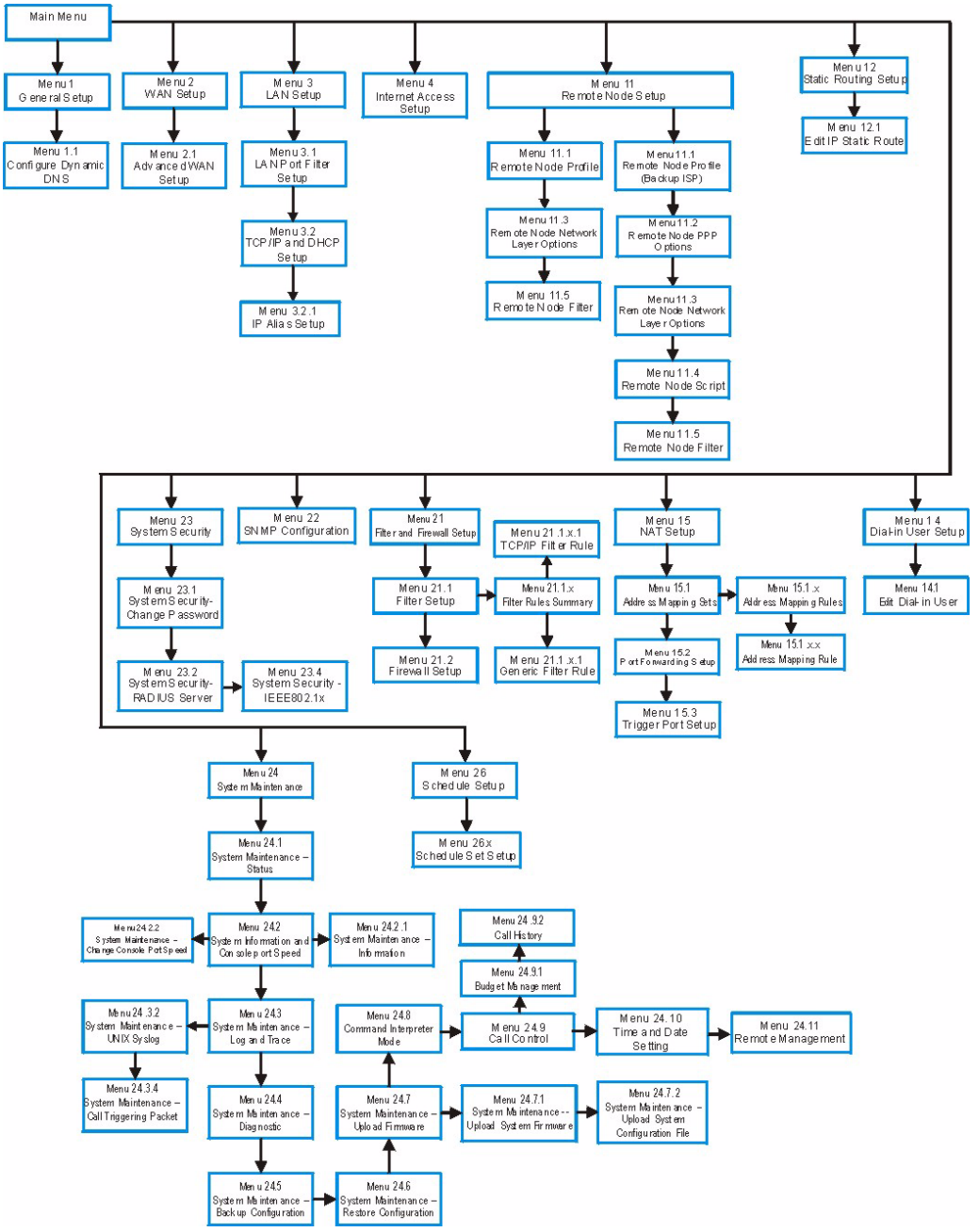
4. Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].

5 Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note that as you type a password, the screen displays an asterisk "*" for each character you type.

SMT Menus at a Glance

Figure 167 SMT Overview



Resetting the Contivity 221

See the chapter that introduces the WebGUI for directions on resetting the Contivity 221.

Chapter 24
SMT Menu 1 - General Setup

Menu 1 - General Setup contains administrative and system-related information.

Introduction to General Setup

Menu 1 - General Setup contains administrative and system-related information.

Configuring General Setup

Enter 1 in the main menu to open **Menu 1: General Setup**.

The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields.

Figure 168 Menu 1: General Setup

```
Menu 1 - General Setup

System Name= Contivity
Domain Name= www.nortelnetworks.com
First System DNS Server= From ISP
        IP Address= N/A
   Second System DNS Server= From ISP
IP Address= N/A
Third System DNS Server= From ISP
     IP Address= N/A
Edit Dynamic DNS= No
```

Press ENTER to Confirm or ESC to Cancel:

The following table describes the fields in this screen.

Table 109 General Setup Menu Fields

Field	Description	Example
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	Contivity 221
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router. The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].	nortelnetworks.com

Table 109 General Setup Menu Fields

Field	Description	Example
First System DNS Server Second System DNS Server Third System DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The Contivity C221 uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Press [SPACE BAR] and then [ENTER] to select an option. Select **From ISP** if your ISP dynamically assigns DNS server information (and the Contivity C221's WAN IP address). The **IP Address** field below displays the (read-only) DNS server IP address that the ISP assigns. If you chose **From ISP**, but the Contivity C221 has a fixed WAN IP address, **From ISP** changes to **None** after you save your changes. If you select **From ISP** for the second or third DNS server, but the ISP does not provide a second or third IP address, **From ISP** changes to **None** after you save your changes. Select **User-Defined** if you have the IP address of a DNS server. The IP address can be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right. A **User-Defined** entry with the IP address set to 0.0.0.0 changes to **None** after you save your changes. A duplicate **User-Defined** entry changes to **None** after you save your changes. Select **None** if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server. Select **Private DNS** if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right. With a private DNS server, you must also configure the first DNS server entry in SMT menu 3.1 to use **DNS Relay**.	

Table 109 General Setup Menu Fields

Field	Description	Example
	You must also configure a VPN branch office rule since the Contivity 221 uses a VPN tunnel when it relays DNS queries to the private DNS server. One of the rule's IP policies must include the LAN IP address of the Contivity 221 as a local IP address and the IP address of the DNS server as a remote IP address. A **Private DNS** entry with the IP address set to 0.0.0.0 changes to **None** after you click **Apply**. A duplicate **Private DNS** entry changes to **None** after you save your changes.	
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1: Configure Dynamic DNS** discussed next.	**No** (default)
	When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

Configuring Dynamic DNS

To configure Dynamic DNS, go to **Menu 1: General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** (shown next). Not all models have every field shown.

Figure 169 Configure Dynamic DNS

```
Menu 1.1 - Configure Dynamic DNS

 Service Provider= WWW.DynDNS.ORG
     Active= No
     DDNS Type= DynamicDNS
     Host Name 1=
     Host Name 2=
     Host Name 3=
     Username=
     Password= ********
     Enable Wildcard Option= No
     Enable Off Line Option= N/A
     IP Address Update Policy:
       DDNS Server Auto Detect IP Address= No
       Use Specified IP Address= No
       Use IP Address= N/A
Press ENTER to confirm or ESC to cancel:
```

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 110 Configure Dynamic DNS Menu Fields

Field	Description	Example
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.	Yes
DDNS Type	Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have a dynamic IP address(es). Select **StaticDNS** if you have a static IP address(s). Select **CustomDNS** to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.	**DynamicDNS** (default)
Host1-3	Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
User	Enter your user name.	
Password	Enter the password assigned to you.	

Table 110 Configure Dynamic DNS Menu Fields

Field	Description	Example
Enable Wildcard	Your Contivity 221 supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** This field is **N/A** when you choose DDNS client as your service provider.	No
Offline	This field is only available when **CustomDNS** is selected in the **DDNS Type** field. Press [SPACE BAR] and then [ENTER] to select **Yes**. When **Yes** is selected, http://www.dyndns.org/traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details).	Yes
IP Address Update Policy:	You can select **Yes** in either the **DDNS Server Auto Detect IP Address** field (recommended) or the **Use Specified IP Address** field, but not both. With the **DDNS Server Auto Detect IP Address** and **Use Specified IP Address** fields both set to **No**, the DDNS server automatically updates the IP address of the host name(s) with the Contivity 221's WAN IP address. DDNS does not work with a private IP address. When both fields are set to **No**, the Contivity 221 must have a public WAN IP address in order for DDNS to work.	
DDNS Server Auto Detect IP Address	Press [SPACE BAR] to select **Yes** and then press [ENTER] to have the DDNS server automatically update the IP address of the host name(s) with the public IP address that the Contivity 221 uses or is behind. You can set this field to **Yes** whether the IP address is public or private, static or dynamic.	Yes
Use Specified IP Address	Press [SPACE BAR] to select **Yes** and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below. Only select **Yes** if the Contivity 221 uses or is behind a static public IP address.	No
Use IP Address	Enter the static public IP address if you select **Yes** in the **Use Specified IP Address** field.	N/A
	When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

The IP address updates when you reconfigure menu 1 or perform DHCP client renewal.

Chapter 25
WAN and Dial Backup Setup

This chapter describes how to configure the WAN using menu 2 and dial-backup using menus 2.1 and 11.1.

Introduction to WAN and Dial Backup Setup

This chapter explains how to configure settings for your WAN port and how to configure the Contivity 221 for a dial backup connection.

WAN Setup

From the main menu, enter 2 to open menu 2

Figure 170 Menu 2.

```
                Menu 2 - WAN Setup
          MAC Address:
            Assigned By= Factory default
            IP Address= N/A
          Dial-Backup:
            Active= No
            Phone Number=
            Port Speed= 115200
            AT Command String:
              Init= at&fs0=0
            Edit Advanced Setup= No
        Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

The following table describes the fields in this screen.

Table 111 MAC Address Cloning in WAN Setup

Field	Description	Example
MAC Address		
Assigned By	Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose **Factory Default** to select the factory assigned default MAC Address. Choose **IP address attached on LAN** to use the MAC Address of that workstation whose IP you give in the following field.	IP address attached on LAN
IP Address	This field is applicable only if you choose the **IP address attached on LAN** method in the **Assigned By** field. Enter the IP address of the computer on the LAN whose MAC you are cloning.	192.168.1.35
	When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

Dial Backup

The Dial Backup port or CON/AUX port can be used in reserve, as a traditional dial-up connection should the broadband connection to the WAN port fail. This feature is not available on all models. To set up the auxiliary port (Dial Backup or CON/AUX) for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection (see the Hardware Installation chapter), then configure

- Menu 2 - WAN Setup,
- Menu 2.1 - Advanced WAN Setup and
- Menu 11.1 - Remote Node Profile (Backup ISP) as shown next

Refer also to the traffic redirect section for information on an alternate backup WAN connection.

Configuring Dial Backup in Menu 2

From the main menu, enter 2 to open menu 2.

Figure 171 Menu 2: Dial Backup Setup

```
                    Menu 2 - WAN Setup
                MAC Address:
                  Assigned By= Factory default
                  IP Address= N/A
                Dial-Backup:
                  Active= No
                  Phone Number=
                  Port Speed= 115200
                  AT Command String:
                    Init= at&fs0=0
                  Edit Advanced Setup= No
            Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

The following table describes the fields in this screen.

Table 112 Menu 2: Dial Backup Setup

Field	Description	Example
Dial-Backup:		
Active	Use this field to turn the dial-backup feature on (**Yes**) or off (**No**).	No
Phone Number	Enter the telephone number assigned to your line by your telephone company. This field only accepts digits; do not include dashes and spaces.	1234567
Port Speed	Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.	115200
AT Command String:		
Init	Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.	at&fs0=0

Table 112 Menu 2: Dial Backup Setup

Field	Description	Example
Edit Advanced Setup	To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 2.1: Advanced Setup**.	Yes
	When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

Advanced WAN Setup

Note: Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands

To edit the advanced setup for the Dial Backup port, move the cursor to the **Edit Advanced Setup** field in

Menu 2 - WAN Setup, press the [SPACE BAR] to select **Yes** and then press [ENTER].

Figure 172 Menu 2.1 Advanced WAN Setup

```
          Menu 2.1 - Advanced WAN Setup
AT Command Strings:                  Call Control:
  Dial= atdt                           Dial Timeout(sec)= 60
  Drop= ~~+++~~ath                     Retry Count= 0
  Answer= ata                          Retry Interval(sec)= N/A
                                       Drop Timeout(sec)= 20
Drop DTR When Hang Up= Yes             Call Back Delay(sec)= 15
AT Response Strings:
  CLID= NMBR =
  Called Id=
  Speed= CONNECT
              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes fields in this menu.

Table 113 Advanced WAN Port Setup: AT Commands Fields

Field	Description	Default
AT Command Strings:		
Dial	Enter the AT Command string to make a call.	atdt
Drop	Enter the AT Command string to drop a call. “~” represents a one second wait, e.g., “~~~+++~~ath” can be used if your modem has a slow response time.	+++ath
Answer	Enter the AT Command string to answer a call.	ata
Drop DTR When Hang Up	Press the [SPACE BAR] to choose either **Yes** or **No**. When **Yes** is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the “AT Command String: Drop” is sent out.	Yes
AT Response String:		
CLID (Calling Line Identification)	Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the Contivity 221 capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR =

Table 113 Advanced WAN Port Setup: AT Commands Fields

Field	Description	Default
Called Id	Enter the keyword preceding the dialed number.	TO
Speed	Enter the keyword preceding the connection speed.	CONNECT

Table 114 Advanced WAN Port Setup: Call Control Parameters

Field	Description	Default
Call Control		
Dial Timeout (sec)	Enter a number of seconds for the Contivity 221 to keep trying to set up an outgoing call before timing out (stopping). The Contivity 221 times out and stops if it cannot set up an outgoing call within the timeout value.	60 seconds
Retry Count	Enter a number of times for the Contivity 221 to retry a busy or no-answer phone number before blacklisting the number.	0 to disable the blacklist control
Retry Interval (sec)	Enter a number of seconds for the Contivity 221 to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.	
Drop Timeout (sec)	Enter a number of seconds for the Contivity 221 to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.	20 seconds
Call Back Delay (sec)	Enter a number of seconds for the Contivity 221 to wait between dropping a callback request call and dialing the co-responding callback call.	15 seconds

Remote Node Profile (Backup ISP)

Enter **2** in **Menu 11 Remote Node Setup** to open **Menu 11.2 Remote Node Profile (Backup ISP)** (shown below) and configure the setup for your Dial Backup port connection. This feature is not available on all models.

Figure 173 Menu 11.2 Remote Node Profile (Backup ISP)

```
          Menu 11.2 - Remote Node Profile (Backup ISP)
Rem Node Name= ?                      Edit PPP Options= No
Active= Yes                           Rem IP Addr= 0.0.0.0
                                      Edit IP= No
Outgoing:                             Edit Script Options= No
  My Login=
  My Password= ********               Telco Option:
  Authen= CHAP/PAP                      Allocated Budget(min)= 0
  Pri Phone #= ?                          Period(hr)= 0
                                        Schedules=
  Sec Phone #=                          Nailed-Up Connection= No
                                      Session Options:
                                        Edit Filter Sets= No
                                        Idle Timeout(sec)= 100
              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 115 Fields in Menu 11.2 Remote Node Profile (Backup ISP)

Field	Description	Example
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the remote node or **No** to disable the remote node.	Yes
Outgoing		
My Login	Enter the login name assigned by your ISP for this remote node.	jim
My Password	Enter the password assigned by your ISP for this remote node.	*****

Table 115 Fields in Menu 11.2 Remote Node Profile (Backup ISP)

Field	Description	Example
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** - Your Contivity 221 will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.	CHAP/PAP
Pri Phone # Sec Phone #	Enter the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your Contivity 221 dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.	
Edit PPP Options	Move the cursor to this field and use the space bar to select [Yes] and press [Enter] to edit the PPP options for this remote node. This brings you to **Menu 11.2.1 - Remote Node PPP Options** (see “Editing PPP Options”).	**No** (default)
Rem IP Addr	Leave the field set to 0.0.0.0 (default) if the remote gateway has a dynamic IP address. Enter the remote gateway’s IP address here if it is static.	0.0.0.0 (default)
Edit IP	This field leads to a “hidden” menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.2.2 - Remote Node Network Layer Options**. Please see “Editing TCP/IP Options” for more information.	**No** (default)
Edit Script Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the dial backup remote node (**Menu 11.2.3 - Remote Node Script**). Please see “Editing Login Script” for more information.	**No** (default)
Telco Option		
Allocated Budget	Enter the maximum number of minutes that this remote node may be called within the time period configured in the **Period** field. The default for this field is 0 meaning there is no budget control and no time limit for accessing this remote node.	0 (default)
Period(hr)	Enter the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour).	0 (default)

Table 115 Fields in Menu 11.2 Remote Node Profile (Backup ISP)

Field	Description	Example
Schedules	You can apply up to four schedule sets here. For more details please refer to Chapter 41 Call Scheduling.	1,3,5
Nailed-Up Connection	Press [SPACE BAR] to select **Yes** to set this connection to always be on, regardless of whether or not there is any traffic. Select **No** to have this connection act as a dial-up connection.	**No** (default)
Session Options		
Edit Filter sets	This field leads to another “hidden” menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.2.4 to edit the filter sets. See “Remote Node Filter for more details.	**No** (default)
Idle Timeout	Enter the number of seconds of idle time (when there is no traffic from the Contivity 221 to the remote node) that can elapse before the Contivity 221 automatically disconnects the PPP connection. This option only applies when the Contivity 221 initiates the call.	100 seconds (default)
	Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

Editing PPP Options

The Contivity 221’s dial back-up feature uses PPP. To edit the remote node PPP options, move the cursor to the **[Edit PPP Options]** field in **Menu 11.2 - Remote Node Profile**, and use the space bar to select **[Yes].** Press [Enter] to open **Menu 11.2.1** as shown next.

Figure 174 Menu 11.2.1: Remote Node PPP Options

```
Menu 11.2.1 - Remote Node PPP Options

                    Encapsulation= Standard PPP

                    Compression= No

                     Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

This table describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

Table 116 Remote Node PPP Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then [ENTER] to select **CISCO PPP** if your Dial Backup WAN device uses Cisco PPP encapsulation, otherwise select **Standard PPP**.	**Standard PPP** (default)
Compression	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable or **No** to disable Stac compression.	**No** (default)

Editing TCP/IP Options

Move the cursor to the **Edit IP** field in menu 11.2, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.2.2 - Network Layer Options**.

Figure 175 Menu 11.2.2: Remote Node Network Layer Options

```
Menu 11.2.2 - Remote Node Network Layer Options
                    IP Address Assignment= Dynamic
                    Rem IP Addr= 0.0.0.0
                    Rem Subnet Mask= 0.0.0.0
                    My WAN Addr= 0.0.0.0

                    Network Address Translation= None
                    Metric= 15
                    Private= No
                    RIP Direction= Both
                      Version= RIP-2B
                    Multicast= None

                     Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this screen.

Table 117 Remote Node Network Layer Options Menu Fields

Field	Description	Example
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields.	**Dynamic** (default)
Rem IP Address	Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Enter the remote gateway's IP address here if you know it (static).	0.0.0.0 (default)
Rem Subnet Mask	Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Enter the remote gateway's subnet mask here if you know it (static).	0.0.0.0 (default)
My WAN Addr	Leave the field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Enter your WAN IP address here if you know it (static). This is the address assigned to your local Contivity 221, not the remote router.	0.0.0.0 (default)

Table 117 Remote Node Network Layer Options Menu Fields

Field	Description	Example
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Press [SPACE BAR] and then [ENTER] to select either **Full Feature, None** or **SUA Only.** Choose **None** to disable NAT**.** Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set! See the Network Address Translation (NAT) chapter for a full discussion on this feature.	**None** (default)
Metric	Enter a number from 1 to 15 to set this route's priority among the Contivity 221's routes. The smaller the number, the higher priority the route has.	15 (default)
Private	This parameter determines if the Contivity 221 will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	No (default)
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the **RIP direction** from **Both/ None**/**In Only**/**Out Only** and **None**.	**Both** (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	RIP-1
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The Contivity 221 supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See the LAN Setup chapter for more information on this feature.	**None** (default)
	Once you have completed filling in **Menu 11.2.2 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11.2, or press [ESC] at any time to cancel.	

Editing Login Script

For some remote gateways, text login is required before PPP negotiation is started. The Contivity 221 provides a script facility for this purpose. The script has six programmable sets; each set is composed of an ‘Expect’ string and a ‘Send’ string. After matching a message from the server to the ‘Expect’ field, the Contivity 221 returns the set’s ‘Send’ string to the server.

For instance, a typical login sequence starts with the server printing a banner, a login prompt for you to enter the user name and a password prompt to enter the password:

```
Welcome to Acme, Inc.
Login: myLogin
Password:
```

To handle the first prompt, you specify “ogin: ” as the ‘Expect’ string and “myLogin” as the ‘Send’ string in set 1. The reason for leaving out the leading “L” is to avoid having to know exactly whether it is upper or lower case. Similarly, you specify “word: ” as the ‘Expect’ string and your password as the ‘Send’ string for the second prompt in set 2.

You can use two variables, $USERNAME and $PASSWORD (all UPPER case), to represent the actual user name and password in the script, so they will not show in the clear. They are replaced with the outgoing login name and password in the remote node when the Contivity 221 sees them in a ‘Send’ string. Please note that both variables must been entered exactly as shown. No other characters may appear before or after, either, i.e., they must be used alone in response to login and password prompts.

Please note that the ordering of the sets is significant, i.e., starting from set 1, the Contivity 221 will wait until the ‘Expect’ string is matched before it proceeds to set 2, and so on for the rest of the script. When both the ‘Expect’ and the ‘Send’ fields of the current set are empty, the Contivity 221 will terminate the script processing and start PPP negotiation. This implies two things: first, the sets must be contiguous; the sets after an empty one are ignored. Second, the last set should match the final message sent by the server. For instance, if the server prints:

login successful.

```
Starting PPP...
```

after you enter the password, then you should create a third set to match the final “PPP...” but without a “Send” string. Otherwise, the Contivity 221 will start PPP prematurely right after sending your password to the server.

If there are errors in the script and it gets stuck at a set for longer than the “Dial Timeout” in menu 2 (default 60 seconds), the Contivity 221 will timeout and drop the line. To debug a script, go to Menu 24.4 to initiate a manual call and watch the trace display to see if the sequence of messages and prompts from the server differs from what you expect.

Figure 176 Menu 11.2.3: Remote Node Setup Script

```
Menu 11.2.3 - Remote Node Script
     Active= No

     Set 1:                                Set 5:
       Expect=                               Expect=
       Send=                                 Send=
     Set 2:                                Set 6:
       Expect=                               Expect=
       Send=                                 Send=
     Set 3:
       Expect=
       Send=
     Set 4:
       Expect=
       Send=
                     Enter here to CONFIRM or ESC to CANCEL:
Press Space Bar to Toggle.
```

The following table describes the fields in this screen.

Table 118 Menu 11.2.3: Remote Node Script Menu Fields

Field	Description	Example
Active	Press [SPACE BAR] and then [ENTER] to select either **Yes** to enable the AT strings or **No** to disable them.	No (default)
Set 1-6: Expect	Enter an Expect string to match. After matching the Expect string, the Contivity 221 returns the string in the **Send** field.	
Set 1-6: Send	Enter a string to send out after the Expect string is matched.	0.0.0.0

Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.2, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.2.4 - Remote Node Filter**.

Use menu 11.2.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Contivity 221 to prevent certain packets from triggering calls. You can specify up to four filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. Please refer to the *Filters* chapter for more information on defining the filters.

Figure 177 Menu 11.2.4: Dial Backup Remote Node Filter

```
Menu 11.2.4 - Remote Node Filter


                    Input Filter Sets:
                      protocol filters=
                        device filters=
                    Output Filter Sets:
                      protocol filters=
                        device filters=
                    Call Filter Sets:
                      protocol filters=
                        device filters=


                     Enter here to CONFIRM or ESC to CANCEL:
```

Chapter 26
LAN Setup

This chapter describes how to configure the LAN using **Menu 3: LAN Setup**.

Introduction to LAN Setup

This chapter describes how to configure the Contivity 221 for LAN connections.

Accessing the LAN Menus

From the main menu, enter 3 to open **Menu 3 – LAN Setup**

Figure 178 Menu 3: LAN Setup.

```
Menu 3 - LAN Setup

                    1. LAN Port Filter Setup
                    2. TCP/IP and DHCP Setup
                          Enter Menu Selection Number:
```

LAN Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to the LAN traffic. You seldom need to filter the LAN traffic, however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

Figure 179 Menu 3.1: LAN Port Filter Setup

```
Menu 3.1 - LAN Port Filter Setup
Input Filter Sets:
  protocol filters=
    device filters=
Output Filter Sets:
  protocol filters=
    device filters=
Press ENTER to Confirm or ESC to Cancel:
```

TCP/IP and DHCP Ethernet Setup Menu

From the main menu, enter 3 to open **Menu 3 - LAN Setup** to configure TCP/IP (RFC 1155) and DHCP Ethernet setup.

Figure 180 Menu 3: TCP/IP and DHCP Setup

```
                Menu 3 - LAN Setup


     1. LAN Port Filter Setup
     2. TCP/IP and DHCP Setup
           Enter Menu Selection Number:
```

From menu 3, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2: TCP/IP and DHCP Ethernet Setup**, as shown next.

Figure 181 Figure 21-4 Menu 3.2: TCP/IP and DHCP Ethernet Setup

```
                Menu 3.2 - TCP/IP and DHCP Ethernet Setup


     DHCP= Server                          TCP/IP Setup:
     Client IP Pool:
       Starting Address= 192.168.1.33      IP Address= 192.168.1.1
       Size of Client IP Pool= 32          IP Subnet Mask= 255.255.255.0
     First DNS Server= From ISP            RIP Direction= Both
       IP Address= N/A                       Version= RIP-1
     Second DNS Server= From ISP           Multicast= None
       IP Address= N/A                     Edit IP Alias= No
     Third DNS Server= From ISP
       IP Address= N/A


                    Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Follow the instructions in the next table on how to configure the DHCP fields.

Table 119 DHCP Ethernet Setup Menu Fields

Field	**Description**	**Example**
DHCP	This field enables/disables the DHCP server. If set to **Server**, your Contivity 221 will act as a DHCP server. If set to **None**, the DHCP server will be disabled. When set to **Server**, the following items need to be set:	Server
Configuration: Client IP Pool Starting Address	 This field specifies the first of the contiguous addresses in the IP address pool.	 192.168.1.33

Table 119 DHCP Ethernet Setup Menu Fields

Field	Description	Example
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.	32
First DNS Server Second DNS Server Third DNS Server	The Contivity C221 passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. Select **From ISP** if your ISP dynamically assigns DNS server information (and the Contivity C221's WAN IP address). The **IP Address** field below displays the (read-only) DNS server IP address that the ISP assigns. If you chose **From ISP**, but the Contivity C221 has a fixed WAN IP address, **From ISP** changes to **None** after you save your changes. If you chose **From ISP** for the second or third DNS server, but the ISP does not provide a second or third IP address, **From ISP** changes to **None** after save your changes. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the **IP Address** field below. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you save your changes. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you save your changes. Select **DNS Relay** to have the Contivity C221 act as a DNS proxy. The Contivity C221's LAN IP address displays in the **IP Address** field below (read-only). The Contivity C221 tells the DHCP clients on the LAN that the Contivity C221 itself is the DNS server. When a computer on the LAN sends a DNS query to the Contivity C221, the Contivity C221 forwards the query to the Contivity C221's system DNS server (configured in the **SYSTEM General** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to **None** after you save your changes. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it	

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

Table 120 LAN TCP/IP Setup Menu Fields

Field	Description	Example
TCP/IP Setup:		
IP Address	Enter the IP address of your Contivity 221 in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your Contivity 221 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Contivity 221.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**.	Both (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The Contivity 221 supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select **None** (default) to disable it.	None
Edit IP Alias	The Contivity 221 supports three logical LAN interfaces via its single physical Ethernet interface with the Contivity 221 itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 3.2.1	Yes

IP Alias Setup

You must use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next.

Figure 182 Menu 3.2.1: IP Alias Setup

```
Menu 3.2.1 - IP Alias Setup


                    IP Alias 1= No
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      RIP Direction= N/A
                        Version= N/A
                      Incoming protocol filters= N/A
                      Outgoing protocol filters= N/A
                    IP Alias 2= No
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      RIP Direction= N/A
                        Version= N/A
                      Incoming protocol filters= N/A
                      Outgoing protocol filters= N/A


                     Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

Use the instructions in the following table to configure IP Alias parameters.

Table 121 IP Alias Setup Menu Field

Field	Description	Example
IP Alias	Choose **Yes** to configure the LAN network for the Contivity 221.	Yes
IP Address	Enter the IP address of your Contivity 221 in dotted decimal notation.	192.168.1.1
IP Subnet Mask	Your Contivity 221 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Contivity 221.	255.255.255.0

Table 121 IP Alias Setup Menu Field

Field	Description	Example
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only, Out Only** or **None**.	None
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	RIP-1
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Contivity 221.	1
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Contivity 221.	2

Chapter 27
Internet Access

This chapter shows you how to configure your Contivity 221 for Internet access.

Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your Contivity 221 to access the Internet. There are three different menu 4 screens depending on whether you chose **Ethernet, PPTP** or **PPPoE Encapsulation**. Contact your ISP to determine what encapsulation type you should use.

Ethernet Encapsulation

If you choose **Ethernet** in menu 4 you will see the next screen.

Figure 183 Menu 4: Internet Access Setup (Ethernet)

```
Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Retype to Confirm= N/A
  Login Server IP= N/A

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only
Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 122 Menu 4: Internet Access Setup Menu Fields

Field	Description
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **Ethernet**. The encapsulation method influences your choices for the **IP Address** field.
Service Type	Press [SPACE BAR] and then [ENTER] to select **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method) or **RR-Telstra**. Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
	DSL users must choose the **Standard** option only. The **My Login**, **My Password** and **Login Server** fields are not applicable in this case.
My Login	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.

Table 122 Menu 4: Internet Access Setup Menu Fields

Field	Description
Retype to Confirm	Enter the password again to make sure that you have entered it correctly.
Login Server	The Contivity 221 will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address Assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose **None** to disable NAT**.** Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many-One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set! Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature.

Configuring the PPTP Client

Note: The Contivity 221 supports only one PPTP server connection at any given time.

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] and then [ENTER] in the **Encapsulation** field in **Menu 4 -Internet Access Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.

Figure 184 Internet Access Setup (PPTP)

```
Menu 4 - Internet Access Setup

        ISP's Name= ChangeMe
        Encapsulation= PPTP
          Service Type= N/A
          My Login= username
        My Password= ******
        Retype to Confirm= ******
        Idle Timeout= 100

         IP Address Assignment= Dynamic
        IP Address= N/A
        IP Subnet Mask= N/A
        Gateway IP Address=N/A
         Network Address Translation= SUA Only

                Press ENTER to Confirm or ESC to Cancel:
```

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

Table 123 New Fields in Menu 4 (PPTP) Screen

Field	Description	Example
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **PPTP**. The encapsulation method influences your choices for the **IP Address** field.	PPTP
Idle Timeout	This value specifies the time, in seconds, that elapses before the Contivity 221 automatically disconnects from the PPTP server.	100 (default)

Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see the *Appendix*.

Figure 185 Internet Access Setup (PPPoE)

```
Menu 4 - Internet Access Setup
ISP's Name= ChangeMe
Encapsulation= PPPoE
  Service Type= N/A
  My Login=
  My Password= ********
  Retype to Confirm= ******
  Idle Timeout= 100
IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= Full Feature
Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

The following table describes the fields in this screen.

Table 124 New Fields in Menu 4 (PPPoE) screen

Field	Description	Example
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **PPPoE**. The encapsulation method influences your choices in the **IP Address** field.	PPPoE
Idle Timeout	This value specifies the time in seconds that elapses before the Contivity 221 automatically disconnects from the PPPoE server.	100 (default)

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

Basic Setup Complete

Well done! You have successfully connected, installed and set up your Contivity 221 to operate on your network as well as access the Internet.



Note: When the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.

You may deactivate the firewall in menu 21.2 or via the Contivity 221 embedded WebGUI. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the *firewall chapters* for more information on the firewall.

Chapter 28
Remote Node Setup

This chapter shows you how to configure a remote node.

Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.1 Remote Node Profile, Menu 11.1.2 - Remote Node Network Layer Options** and **Menu 11.1.4 - Remote Node Filter**.

Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 Remote Node Setup** (shown below).

Then enter **1** to open **Menu 11.1 Remote Node Profile** and configure the setup for your regular ISP. Enter **2** to open **Menu 11.1 Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection.

Figure 186 Menu 11 Remote Node Setup

```
Menu 11 - Remote Node Setup


  1. ChangeMe (ISP, SUA)
  2. -GUI (BACKUP_ISP, SUA)



           Enter Node # to Edit:
```

Remote Node Profile Setup

The following explains how to configure the remote node profile menu.

Ethernet Encapsulation

There are two variations of menu 11.1 depending on whether you choose **Ethernet Encapsulation** or **PPPoE Encapsulation.** You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.

Figure 187 Menu 11.1: Remote Node Profile for Ethernet Encapsulation

```
            Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe              Route= IP
Active= Yes

Encapsulation= Ethernet              Edit IP= No
Service Type= Standard               Session Options:
Service Name= N/A                      Edit Filter Sets= No
Outgoing:
  My Login= N/A
  My Password= N/A                  Edit Traffic Redirect= No
  Retype to Confirm= N/A
  Server IP= N/A


              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 125 Fields in Menu 11.1

Field	Description	Example
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node).	Yes
Encapsulation	**Ethernet** is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to **PPPoE** or **PPTP** encapsulation.	Ethernet
Service Type	Press [SPACE BAR] and then [ENTER] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method) or **RR-Manager** (RoadRunner Manager authentication method). Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.	Standard

Table 125 Fields in Menu 11.1

Field	Description	Example
Service Name	If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here. Only valid with **PPPoE** encapsulation.	poellc
Outgoing My Login	This field is applicable for **PPPoE** encapsulation only. Enter the login name assigned by your ISP when the Contivity 221 calls this remote node. Some ISPs append this field to the **Service Name** field above (e.g., jim@poellc) to access the PPPoE server.	jim
My Password	Enter the password assigned by your ISP when the Contivity 221 calls this remote node. Valid for **PPPoE** encapsulation only.	*****
Retype to Confirm	Type your password again to make sure that you have entered it correctly.	*****
Server IP	This field is valid only when **RoadRunner** is selected in the **Service Type** field. The Contivity 221 will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.	
Route	This field refers to the protocol that will be routed by your Contivity 221.	IP
Edit IP	This field leads to a “hidden” menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to M**enu 11.1.2 - Remote Node Network Layer Options**.	**No** (default)
Session Options Edit Filter sets	This field leads to another “hidden” menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.1.4 to edit the filter sets. Please see “Remote Node Filter” section for more details.	**No** (default)
	Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

PPPoE Encapsulation

The Contivity 221 supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you’re using the Contivity 221 with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE,** then you will see the next screen. Please see the *Appendices* for more information on PPPoE.

Figure 188 Menu 11.1: Remote Node Profile for PPPoE Encapsulation

```
                    Menu 11.1 - Remote Node Profile

  Rem Node Name= ChangeMe             Route= IP
  Active= Yes

  Encapsulation= PPPoE                Edit IP= No
  Service Type= Standard              Telco Option:
 Service Name=                        Allocated Budget(min)= 0
  Outgoing:                            Period(hr)= 0
    My Login=                          Schedules=
   My Password= ********               Nailed-Up Connection= No
    Retype to Confirm= ********
    Authen= CHAP/PAP
                                       Session Options:
                                         Edit Filter Sets= No
                                         Idle Timeout(sec)= 100

                                      Edit Traffic Redirect= No

                Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes a specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter a case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The Contivity 221 does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the Contivity 221 will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

The following table describes the fields specific to PPPoE encapsulation.

Table 126 Fields in Menu 11.1 (PPPoE Encapsulation Specific)

Field	Description	Example
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** - Your Contivity 221 will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.	CHAP/PAP
Telco Option Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	0 (default)
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period(hr)** is 1 (hour).	0 (default)
Schedules	You can apply up to four call schedule sets here.	
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	**No** (default)
Session Options Idle Timeout	Type the length of idle time (when there is no traffic from the Contivity 221 to the remote node) in seconds that can elapse before the Contivity 221 automatically disconnects the PPPoE connection. This option only applies when the Contivity 221 initiates the call.	100 seconds (default)

PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see the *Appendices* for information on PPTP.

Figure 189 Menu 11.1: Remote Node Profile for PPTP Encapsulation

```
                    Menu 11.1 - Remote Node Profile

  Rem Node Name= ChangeMe             Route= IP
  Active= Yes

  Encapsulation= PPTP                 Edit IP= No
  Service Type= Standard              Telco Option:
 Service Name=                        Allocated Budget(min)= 0
  Outgoing:                            Period(hr)= 0
    My Login=                          Schedules=
   My Password= ********               Nailed-Up Connection= No
    Retype to Confirm= ********
    Authen= CHAP/PAP
   PPTP                                Session Options:
     My IP Addr=                        Edit Filter Sets= No
     My IP Mask=                        Idle Timeout(sec)= 100
     Server IP Addr=
     Connection ID/Name=              Edit Traffic Redirect= No

                Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

The next table shows how to configure fields in menu 11.1 not previously discussed.

Table 127 Fields in Menu 11.1 (PPTP Encapsulation)

Field	Description	Example
Encapsulation	Press [SPACE BAR] and then [ENTER] to select **PPTP**. You must also go to menu 11.1.2 to check the IP Address setting once you have selected the encapsulation method.	PPTP
My IP Addr	Enter the IP address of the WAN Ethernet port.	10.0.0.140
My IP Mask	Enter the subnet mask of the WAN Ethernet port.	255.255.255.0
My Server IP Addr	Enter the IP address of the ANT modem.	10.0.0.138
Connection ID/ Name	Enter the connection ID or connection name in the ANT. It must follow the “c:id” and “n:name” format. This field is optional and depends on the requirements of your DSL modem.	N:My ISP
Schedules	You can apply up to four call schedule sets here.	
Nailed-Up Connections	Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to make the connection to this remote node a nailed-up connection.	No

Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.1.2 - Network Layer Options**.

Figure 190 Menu 11.1.2: Remote Node Network Layer Options for Ethernet Encapsulation

```
Menu 11.1.2 - Remote Node Network Layer Options

  IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Addr= N/A

  Network Address Translation= SUA Only
  Metric= N/A
  Private= N/A
  RIP Direction= None
    Version= N/A
  Multicast= None

   Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this screen.

Table 128 Remote Node Network Layer Options Menu Fields

Field	Description	Example
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields.	**Dynamic** (default)
(Rem) IP Address	If you have a Static IP Assignment, enter the IP address assigned to you by your ISP.	
(Rem) IP Subnet Mask	If you have a Static IP Assignment, enter the subnet mask assigned to you.	

Table 128 Remote Node Network Layer Options Menu Fields

Field	Description	Example
Gateway IP Addr	This field is applicable to **Ethernet** encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.	
My WAN Addr	This field is applicable to **PPPoE** and **PPTP** encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your Contivity 221. Note that this is the address assigned to your local Contivity 221, not the remote router.	
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose **None** to disable NAT**.** Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set! See *Chapter 31, "Network Address Translation (NAT)* for a full discussion on this feature.	**SUA Only** (default)
Metric	Enter a number from 1 to 15 to set this route's priority among the Contivity 221's routes. The smaller the number, the higher priority the route has.	1
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the Contivity 221 will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	No
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from **Both**/ **None**/**In Only**/**Out Only**. The default for RIP on the WAN side is **None**. It is recommended that you do not change this setting.	**None** (default)

Table 128 Remote Node Network Layer Options Menu Fields

Field	Description	Example
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**/**RIP-2B**/**RIP-2M** or **None**.	N/A
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The Contivity 221 supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2)**. Press [SPACE BAR] to enable IP Multicasting or select **None** to disable it.	**None** (default)
	Once you have completed filling in **Menu 11.1.2 Remote Node Network Layer Options**, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration and return to menu 11.1, or press [ESC] at any time to cancel.	

Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.1.4-Remote Node Filter**.

Use menu 11.1.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Contivity 221 to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to Chapter 33, “Filter Configuration. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 191 Menu 11.1.4: Remote Node Filter (Ethernet Encapsulation)

```
            Menu 11.1.4 - Remote Node Filter

        Input Filter Sets:
          protocol filters=
            device filters=
        Output Filter Sets:
          protocol filters=
            device filters=

         Enter here to CONFIRM or ESC to CANCEL:
```

Figure 192 Menu 11.1.4: Remote Node Filter (PPPoE or PPTP Encapsulation)

```
  Menu 11.1.4 - Remote Node Filter
        Input Filter Sets:
          protocol filters=
            Device filters=
        Output Filter Sets:
          protocol filters=
            device filters=
        Call Filter Sets:
          protocol filters=
            Device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

To configure the parameters for traffic redirect, enter 11 from the main menu to display **Menu 11.1—Remote Node Profile** as shown next.

Figure 193 Menu 11.1: Remote Node Profile

```
                Menu 11.1 - Remote Node Profile

    Rem Node Name= ?               Route= IP
    Active= Yes

  Encapsulation= Ethernet          Edit IP= No
  Service Type= Standard           Session Options:
    Service Name= N/A               Edit Filter Sets= No
    Outgoing:
      My Login= N/A
      My Password= N/A             Edit Traffic Redirect= Yes
Retype to Confirm= N/A
Server IP= N/A

           Press ENTER to Confirm or ESC to Cancel.
```

To configure traffic redirect properties, press [SPACE BAR] to select **Yes** in the **Edit Traffic Redirect** field and then press [ENTER].

Table 129 Menu 11.1: Remote Node Profile (Traffic Redirect Field)

Field	Description	Example
Edit Traffic Redirect	Press [SPACE BAR] to select **Yes** or **No**. Select **No** (default) if you do not want to configure this feature. Select **Yes** and press [ENTER] to configure **Menu 11.1.5 — Traffic Redirect Setup**.	Yes
	Press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

Traffic Redirect Setup

Configure parameters that determine when the Contivity 221 will forward WAN traffic to the backup gateway using **Menu 11.1.5 — Traffic Redirect Setup**.

Figure 194 Menu 11.1.5: Traffic Redirect Setup

```
Menu 11.1.5 - Traffic Redirect Setup

    Active= Yes
    Configuration:
      Backup Gateway IP Address= 0.0.0.0
      Metric= 15
      Check WAN IP Address= 0.0.0.0
        Fail Tolerance= 2
        Period (sec)= 5
        Timeout (sec)= 3

Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 130 Menu 11.1.5: Traffic Redirect Setup

Field	Description	Example
Active	Press [SPACE BAR] and select **Yes** (to enable) or **No** (to disable) traffic redirect setup. The default is **No**.	Yes
Configuration: Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The Contivity 221 automatically forwards traffic to this IP address if the Contivity 221's Internet connection terminates.	0.0.0.0
Metric	Enter a number from 1 to 15 to set this route's priority among the Contivity 221's routes. The smaller the number, the higher priority the route has.	15 (default)
Check WAN IP Address	Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your Contivity 221's WAN accessibility. The Contivity 221 uses the default gateway IP address if you do not enter an IP address here. If you are using PPTP or PPPoE Encapsulation, enter "0.0.0.0" to configure the Contivity 221 to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.	0.0.0.0

Table 130 Menu 11.1.5: Traffic Redirect Setup

Field	Description	Example
Fail Tolerance	Enter the number of times your Contivity 221 may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. Two to five is usually a good number.	2
Period (sec)	Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number.	5
Timeout (sec)	Enter the number of seconds the Contivity 221 waits for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The number in this field should be less than the number in the **Period** field. Three to 50 is usually a good number. The WAN connection is considered “down” after the Contivity 221 times out the number of times specified in the **Fail Tolerance** field.	3
	When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 29
IP Static Route Setup

This chapter shows you how to configure static routes with your Contivity 221.

IP Static Route Setup

Enter 12 from the main menu. Select one of the IP static routes as shown next to configure IP static routes in menu 12. 1.

Figure 195 Menu 12: IP Static Route Setup

```
                Menu 12 - IP Static Route Setup


        1. _________
        2. _________
        3. _________
        4. _________
        5. _________
        6. _________
        7. _________
        8. _________
        9. _________
        10. _________
        11. _________
        12. _________

                  Enter selection number:
```

Now, enter the index number of the static route that you want to configure.

Figure 196 Menu 12. 1: Edit IP Static Route

```
        Menu 12.1 - Edit IP Static Route

Route #: 1
Route Name= ?
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2
                    Private= No

    Press ENTER to CONFIRM or ESC to CANCEL:
```

The following table describes the IP Static Route Menu fields.

Table 131 IP Static Route Menu Fields

Field	Description
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Contivity 221 that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Contivity 221; over the WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Enter a number from 1 to 15 to set this route's priority among the Contivity 221's routes. The smaller the number, the higher priority the route has.

Table 131 IP Static Route Menu Fields

Field	Description
Private	This parameter determines if the Contivity 221 will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
	Once you have completed filling in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.

Chapter 30
Dial-in User Setup

This chapter shows you how to create user accounts on the Contivity 221.

Dial-in User Setup

By storing user profiles locally, your Contivity 221 is able to authenticate users without interacting with a network RADIUS server.

Follow the steps below to set up user profiles on your Contivity 221.

From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.

Figure 197 Menu 14- Dial-in User Setup

```
                    Menu 14 - Dial-in User Setup

1. ________          9. ________         17. ________         25. ________
2. ________         10. ________         18. ________         26. ________
3. ________         11. ________         19. ________         27. ________
4. ________         12. ________         20. ________         28. ________
5. ________         13. ________         21. ________         29. ________
6. ________         14. ________         22. ________         30. ________
7. ________         15. ________         23. ________         31. ________
8. ________         16. ________         24. ________         32. ________

                    Enter Menu Selection Number:
```

Type a number and press [ENTER] to edit the user profile.

Figure 198 Menu 14.1- Edit Dial-in User

```
    Menu 14.1 - Edit Dial-in User

User Name= test
Active= Yes
Password= ********
Press ENTER to Confirm or ESC to Cancel:
Leave name field blank to delete profile
```

The following table describes the fields in this screen.

Table 132 Menu 14.1- Edit Dial-in User

Field	Description
User Name	Enter a username up to 31 alphanumeric characters long for this user profile. This field is case sensitive.
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
	When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.

Chapter 31
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Contivity 221.

Using NAT



Note: You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the Contivity 221.

SUA (Single User Account) Versus NAT

SUA (Single User Account) is an implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. Please *see "Address Mapping Sets"* for a detailed description of the NAT set for SUA. The Contivity 221 also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.



Note: Choose **SUA Only** if you have just one public WAN IP address for your Contivity 221.

Choose **Full Feature** if you have multiple public WAN IP addresses for your Contivity 221.

Applying NAT

You apply NAT via menus 4 or 11.1.2 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup.**

Figure 199 Menu 4: Applying NAT for Internet Access

```
Menu 4 - Internet Access Setup

        Encapsulation= Ethernet
          Service Type= Standard
          My Login= N/A
          My Password= N/A
          Login Server IP= N/A

        IP Address Assignment= Dynamic
          IP Address= N/A
          IP Subnet Mask= N/A
          Gateway IP Address= N/A
        Network Address Translation= SUA Only

        Press ENTER to Confirm or ESC to
Cancel:
```

The following figure shows how you apply NAT to the remote node in menu 11.1.

Enter 11 from the main menu.

Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.1.2 - Remote Node Network Layer Options.**

Figure 200 Menu 11.1.2: Applying NAT to the Remote Node

```
Menu 11.1.2 - Remote Node Network Layer Options

   IP Address Assignment= Dynamic
   IP Address= N/A
   IP Subnet Mask= N/A
   Gateway IP Addr= N/A

   Network Address Translation= Full Feature
   Metric= N/A
   Private= N/A
   RIP Direction= None
     Version= N/A
   Multicast= None

    Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this screen.

Table 133 Applying NAT in Menus 4 & 11.1.2

Field	Description	Options
Network Address Translation	When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - *see "Address Mapping Sets"* for further discussion). Choose **Full Feature** if you have multiple public WAN IP addresses for your Contivity 221. When you select **Full Feature** you must configure at least one address mapping set!	Full Feature
	NAT is disabled when you select this option.	None
	When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - *see "Address Mapping Sets"*). Choose **SUA Only** if you have just one public WAN IP address for your Contivity 221.	SUA Only

NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. You can see two NAT address mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.1.2, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. To configure NAT, enter 15 from the main menu to bring up the following screen.

Figure 201 Menu 15: NAT Setup

```
                Menu 15 — NAT Setup

1. Address Mapping Sets
2. Port Forwarding Setup
3. Trigger Port Setup


          Enter Menu Selection Number:
```



Note: Configure LAN IP addresses in NAT menus 15.1 and 15.2.

Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

Figure 202 Menu 15.1: Address Mapping Sets

```
Menu 15.1 — Address Mapping Sets

     1. NAT_SET
   255. SUA (read only)




       Enter Menu Selection Number:
```

SUA Address Mapping Set

Enter 255 to display the next screen (*see "SUA (Single User Account) Versus NAT")*. The fields in this menu cannot be changed.

Figure 203 Menu 15.1.255: SUA Address Mapping Rules

```
                Menu 15.1.255 - Address Mapping Rules

  Set Name= SUA

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  0.0.0.0          255.255.255.255  0.0.0.0                           M-1
 2.                                    0.0.0.0                          Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this screen.

Note: Menu 15.1.255 is read-only.

Table 134 SUA Address Mapping Rules

Field	Description	Example
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP	**Local Start IP** is the starting local IP address (ILA).	0.0.0.0

Table 134 SUA Address Mapping Rules

Field	Description	Example
Local End IP	**Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the start IP is 0.0.0.0 and the end IP is 255.255.255.255.	255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	
Type	These are the mapping types discussed above. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
	Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.	

User-Defined Address Mapping Sets

Now look at option 1 in menu 15.1. Enter 1 to bring up this menu. Look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.



Note: The entire set will be deleted if you leave the **Set Name** field blank and press [ENTER] at the bottom of the screen.

Figure 204 Menu 15.1.1: First Set

```
                    Menu 15.1.1 - Address Mapping Rules

 Set Name= NAT_SET

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.
 2
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                    Action= Edit          Select Rule=

                    Press ENTER to Confirm or ESC to Cancel:
```



Note: The **Type**, **Local** and **Global Start/End IP**s are configured in menu 15.1.1.1 (described later) and the values are displayed here.

Ordering Your Rules

Ordering your rules is important because the Contivity 221 applies the rules in the order that you specify. When a rule matches the current packet, the Contivity 221 takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9.

In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 135 Fields in Menu 15.1.1

Field	Description	Example
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.	NAT_SET
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.	Edit
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1



Note: You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.



Note: An **IP End** address must be numerically greater than its corresponding **IP Start** address.

Figure 205 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

```
 Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start=
  End  = N/A

Global IP:
  Start=
  End  = N/A



Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 136 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

Field	Description	Example
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. **Server** allows you to specify multiple servers of different types behind NAT to this computer. Please *see "Example 3: Multiple Public IP Addresses With Inside Servers"* for an example.	**One-to-One**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.	
Start	Enter the starting local IP address (ILA).	0.0.0.0
End	Enter the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.	N/A

Table 136 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

Field	Description	Example
Global IP Start	Enter the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.	0.0.0.0
End	Enter the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.	N/A
	Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.	

Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**
2. Enter 2 to go to **Menu 15.2 - NAT Server Setup**.
3. Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.
4. Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.
5. Press [ENTER] at the “Press ENTER to confirm …” prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

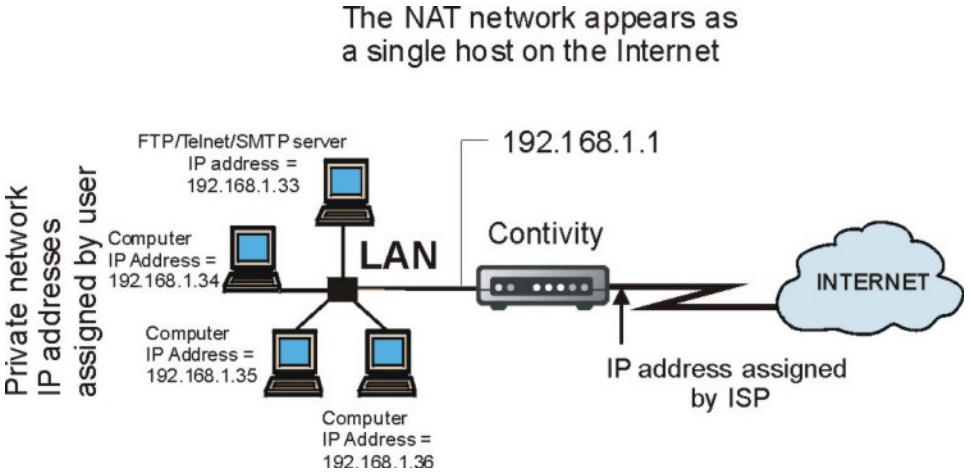
Figure 206 Menu 15.2: NAT Server Setup

```
                Menu 15.2 - NAT Server Setup


 Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------
   1.    Default          Default        0.0.0.0
   2.      21               25           192.168.1.33
   3.      0                0            0.0.0.0
   4.      0                0            0.0.0.0
   5.      0                0            0.0.0.0
   6.      0                0            0.0.0.0
   7.      0                0            0.0.0.0
   8.      0                0            0.0.0.0
   9.      0                0            0.0.0.0
  10.      0                0            0.0.0.0
  11.      0                0            0.0.0.0
  12.      1026             1026         RR Reserved

      Press ENTER to Confirm or ESC to Cancel:
```

Figure 207 Multiple Servers Behind NAT Example



General NAT Examples

The following are some examples of NAT configuration.

Internet Access Only

In the following Internet access example, you only need one rule where all your ILAs (Inside Local addresses) map to one dynamic IGA (Inside Global Address) assigned by your ISP.

Figure 208 NAT Example 1

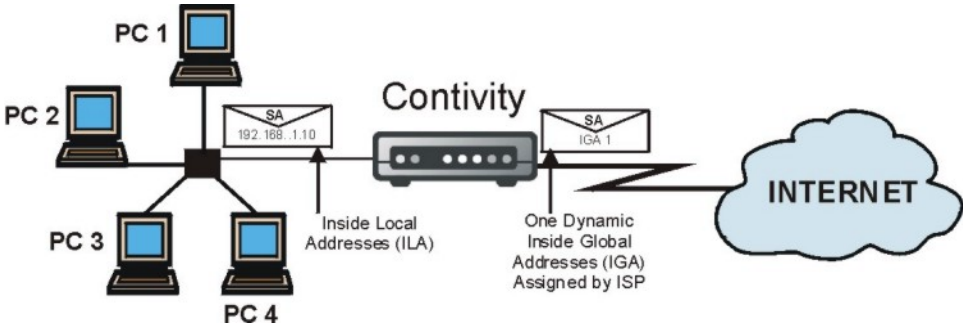


Figure 209 Menu 4: Internet Access & NAT Example

```
Menu 4 - Internet Access Setup

  ISP's Name= ChangeMe
  Encapsulation= Ethernet
  Service Type= Standard
    My Login= N/A
    My Password= N/A
    Login Server IP= N/A

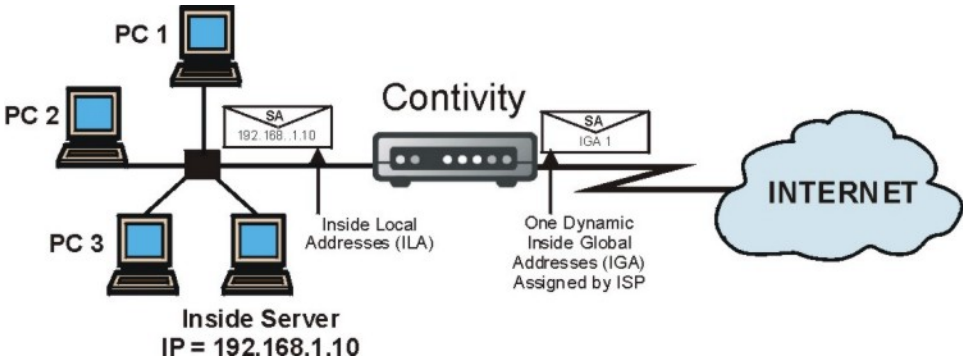
  IP Address Assignment= Dynamic
    IP Address= N/A
    IP Subnet Mask= N/A
    Gateway IP Address= N/A
  Network Address Translation= SUA Only

  Press ENTER to Confirm or ESC to Cancel:
```

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section General NAT Examples.* The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.1.2 is specifically pre-configured to handle this case.

Example 2: Internet Access with an Inside Server

Figure 210 NAT Example 2



In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

Figure 211 Menu 15.2: Specifying an Inside Server

```
                Menu 15.2 - NAT Server Setup


 Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------
   1.    Default          Default        192.168.1.10
   2.      0                0            0.0.0.0
   3.      0                0            0.0.0.0
   4.      0                0            0.0.0.0
   5.      0                0            0.0.0.0
   6.      0                0            0.0.0.0
   7.      0                0            0.0.0.0
   8.      0                0            0.0.0.0
   9.      0                0            0.0.0.0
  10.      0                0            0.0.0.0
  11.      0                0            0.0.0.0
  12.      1026             1026         RR Reserved

      Press ENTER to Confirm or ESC to Cancel:
```

Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

1 Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

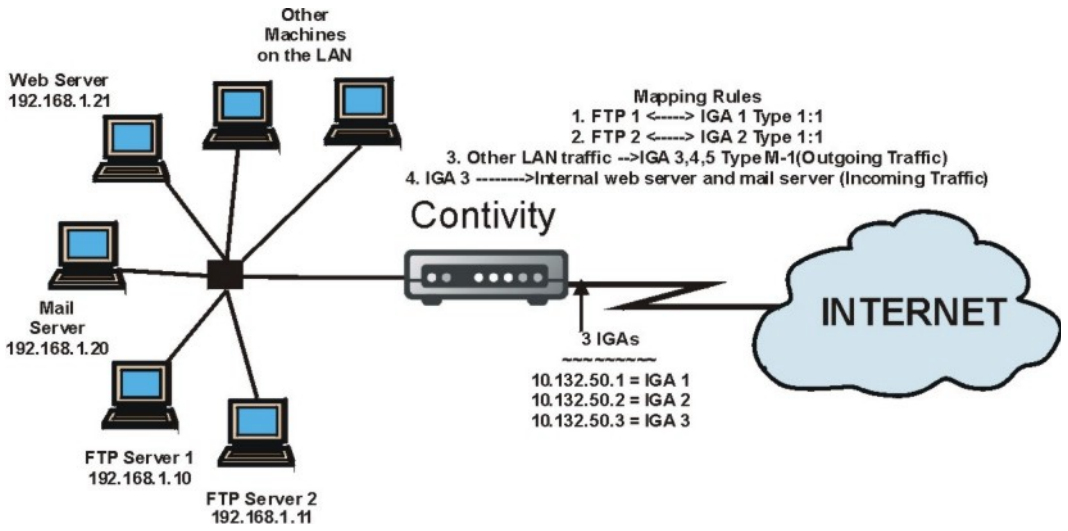
2 Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

3 Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

4 You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

Figure 212 NAT Example 3



1 In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.1.2) see Figure 213.

2 Then enter 15 from the main menu.

3 Enter 1 to configure the Address Mapping Sets.

4 Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.

5 Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (see Figure 214*)*.

6 Repeat the previous step for rules 2 to 4 as outlined above.

7 When finished, menu 15.1.1 should look like as shown in Example 3: Final Menu 15.1.1.

Figure 213 Example 3: Menu 11.1.2

```
     Menu 11.1.2 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= Full Feature
Metric= N/A
Private= N/A
RIP Direction= None
Version= N/A

         Enter here to CONFIRM or ESC to CANCEL:
```

The following figure shows how to configure the first rule.

Figure 214 Example 3: Menu 15.1.1.1

```
          Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start= 192.168.1.10
  End  = N/A

Global IP:
  Start= 10.132.50.1
  End  = N/A

              Press ENTER to Confirm or ESC to Cancel:
```

Figure 215 Example 3: Final Menu 15.1.1

```
Menu 15.1.1 - Address Mapping Rules

  Set Name= Example3

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  ------
  1. 192.168.1.10                      10.132.50.1                       1-1
  2  192.168.1.11                      10.132.50.2                       1-1
  3. 0.0.0.0           255.255.255.255  10.132.50.3                       M-1
  4.                                   10.132.50.3                      Server
  5.
  6.
  7.
  8.
  9.
 10.
                      Action= Edit          Select Rule=
```

Now configure the IGA3 to map to our web server and mail server on the LAN.

8 Enter 15 from the main menu.

9 Now enter 2 from this menu and configure it as shown in Example 3: Menu 15.2.

Figure 216 Example 3: Menu 15.2

```
                Menu 15.2 - NAT Server Setup

 Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------
   1.    Default          Default        0.0.0.0
   2.      80               80          192.168.1.21
   3.      25               25          192.168.1.20
   4.       0                0           0.0.0.0
   5.       0                0           0.0.0.0
   6.       0                0           0.0.0.0
   7.       0                0           0.0.0.0
   8.       0                0           0.0.0.0
   9.       0                0           0.0.0.0
  10.       0                0           0.0.0.0
  11.       0                0           0.0.0.0
  12.      1026             1026         RR Reserved

      Press ENTER to Confirm or ESC to Cancel:
```

Configuring Trigger Port Forwarding



Note: Only one LAN computer can use a trigger port (range) at a time.

Enter 3 in menu 15 to display **Menu 15.3 — Trigger Port Setup**, shown next.

Figure 217 Menu 15.3: Trigger Port Setup

```
                    Menu 15.3 - Trigger Port Setup

                    Incoming                Trigger
Rule    Name        Start Port   End Port   Start Port   End Port
-------------------------------------------------------------------------
    1.  Real Audio  6970         7170       7070         7070
    2.              0            0          0            0
    3.              0            0          0            0
    4.              0            0          0            0
    5.              0            0          0            0
    6.              0            0          0            0
    7.              0            0          0            0
    8.              0            0          0            0
    9.              0            0          0            0
   10.              0            0          0            0
   11.              0            0          0            0
   12.              0            0          0            0
                Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 137 Menu 15.3: Trigger Port Setup Description

Field	Description	Example
Rule	This is the rule index number.	1
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.	Real Audio
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Contivity 221 forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	6970

Table 137 Menu 15.3: Trigger Port Setup Description

Field	Description	Example
End Port	Enter a port number or the ending port number in a range of port numbers.	7170
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the Contivity 221 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	7070
End Port	Enter a port number or the ending port number in a range of port numbers.	7070
	Press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

Chapter 32
Introducing the Firewall

This chapter shows you how to get started with the firewall.

Using SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next**.**

Figure 218 Menu 21: Filter and Firewall Setup

```
 Menu 21 - Filter and Firewall Setup


1. Filter Setup
2. Firewall Setup



                Enter Menu Selection Number:
```

Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Use the WebGUI to configure firewall rules.

Figure 219 Menu 21.2: Firewall Setup

```
                Menu 21.2 - Firewall Setup

The firewall protects against Denial of Service (DoS) attacks when
it is active.

Your network is vulnerable to attacks when the firewall is turned off.

Refer to the User's Guide for details about the firewall default
policies.

You may define additional policy rules or modify existing ones but
please exercise extreme caution in doing so.

    Active: Yes

   You can use the WebGUI to configure the firewall.

            Press ENTER to Confirm or ESC to Cancel:
```



Note: Configure the firewall rules using the WebGUI or CLI commands.

Chapter 33
Filter Configuration

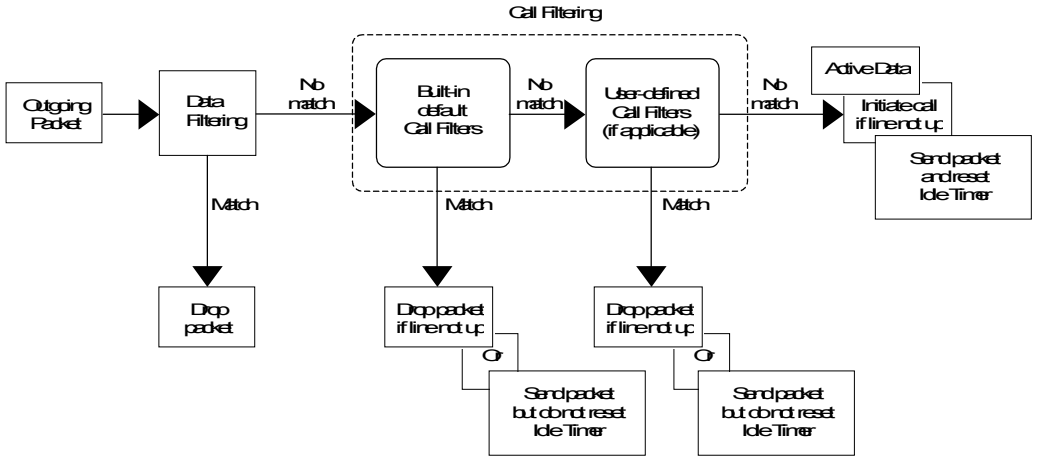
This chapter shows you how to create and apply filters.

Introduction to Filters

Your Contivity 221 uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

Figure 220 Outgoing Packet Filtering Process



For incoming packets, your Contivity 221 applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

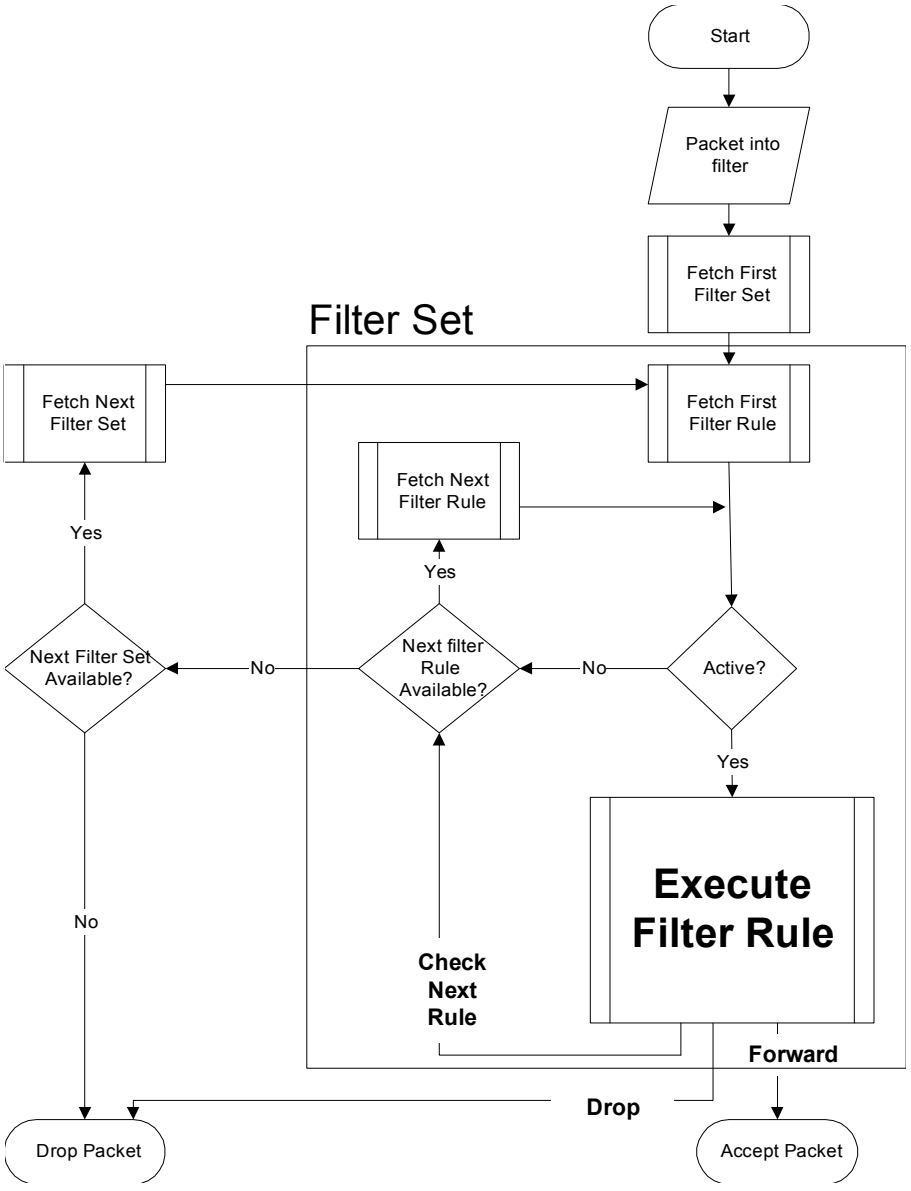
Filter Structure

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The Contivity 221 allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. Please also see Figure 225 for the logic flow when executing an IP filter.

Figure 221 Filter Rule Process



You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Configuring a Filter Set

The Contivity 221 includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

1 Enter 21 in the main menu to open menu 21.

Figure 222 Menu 21: Filter and Firewall Setup

```
Menu 21 - Filter and Firewall Setup


  1. Filter Setup
  2. Firewall Setup




                        Enter Menu Selection
Number:
```

2 Enter 1 to bring up the following menu.

Figure 223 Menu 21.1: Filter Set Configuration

```
Menu 21.1 - Filter Set Configuration

Filter                                Filter
Set #        Comments                 Set #        Comments
------  -----------------             ------  -----------------
  1      _________________               7      _________________
  2      _________________               8      _________________
  3      _________________               9      _________________
  4      _________________              10      _________________
  5      _________________              11      _________________
  6      _________________              12      _________________


                Enter Filter Set Number to Configure= 0

                Edit Comments= N/A

                Press ENTER to Confirm or ESC to Cancel:
```

3. Select the filter set you wish to configure (1-12) and press [ENTER].
4. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
5. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

Table 138 Abbreviations Used in the Filter Rules Summary Menu

Field	Description
#	The filter rule number: 1 to 6.
A	Active: “Y” means the rule is active. “N” means the rule is inactive.
Type	The type of filter rule: “GEN” for Generic, “IP” for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. “Y” means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. “N” means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N“ means to check the next rule.
n	Action Not Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 139 Rule Abbreviations Used

Abbreviation	Description
IP	
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number
GEN	

Table 139 Rule Abbreviations Used

Abbreviation	Description
Off	Offset
Len	Length

The next section provides information on configuring the filter rules.

Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the Contivity 221 will warn you and will not allow you to save.

Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 - TCP/IP Filter Rule**, as shown next.

Figure 224 Menu 21.1.1.1: TCP/IP Filter Rule

```
            Menu 21.1.1.1 - TCP/IP Filter Rule
Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0      IP Source Route= No
Destination: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 137
Port # Comp= Equal
Source: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #=
Port # Comp= None
TCP Estab= No
More= N/A             Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule
         Press ENTER to Confirm or ESC to Cancel:
               Press Space Bar to Toggle.
```

The following table describes how to configure your TCP/IP filter rule.

Table 140 TCP/IP Filter Rule Menu Fields

Field	Description	Options
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the filter rule or **No** to deactivate it.	Yes No
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.	0-255
IP Source Route	Press [SPACE BAR] and then [ENTER] to select **Yes** to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.	Yes No
Destination		
IP Address	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the **Destination: IP Addr**.	0.0.0.0

Table 140 TCP/IP Filter Rule Menu Fields

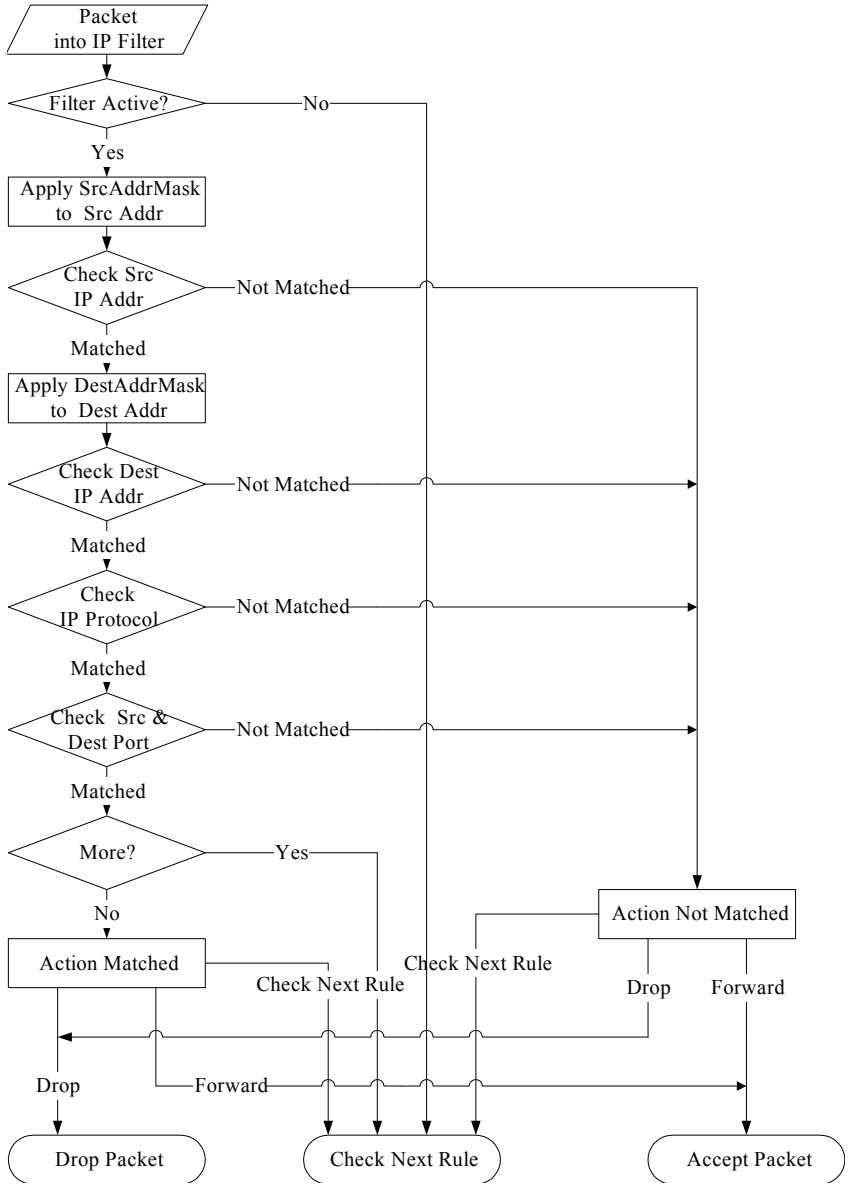
Field	Description	Options
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given **in Destination: Port #**.	None Less Greater Equal Not Equal
Source		
IP Address	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the **Source: IP Addr**.	0.0.0.0
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in **Source: Port #**.	None Less Greater Equal Not Equal
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select **Yes**, to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if **No**, it is ignored.	Yes No
More	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. If **Yes**, a matching packet is passed to the next filter rule before an action is taken; if **No**, the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	Yes No
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	None Action Matched Action Not Matched **Both**

Table 140 TCP/IP Filter Rule Menu Fields

Field	Description	Options
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.	Check Next Rule Forward Drop
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.	Check Next Rule Forward Drop
	When you have **Menu 21.1.1.1 - TCP/IP Filter Rule** configured, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.	

The following figure illustrates the logic flow of an IP filter.

Figure 225 Executing an IP Filter



Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the Contivity 221 treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The Contivity 221 applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.4.1 and press [ENTER] to open Generic Filter Rule, as shown below.

Figure 226 Menu 21.1.1.1: Generic Filter Rule

```
              Menu 21.1.1.1 - Generic Filter Rule

Filter #: 1,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No            Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

            Press ENTER to Confirm or ESC to Cancel:
                   Press Space Bar to Toggle.
```

The following table describes the fields in the Generic Filter Rule menu.

Table 141 Generic Filter Rule Menu Fields

Field	Description	Options
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.	**Generic Filter Rule** **TCP/IP Filter Rule**
Active	Select **Yes** to turn on the filter rule or **No** to turn it off.	Yes / No
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	0-255
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	0-8
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.	
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If **More** is **Yes**, then Action Matched and Action Not Matched will be **No**.	Yes No
Log	Select the logging option from the following: **None** - No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	None Action Matched Action Not Matched Both
Action Matched	Select the action for a packet matching the rule.	Check Next Rule Forward Drop

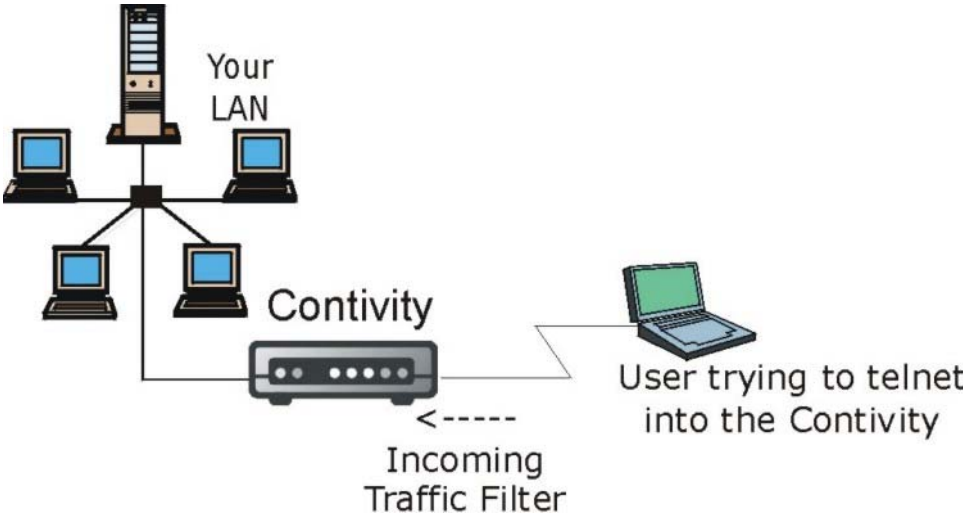
Table 141 Generic Filter Rule Menu Fields

Field	Description	Options
Action Not Matched	Select the action for a packet not matching the rule.	Check Next Rule Forward Drop
	Once you have completed filling in **Menu 21.1.1.1 - Generic Filter Rule**, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.	

Example Filter

Let's look at an example to block outside users from accessing the Contivity 221 via telnet. Please see the included disk for more example filters.

Figure 227 Telnet Filter Example



1. Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
2. Enter 1 to open **Menu 21.1 - Filter Set Configuration**.
3. Enter the index of the filter set you wish to configure (say 3) and press [ENTER].

4. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
5. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.
6. Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

Figure 228 Example Filter: Menu 21.1.3.1

```
 Menu 21.1.3.1 - TCP/IP Filter Rule

  Filter #: 3,1
  Filter Type= TCP/IP Filter Rule
  Active= Yes
  IP Protocol= 6      IP Source Route= No
  Destination: IP Addr= 0.0.0.0
               IP Mask= 0.0.0.0
               Port #= 23
               Port # Comp= Equal
       Source: IP Addr= 0.0.0.0
               IP Mask= 0.0.0.0
               Port #= 0
               Port # Comp= None
  TCP Estab= No
  More= No             Log= None
  Action Matched= Drop
  Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:
       Press Space Bar to Toggle.
```

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set. The screen shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination telnet ports (**DP = 23**). **M = N** means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

Figure 229 Example Filter Rules Summary: Menu 21.1.3

```
                    Menu 21.1.3 - Filter Rules Summary

 # A Type                       Filter Rules                              M m n
 - - ---- ------------------------------------------------------------- -
- -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                           N D F
 2 N
 3 N
 4 N
 5 N
 6 N


                Enter Filter Rule Number (1-6) to Configure: 1
```

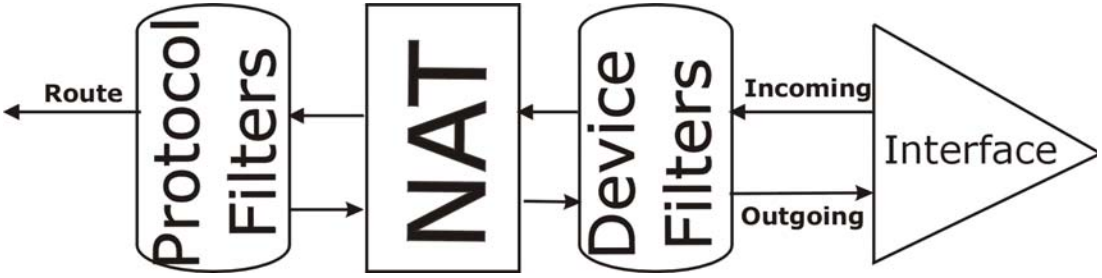
After you've created the filter set, you must apply it.

1. Enter 11 from the main menu to go to menu 11.
2. Then enter **1** to open **Menu 11.1 Remote Node Profile**.
3. Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
4. This brings you to menu 11.1.4. Apply a filter set (our example filter set 3) as shown in Figure 232.
5. Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.1.4.

Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Contivity 221 applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the Contivity 221 is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

Figure 230 Protocol and Device Filter Sets



Firewall Versus Filters

Firewall configuration is discussed in the *firewall* chapters of this manual. Further comparisons are also made between filtering, NAT and the firewall.

Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The Contivity 221 already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.



Note: If you do not activate the firewall, it is advisable to apply filters.

Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the Contivity 221 and output filter sets filter outgoing traffic from the Contivity 221. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 231 Filtering LAN Traffic

```
Menu 3.1 - LAN Port Filter Setup

 Input Filter Sets:
   protocol filters=
     device filters=
 Output Filter Sets:
   protocol filters=
     device filters=


   Ethernet Interface= 10BaseT
   Input Filter Sets=
   Output Filter Sets=


Press ENTER to Confirm or ESC to Cancel:
```

Applying Remote Node Filters

Go to menu 11.1.4 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The Contivity 221 already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

Figure 232 Filtering Remote Node Traffic

```
Menu 11.1.4 - Remote Node Filter Setup


      Input Filter Sets:
        protocol filters=
         device filters=
      Output Filter Sets:
        protocol filters=
         device filters=

Press ENTER to Confirm or ESC to Cancel:
```

Chapter 34
SNMP Configuration

This chapter explains SNMP configuration menu 22.



Note: SNMP is only available if TCP/IP is configured.

SNMP Configuration

To configure SNMP, enter 22 from the main menu to display **Menu 22 - SNMP Configuration** as shown next. The "community" for **Get**, **Set** and **Trap** fields is SNMP terminology for password.

Figure 233 Menu 22: SNMP Configuration

```
Menu 22 - SNMP Configuration

 SNMP:
   Get Community= public
   Set Community= public
   Trusted Host= 0.0.0.0
   Trap:
     Community= public
     Destination= 0.0.0.0
Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the SNMP configuration parameters.

Table 142 SNMP Configuration Menu Fields

Field	Description	Example
Get Community	Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station.	**Public** (default)
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.	**Public** (default)
Trusted Host	If you enter a trusted host, your Contivity 221 will only respond to SNMP messages from this address. A blank (default) field means your Contivity 221 will respond to all SNMP messages it receives, regardless of source.	0.0.0.0
Trap Community	Type the Trap community, which is the password sent with each trap to the SNMP manager.	Public
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
	When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

SNMP Traps

The Contivity 221 will send traps to the SNMP manager when any one of the following events occurs:

Table 143 SNMP Traps

Trap #	Trap Name	Description
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).

Table 143 SNMP Traps

Trap #	Trap Name	Description
6	whyReboot (defined in MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

Chapter 35
System Security

This chapter describes how to configure the system security on the Contivity 221.

System Security

You can configure the system password, an external RADIUS server and 802.1x in this menu.

System Password

Figure 234 Menu 23 System Security

```
                    Menu 23 - System Security

                1. Change Password
                2. RADIUS Server

                4. IEEE802.1x

        Enter Menu Selection Number:
```

You should change the default password. If you forget your password you have to restore the default configuration file. For more information, see "Resetting the Contivity 221" in Chapter 2 Introducing the WebGUI.

Configuring External RADIUS Server

Enter 23 in the main menu to display **Menu 23 – System Security**.

Figure 235 Menu 23 System Security

```
                    Menu 23 - System Security

                1. Change Password
                2. RADIUS Server

                4. IEEE802.1x

        Enter Menu Selection Number:
```

From **Menu 23- System Security**, enter 2 to display **Menu 23.2 – System Security – RADIUS Server** as shown next.

Figure 236 Menu 23.2 System Security: RADIUS Server

```
Menu 23.2 - System Security - RADIUS Server

Authentication Server:
Active= No
Server Address= 0.0.0.0
Port #= 1812
Shared Secret= ********

Accounting Server:
Active= No
Server Address= 0.0.0.0
Port #= 1813
Shared Secret= ********

Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 144 Menu 23.2 System Security: RADIUS Server

Field	Description
Authentication Server	
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external authentication server.
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.

Table 144 Menu 23.2 System Security: RADIUS Server

Field	Description
Port #	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Contivity 221. The key is not sent over the network. This key must be the same on the external authentication server and Contivity 221.
Accounting Server	
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external accounting server.
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port #	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the Contivity 221. The key is not sent over the network. This key must be the same on the external accounting server and Contivity 221.
	When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.

IEEE 802.1x

The IEEE 802.1x standards outline enhanced security methods for both the authentication of users and encryption key management.

Follow the steps below to enable EAP authentication on your Contivity 221.

1 From the main menu, enter 23 to display **Menu23 – System Security**.

Figure 237 Menu 23 System Security

```
   Menu 23 - System Security

1. Change Password
2. RADIUS Server

4. IEEE802.1x

Enter Menu Selection Number:
```

2 Enter 4 to display **Menu 23.4 – System Security – IEEE802.1x**.

Figure 238 Menu 23.4 System Security: IEEE802.1x

```
Menu 23.4 - System Security - IEEE802.1x

Port Control= Authentication Required
ReAuthentication Timer (in second)= 1800
Idle Timeout (in second)= 3600

Authentication Databases= Local User Database Only

                    Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

The following table describes the fields in this menu.

Table 145 Menu 23.4 System Security: IEEE802.1x

Field	Description
Port Control	Press [SPACE BAR] and select a security mode. Select **No Authentication Required** to allow any computer access to your network without entering usernames and passwords. This is the default setting. Selecting **Authentication Required** means computers have to enter usernames and passwords before access to the network is allowed. Select **No Access Allowed** to block all computers access to the network. The following fields are not available when you select **No Authentication Required** or **No Access Allowed**.
ReAuthentication Timer (in second)	Specify how often a client has to re-enter username and password to stay connected to the network. This field is activated only when you select **Authentication Required** in the **Port Control** field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is **1800** seconds (or 30 minutes).
Idle Timeout (in second)	The Contivity 221 automatically disconnects a client from the network after a period of inactivity. The client needs to enter the username and password again before access to the network is allowed. This field is activated only when you select **Authentication Required** in the **Port Control** field. The default time interval is **3600** seconds (or 1 hour).

Table 145 Menu 23.4 System Security: IEEE802.1x

Field	Description
Authentication Databases	The authentication database contains user login information. The local user database is the built-in database on the Contivity 221. The RADIUS is an external server. Use this field to decide which database the Contivity 221 should use (first) to authenticate a user. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local User Database Only** to have the Contivity 221 just check the built-in user database on the Contivity 221 for a user's username and password. Select **RADIUS Only** to have the Contivity 221 just check the user database on the specified RADIUS server for a user's username and password. Select **Local first, then RADIUS** to have the Contivity 221 first check the user database on the Contivity 221 for a user's username and password. If the user name is not found, the Contivity 221 then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the Contivity 221 first check the user database on the specified RADIUS server for a user's username and password. If the Contivity 221 cannot reach the RADIUS server, the Contivity 221 then checks the local user database on the Contivity 221. When the user name is not found or password does not match in the RADIUS server, the Contivity 221 will not check the local user database and the authentication fails.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the Contivity 221 for authentication

Chapter 36
System Information & Diagnosis

This chapter covers SMT menus 24.1 to 24.4.

Introduction to System Status

This chapter covers the diagnostic tools that help you to maintain your Contivity 221. These tools include updates on system status, port status and log and trace capabilities.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

Figure 239 Menu 24: System Maintenance

```
                Menu 24 - System Maintenance


 1. System Status
 2. System Information and Console Port Speed
 3. Log and Trace
 4. Diagnostic
 5. Backup Configuration
 6. Restore Configuration
 7. Upload Firmware
 8. Command Interpreter Mode
 9. Call Control
 10. Time and Date Setting
 11. Remote Management Setup

                Enter Menu Selection Number:
```

System Status

The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your Contivity 221. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.

To get to the System Status:

1. Enter number 24 to go to **Menu 24 - System Maintenance**.
2. In this menu, enter 1 to open System Maintenance - Status.
3. There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN connection, 9 resets the counters and [ESC] takes you back to the previous screen.

Figure 240 Menu 24.1: System Maintenance: Status

```
                Menu 24.1 - System Maintenance - Status 03:06:17
 Sat. Jan. 01, 2000

Port Status TxPkts RxPkts Cols Tx B/s Rx B/s Up Time
 WAN Down 0 0 0 0 0 0:00:00
 LAN Down 463 792 0 0 0 0:00:00

Port Ethernet Address IP Address IP Mask DHCP
 WAN 00:a0:c5:01:23:46 0.0.0.0 0.0.0.0 Client
 LAN 00:a0:c5:01:23:45 192.168.1.1 255.255.255.0 Server

 System up Time: 3:06:20
 Name:
 Routing: IP
 RAS F/W Version: VE221_2.5.0.0.003 | 08/01/2003

 Press Command:

                COMMANDS: 1-Drop WAN 9-Reset Counters ESC-Exit
```

The following table describes the fields present in **Menu 24.1 - System Maintenance - Status**. These fields are READ-ONLY and meant for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

Table 146 System Maintenance: Status Menu Fields

Field	Description
Port	Identifies a port (WAN, or LAN) on the Contivity 221.
Status	Shows the port speed and duplex setting if you're using **Ethernet Encapsulation** and **Down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using **PPPoE Encapsulation**.
TxPkts	The number of transmitted packets on this port.
RxPkts	The number of received packets on this port.

Table 146 System Maintenance: Status Menu Fields

Field	Description
Cols	The number of collisions on this port.
Tx B/s	Shows the transmission speed in Bytes per second on this port.
Rx B/s	Shows the reception speed in Bytes per second on this port.
Up Time	Total amount of time the line has been up.
Ethernet Address	The Ethernet address of the port listed on the left.
IP Address	The IP address of the port listed on the left.
IP Mask	The IP mask of the port listed on the left.
DHCP	The DHCP setting of the port listed on the left.
System up Time	The total time the Contivity 221 has been on.
RAS F/W Version	The Nortel Networks firmware version and the date created.
Name	This is the Contivity 221's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
	You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24

System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

1. Enter 24 to go to **Menu 24 – System Maintenance**.
2. Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.
3. From this menu you have two choices as shown in the next figure:

Figure 241 System Information and Console Port Speed

```
Menu 24.2 - System Information and Console Port Speed

                1. System Information
                2. Console Port Speed
                Please enter selection:
```

Chapter 37
System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, Ethernet address, IP address, etc.

Figure 242 Menu 24.2.1: System Maintenance Information:

```
Menu 24.2.1 - System Maintenance - Information

    Name:
    Routing: IP
    RAS F/W Version: VE221_2.5.0.0.003 | 09/03/2004
    Country Code: 255

    LAN
    Ethernet Address: 00:A0:C5:00:00:01
    IP Address: 192.168.1.1
    IP Mask: 255.255.255.0
    DHCP: Server


    Press ESC or RETURN to Exit:
```

Table 147 Fields in System Maintenance: Information

Field	Description
Name	This is the Contivity 221's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
RAS F/W Version	Refers to the version of Nortel Networks' Network Operating System software.
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) address of your Contivity 221.
IP Address	This is the IP address of the Contivity 221 in dotted decimal notation.
IP Mask	This shows the IP mask of the Contivity 221.
DHCP	This field shows the DHCP setting of the Contivity 221.
	When finished viewing, press [ESC] or [ENTER] to exit.

Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – Console Port Speed**. Your Contivity 221 supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown next.

Figure 243 Menu 24.2.2: System Maintenance: Change Console Port Speed

```
Menu 24.2.2 - System Maintenance - Change Console Port Speed

                Console Port Speed: 115200

                Press ENTER to Confirm or ESC to Cancel:
               Press Space Bar to Toggle.
```

Log and Trace

The Contivity 221 has a syslog facility for message logging, and a trace function for viewing call-triggering packets.

Figure 244 Menu 24.3: System Maintenance: Log and Trace

```
Menu 24.3 - System Maintenance - Log and Trace

2. Syslog Logging
4. Call-Triggering Packet



Press ENTER to Confirm or ESC to Cancel
```

Syslog Logging

The Contivity 221 uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - Syslog Logging**, as shown next.

Figure 245 Menu 24.3.2: System Maintenance: Syslog Logging

```
Menu 24.3.2 - System Maintenance - Syslog Logging

Syslog:
Active= No
Syslog Server IP Address= ?
Log Facility= Local 1









Press ENTER to Confirm or ESC to Cancel
```

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 148 System Maintenance Menu Syslog Parameters

Parameter	Description
Syslog: Active	 Press [SPACE BAR] and then [ENTER] to turn syslog on or off.

Table 148 System Maintenance Menu Syslog Parameters

Parameter	Description
Syslog Server IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to the documentation of your syslog program for more details.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your Contivity 221 sends five types of syslog messages. Some examples of these syslog messages with their message formats are shown next:

CDR

CDR Message Format
SdcmdSyslogSend(SYSLOG_CDR, SYSLOG_INFO, String); String = board xx line xx channel xx, call xx, str board = the hardware board ID line = the WAN ID in a board Channel = channel ID within the WAN call = the call reference number which starts from 1 and increments by 1 for each new call str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.) L02 Tunnel Connected(L2TP) C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number) L02 Call Terminated C02 Call Terminated Jul 19 11:19:27 192.168.102.2 RAS: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002 Jul 19 11:19:32 192.168.102.2 RAS: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002 Jul 19 11:20:06 192.168.102.2 RAS: board 0 line 0 channel 0, call 1, C02 Call Terminated

Packet Triggered

Packet triggered Message Format
SdcmdSyslogSend(SYSLOG_PKTTRI, SYSLOG_NOTICE, String); String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG) Data: We will send forty-eight Hex characters to the server Jul 19 11:28:39 192.168.102.2 RAS: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c0200010061626364656 66768696a6b6c6d6e6f7071727374 Jul 19 11:28:56 192.168.102.2 RAS: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600 220008cd40000020405b4 Jul 19 11:29:06 192.168.102.2 RAS: Packet Trigger: Protocol=1, Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d143013500 4000077600000

Filter Log

Filter log Message Format
SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String); String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D). Src: Source Address Dst: Destination Address prot: Protocol (“TCP”,”UDP”,”ICMP”) spo: Source port dpo: Destination port Mar 03 10:39:43 202.132.155.97 RAS: GEN[ffffffffffnordff0080] }S05>R01mF Mar 03 10:41:29 202.132.155.97 RAS: GEN[00a0c5f502fnord010080] }S05>R01mF Mar 03 10:41:34 202.132.155.97 RAS: IP[Src=192.168.1.33 Dst=202.132.155.93 ICMP]}S04>R01mF Mar 03 11:59:20 202.132.155.97 RAS: GEN[00a0c5f502fnord010080] }S05>R01mF Mar 03 12:00:52 202.132.155.97 RAS: GEN[fffffffffff0080] }S05>R01mF Mar 03 12:00:57 202.132.155.97 RAS: GEN[00a0c5f502010080] }S05>R01mF Mar 03 12:01:06 202.132.155.97 RAS: IP[Src=192.168.1.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF

PPP Log

PPP Log Message Format
SdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String); String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP Jul 19 11:42:44 192.168.102.2 RAS: ppp:LCP Closing Jul 19 11:42:49 192.168.102.2 RAS: ppp:IPCP Closing Jul 19 11:42:54 192.168.102.2 RAS: ppp:CCP Closing

Firewall Log

```
Firewall Log Message Format
SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);
buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot |
rule | action]
Src: Source Address
spo: Source port (empty means no source port information)
Dst: Destination Address
dpo: Destination port (empty means no destination port information)
prot: Protocol (“TCP”,”UDP”,”ICMP”, ”IGMP”, ”GRE”, ”ESP”)
rule: <a,b> where a means "set" number; b means "rule" number.
Action: nothing(N) block (B) forward (F)
08-01-2000 11:48:41 Local1.Notice 192.168.10.10 RAS: FW 172.21.1.80 :137
->172.21.1.80 :137 |UDP|default permit:<2,0>|B
08-01-2000 11:48:41 Local1.Notice 192.168.10.10 RAS: FW 192.168.77.88
:520 ->192.168.77.88 :520 |UDP|default permit:<2,0>|B
08-01-2000 11:48:39 Local1.Notice 192.168.10.10 RAS: FW 172.21.1.50
->172.21.1.50 |IGMP<2>|default permit:<2,0>|B
08-01-2000 11:48:39 Local1.Notice 192.168.10.10 RAS: FW 172.21.1.25
->172.21.1.25 |IGMP<2>|default permit:<2,0>|B
```

Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

Figure 246 Call-Triggering Packet Example

```
IP Frame: ENET0-RECV Size: 44/ 44 Time: 17:02:44.262
 Frame Type:

 IP Header:
 IP Version = 4
 Header Length = 20
 Type of Service = 0x00 (0)
 Total Length = 0x002C (44)
 Identification = 0x0002 (2)
 Flags = 0x00
 Fragment Offset = 0x00
 Time to Live = 0xFE (254)
 Protocol = 0x06 (TCP)
 Header Checksum = 0xFB20 (64288)
 Source IP = 0xC0A80101 (192.168.1.1)
 Destination IP = 0x00000000 (0.0.0.0)

 TCP Header:
 Source Port = 0x0401 (1025)
 Destination Port = 0x000D (13)
 Sequence Number = 0x05B8D000 (95997952)
 Ack Number = 0x00000000 (0)
 Header Length = 24
 Flags = 0x02 (....S.)
 Window Size = 0x2000 (8192)
 Checksum = 0xE06A (57450)
 Urgent Ptr = 0x0000 (0)
 Options =
 0000: 02 04 02 00

 RAW DATA:
 0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01 E......... ....
 0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00 ................
```

```
 0020: 60 02 20 00 E0 6A 00 00-02 04 02 00
Press any key to continue...
```

The diagnostic facility allows you to test the different aspects of your Contivity 221 to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown next.

Follow the procedure below to get to **Menu 24.4 - System Maintenance – Diagnostic.**

From the main menu, select option 24 to open **Menu 24 - System Maintenance**.

From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.

Figure 247 Menu 24.4: System Maintenance: Diagnostic

```
Menu 24.4 - System Maintenance - Diagnostic

                    TCP/IP
                       1. Ping Host
                       2. WAN DHCP Release
                       3. WAN DHCP Renewal
                       4. PPPoE/PPTP Setup Test

                     System
                       11. Reboot System



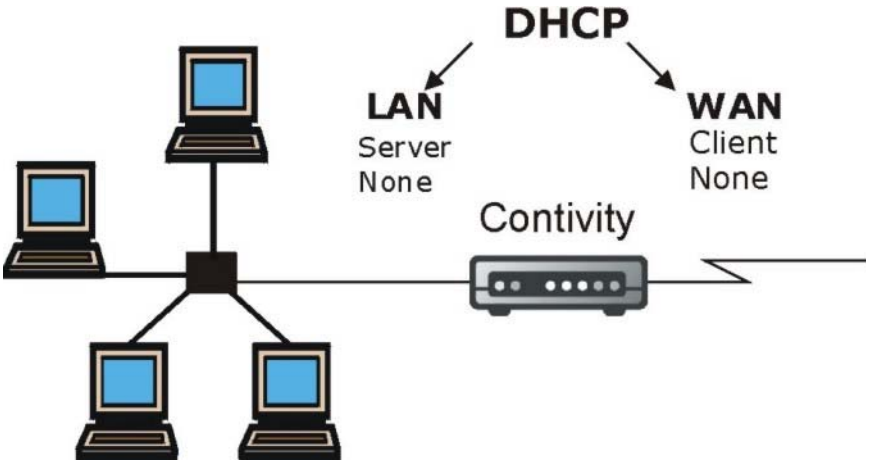
                       Enter Menu Selection Number:


                       Host IP Address= N/A
```

WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in WAN & LAN DHCP. LAN DHCP has already been discussed. The Contivity 221 can act either as a WAN DHCP client (IP Address Assignment field in menu 4 or menu 11.1.2 is Dynamic and the Encapsulation field in menu 4 or menu 11 is Ethernet) or None, (when you have a static IP). The WAN Release and Renewal fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

Figure 248 WAN & LAN DHCP



The following table describes the diagnostic tests available in menu 24.4 for your Contivity 221 and associated connections.

Table 149 System Maintenance Menu Diagnostic

Field	Description
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the **Host IP Address** field below.
WAN DHCP Release	Enter 2 to release your WAN DHCP settings.
WAN DHCP Renewal	Enter 3 to renew your WAN DHCP settings.

Table 149 System Maintenance Menu Diagnostic

Field	Description
Internet Setup Test	Enter 4 to test the Internet setup. You can also test the Internet setup in **Menu 4 - Internet Access**. Please refer to the *Internet Access* chapter for more details. This feature is only available for dial-up connections using PPPoE or PPTP encapsulation.
Reboot System	Enter 11 to reboot the Contivity 221.
Host IP Address=	If you entered 1 in **Ping Host**, then enter the IP address of the computer you want to ping in this field.
	Enter the number of the selection you would like to perform or press [ESC] to cancel.

Chapter 38
Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files.

Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It comes with a “rom” filename extension. Once you have customized the Contivity 221's settings, they can be saved back to your computer under a filename of your choosing.

The system firmware (sometimes referred to as the “ras” file) has a “bin” filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.



Note: Only use firmware for your Contivity 221’s specific model. Refer to the label on the bottom of your Contivity 221.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the Contivity 221.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file “config.cfg”.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Contivity 221 only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the Contivity 221 and the external filename refers to the filename not on the Contivity 221, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the F/W version field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press “y” when prompted in the SMT menu to go into debug mode.

Table 150 Filename Conventions

File Type	Internal Name	External Name	Description
Configuration File	Rom-0	This is the configuration filename on the Contivity 221. Uploading the rom-0 file replaces the entire ROM file system, including your Contivity 221 configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the name for the firmware on the Contivity.	*.bin

Backup Configuration



Note: The Contivity 221 displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2; depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current Contivity 221 configuration to your computer. Backup is highly recommended once your Contivity 221 is functioning properly. FTP is the preferred methods for backing up your current configuration to your computer since they are faster. You

can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the Contivity 221 to the computer, while upload means from your computer to the Contivity 221.

Backup Configuration

Follow the instructions as shown in the next screen.

Figure 249 Menu 24.5 - System Maintenance - Backup Configuration

```
                Menu 24.5 - System Maintenance - Backup Configuration

To transfer the configuration file to your workstation, follow the
procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Contivity 221. Then type "admin"
and SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current Contivity 221 configuration to
   your workstation.
For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Contivity 221 manual.


                Press ENTER to Exit:
```

Using the FTP Command from the Command Line

1. Launch the FTP client on your computer.
2. Enter "open", followed by a space and the IP address of your Contivity 221.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "setup").
5. Enter "bin" to set transfer mode to binary.

6 Use “get” to transfer files from the Contivity 221 to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the Contivity 221 to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

7 Enter “quit” to exit the ftp prompt.

Example of FTP Commands from the Command Line

Figure 250 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 config.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 151 General Commands for GUI-based FTP Clients

Command	Description
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.

Table 151 General Commands for GUI-based FTP Clients

Command	Description
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

TFTP and FTP over WAN Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

- You have disable Telnet service in menu 24.11.
- You have applied a filter in menu 3.1 (LAN) or in menu 11.1.4 (WAN) to block Telnet service.
- The IP address in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the Contivity 221 will disconnect the Telnet session immediately.
- You have an SMT console session running.

Backup Configuration Using TFTP

The Contivity 221 supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the Contivity 221 and log in. Because TFTP does not have any security checks, the Contivity 221 records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.

4 Launch the TFTP client on your computer and connect to the Contivity 221. Set the transfer mode to binary before starting data transfer.

5 Use the TFTP client (see the example below) to transfer files between the Contivity 221 and the computer. The file name for the configuration file is "rom-0" (rom-zero, not capital o).



Note: Telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the Contivity 221 to the computer and "binary" to set binary transfer mode.

TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the Contivity 221 IP address, "get" transfers the file source on the Contivity 221 (rom-0, name of the configuration file on the Contivity 221) to the file destination on the computer and renames it config.rom.

GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 152 General Commands for GUI-based TFTP Clients

Command	Description
Host	Enter the IP address of the Contivity 221. 192.168.1.1 is the Contivity 221's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the Contivity 221 and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the Contivity 221. The filename for the firmware is "ras" and for the configuration file, is "rom-0".

Table 152 General Commands for GUI-based TFTP Clients

Command	Description
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to the Remote Management section to read about configurations that disallow TFTP and FTP over WAN.

Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Display menu 24.5 and enter “y” at the following screen.

Figure 251 Menu 24.5 System Maintenance: Backup Configuration

```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

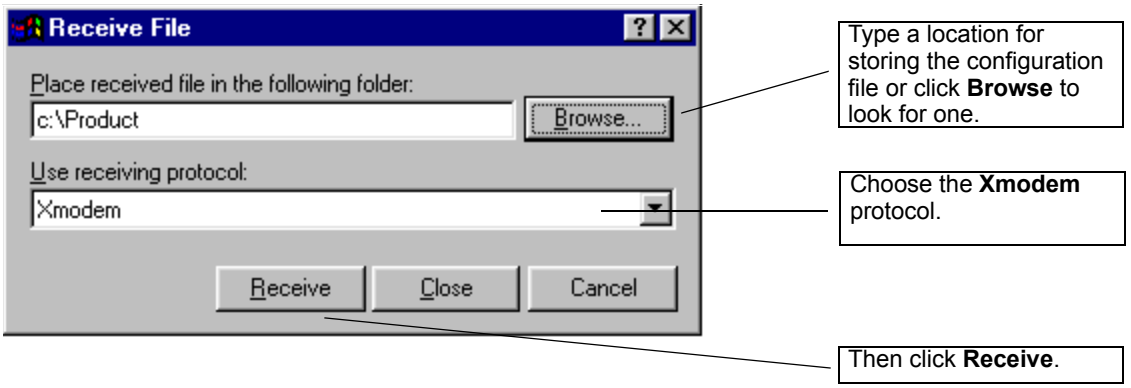
The following screen indicates that the Xmodem download has started.

Figure 252 Menu 24.5 System Maintenance: Starting Xmodem Download Screen

```
You can enter ctrl-x to terminate operation any time.
Starting XMODEM download...
```

Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

Figure 253 Backup Configuration Example



After a successful backup you will see the following screen. Press any key to return to the SMT menu.

Figure 254 Successful Backup Confirmation Screen

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your Contivity 221 since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Warning: Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Contivity 221.

Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

Figure 255 Telnet into Menu 24.6

```
                Menu 24.6 -- System Maintenance - Restore Configuration

To transfer the firmware and configuration file to your workstation,
follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Contivity 221. Then type "admin"
and SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-0 is the
   remote file name on the Contivity 221. This restores the configuration
to your Contivity 221.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Contivity 221 manual.

                Press ENTER to Exit:
```

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your Contivity 221.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “setup”).
5. Enter “bin” to set transfer mode to binary.
6. Find the “rom” file (on your computer) that you want to restore to your Contivity 221.
7. Use “put” to transfer files from the Contivity 221 to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the Contivity 221. See earlier in this chapter for more information on filename conventions.
8. Enter “quit” to exit the ftp prompt. The Contivity 221 will automatically restart after a successful restore process.

Restore Using FTP Session Example

Figure 256 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to the Remote Management section to read about configurations that disallow TFTP and FTP over WAN.

Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

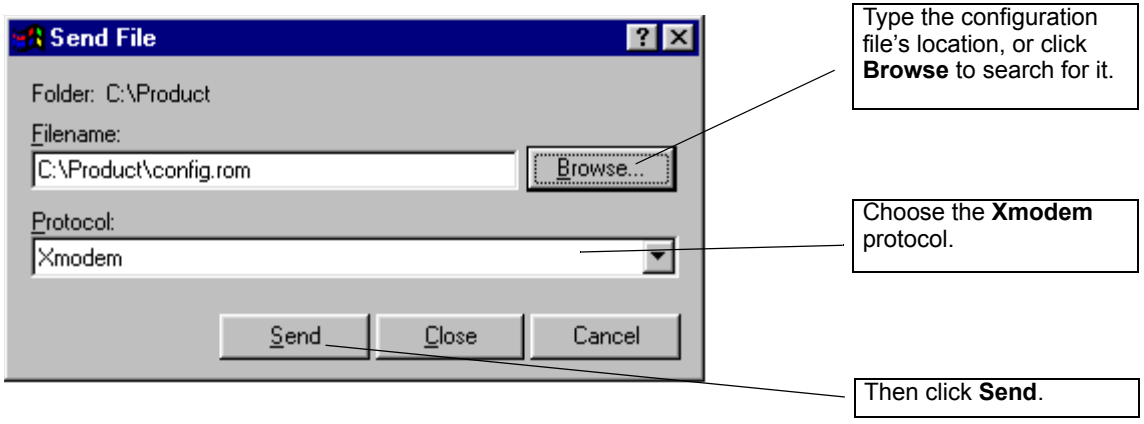
Display menu 24.6 and enter “y” at the following screen.

Figure 257 System Maintenance: Restore Configuration

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

The following screen indicates that the Xmodem download has started.

Figure 258 System Maintenance: Starting Xmodem Download Screen



Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

```
Starting XMODEM download (CRC mode) ...
CCCCCCCCC
```

After a successful restoration you will see the following screen. Press any key to restart the Contivity 221 and return to the SMT menu.

Figure 259 Successful Restoration Confirmation Screen

```
Save to ROM

Hit any key to start system reboot.
```

Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous "Restore Configuration section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File** (for console port).



Warning: Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Contivity 221.

Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the Contivity 221, you will see the following screens for uploading firmware and the configuration file using FTP.

Figure 260 Telnet Into Menu 24.7.1 Upload System Firmware

```
                Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:
  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "admin" and
     SMT password as requested.
  3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
     of your firmware upgrade file on your workstation and "ras" is the
     remote file name on the system.
  4. The system reboots automatically after a successful firmware upload.
For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.


                Press ENTER to Exit:
```

Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

Figure 261 Telnet Into Menu 24.7.2 System Maintenance

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:
  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "admin" and
     SMT password as requested.
  3. Type "put configurationfilename rom-0" where "configurationfilename"
     is the name of your system configuration file on your workstation,
which
     will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system configuration
     file process is complete.
For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.


                Press ENTER to Exit:
```

To upload the firmware and the configuration file, follow these examples

FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your Contivity 221.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “setup”).
5. Enter “bin” to set transfer mode to binary.
6. Use “put” to transfer files from the computer to the Contivity 221, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the Contivity 221 and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the Contivity 221 and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the Contivity 221 to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.



Note: The Contivity 221 automatically restarts after a successful file upload.

FTP Session Example of Firmware File Upload

Figure 262 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to the Remote Management section to read about configurations that disallow TFTP and FTP over WAN.

TFTP File Upload

The Contivity 221 also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

1. To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.
2. Use telnet from your computer to connect to the Contivity 221 and log in. Because TFTP does not have any security checks, the Contivity 221 records the IP address of the telnet client and accepts TFTP requests only from this address.
3. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
4. Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.
5. Launch the TFTP client on your computer and connect to the Contivity 221. Set the transfer mode to binary before starting data transfer.
6. Use the TFTP client (see the example below) to transfer files between the Contivity 221 and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the Contivity 221 in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the Contivity 221 to the computer, “put” the other way around, and “binary” to set binary transfer mode.

TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the Contivity 221’s IP address and “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the Contivity 221).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your Contivity 221. However, in the event of your network being down, uploading files is only possible with a direct connection to your Contivity 221 via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

Uploading Firmware File Via Console Port

Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 – System Maintenance – Upload System Firmware**, then follow the instructions as shown in the following screen.

Figure 263 Menu 24.7.1 as seen using the Console Port

```
Menu 24.7.1 - System Maintenance - Upload System Firmware

          To upload system firmware:
          1. Enter "y" at the prompt below to go into debug mode.
          2. Enter "atur" after "Enter Debug Mode" message.
          3. Wait for "Starting XMODEM upload" message before activating
             Xmodem upload on your terminal.
          4. After successful firmware upload, enter "atgo" to restart the
             Contivity 221.

         Warning: Proceeding with the upload will erase the current system
          firmware.

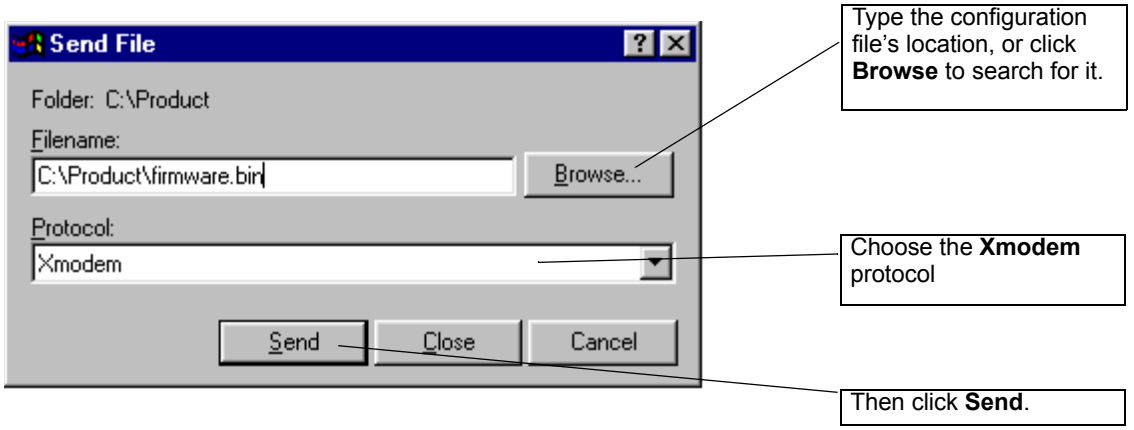
 Do You Wish To Proceed:(Y/N)
```

After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 264 Example Xmodem Upload



After the configuration upload process has completed, restart the Contivity 221 by entering "**`atgo`**".

Uploading Configuration File Via Console Port

1 Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 – System Maintenance – Upload System Configuration File**. Follow the instructions as shown in the next screen.

Figure 265 Menu 24.7.2 as seen using the Console Port

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

          To upload system configuration file:
          1. Enter "y" at the prompt below to go into debug mode.
          2. Enter "atlc" after "Enter Debug Mode" message.
          3. Wait for "Starting XMODEM upload" message before activating
             Xmodem upload on your terminal.
          4. After successful firmware upload, enter "atgo" to restart the
             system.

          Warning:
          1. Proceeding with the upload will erase the current
             configuration file.
          2. The system's console port speed (Menu 24.2.2) may change
             when it is restarted; please adjust your terminal's speed
             accordingly. The password may change (menu 23), also.
          3. When uploading the DEFAULT configuration file, the console
             port speed will be reset to 9600 bps and the password to
             "setup".

               Do You Wish To Proceed:(Y/N)
```

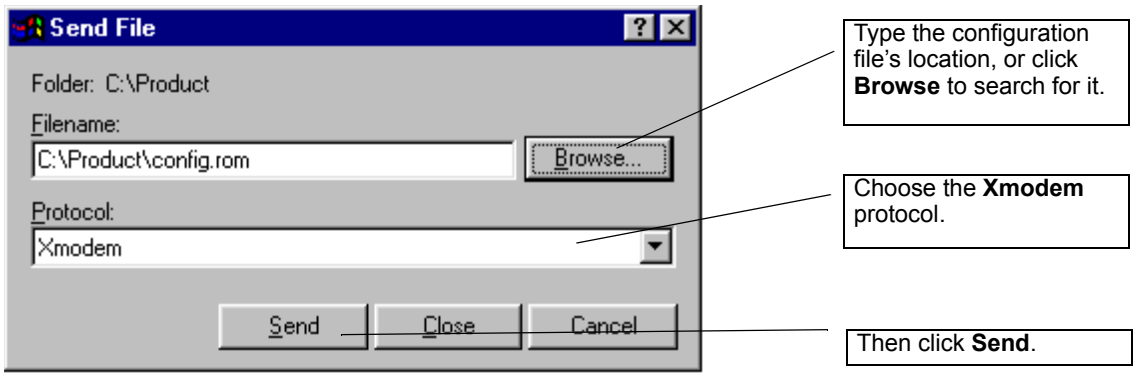
2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

3 Enter "**atgo**" to restart the Contivity 221.

Example Xmodem Configuration Upload Using HyperTerminal

1 Click **Transfer**, then **Send File** to display the following screen.

Figure 266 Example Xmodem Upload



2 After the configuration upload process has completed, restart the Contivity 221 by entering "**`atgo`**".

Chapter 39
System Maintenance Menus 8 to 10

This chapter leads you through SMT menus 24.8 to 24.10.

Command Interpreter Mode

The Command Interpreter (CI) is a part of the main router firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or nortelnetworks.com for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**.



Note: Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Figure 267 Command Mode in Menu 24

```
Menu 24 - System Maintenance

 1. System Status
 2. System Information and Console Port Speed
 3. Log and Trace
 4. Diagnostic
 5. Backup Configuration
 6. Restore Configuration
 7. Firmware Update
 8. Command Interpreter Mode
 9. Call Control
 10. Time and Date Setting
 11. Remote Management Setup



 Enter Menu Selection Number:
```

Command Syntax

The command keywords are in courier new font.

Enter the command keywords exactly as shown, do not abbreviate.

The required fields in a command are enclosed in angle brackets <>.

The optional fields in a command are enclosed in square brackets [].

The |symbol means “or”.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

A list of commands can be found by typing help or ? at the command prompt. Always type the full command. Type exit to return to the SMT main menu when finished.

Figure 268 Valid Commands

```
ras> ?

Valid commands are:

sys             exit            ether           ip
ipsec           bm              certificates    radius
8021x
```

Table 153 Valid Commands

Command	Description
sys	The system commands display device information and configure device settings.
exit	This command returns you to the SMT main menu.
ether	These commands display Ethernet information and configure Ethernet settings.
ip	These commands display IP information and configure IP settings.
ipsec	These commands display IPSec information and configure IPSec settings.
bm	These commands display bandwidth management information and configure bandwidth management settings.
certificates	These commands display certificate information and configure certificate settings.
radius	These commands display RADIUS information.
8021x	These commands display IEEE 802.1x information.

Call Control Support

The Contivity 221 provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the Contivity 221 within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

Figure 269 Call Control

```
Menu 24.9 - System Maintenance - Call Control


 1.Budget Management
 2.Call History
Enter Menu Selection Number:
```

Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

Figure 270 Budget Management

```
                    Menu 24.9.1 - Budget Management

Remote Node      Connection Time/Total Budget    Elapsed Time/Total Period
1.ChangeMe       No Budget                       No Budget

2.GUI            No Budget                       No Budget


                    Reset Node (0 to update screen):
```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

Table 154 Budget Management

Field	Description	Example
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/ Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1).	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1-hour time period has lapsed.
	Enter “0” to update the screen or press [ESC] to return to the previous screen.	

Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

Figure 271 Call History

```
Menu 24.9.2 - Call History

Phone Number      Dir   Rate     #call      Max       Min       Total
 1.
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

Enter Entry to Delete(0 to exit):
```

The following table describes the fields in this screen.

Table 155 Call History Fields

Field	Description
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
	You may enter an entry number to delete it or ‘”0” to exit.

Time and Date Setting

There is a software mechanism to set the time manually or get the current time and date from an external server when you turn on your Contivity 221. Menu 24.10 allows you to update the time and date settings of your Contivity 221. The real time is then displayed in the Contivity 221 error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

Figure 272 Menu 24: System Maintenance

```
                Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup

               Enter Menu Selection Number:
```

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your Contivity 221 as shown in the following screen.

Figure 273 Menu 24.10 System Maintenance: Time and Date Setting

```
Menu 24.10 - System Maintenance - Time and Date Setting

 Time Protocol= NTP (RFC-1305)
 Time Server Address= time-b.nist.gov

 Current Time:                          01 : 07 : 41
 New Time (hh:mm:ss):                   N/A  N/A  N/A

 Current Date:                          2000 - 01 - 01
 New Date (yyyy-mm-dd):                 N/A    N/A  N/A

 Time Zone= GMT

 Daylight Saving= No
 Start Date (mm-nth-week-hr):           Jan. - 1st  - Sat. -  00
 End Date (mm-nth-week-hr):             Jan. - 1st  - Sat. -  00


            Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

The following table describes the fields in this screen.

Table 156 Time and Date Setting Fields

Field	Description
Time Protocol	Enter the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC-1305)**, is similar to **Time (RFC-868)**. Select **Manual** to enter the new time and new date manually.
Time Server Address	Enter the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format. This field is available when you select **Manual** in the **Time Protocol** field.

Table 156 Time and Date Setting Fields

Field	Description
Current Date	This field displays an updated date only when you reenter this menu.
New Date	Enter the new date in year, month and day format. This field is available when you select **Manual** in the **Time Protocol** field.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose **Yes**.
Start Date (mm-nth-week-hr)	Configure the day and time when Daylight Saving Time starts if you selected **Yes** in the **Daylight Saving** field. The **hr** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Apr.**, **1st**, **Sun.** and type 02 in the **hr** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Mar.**, **Last**, **Sun.** The time you type in the **hr** field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date (mm-nth-week-hr)	Configure the day and time when Daylight Saving Time ends if you selected **Yes** in the **Daylight Saving** field. The **hr** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Oct.**, **Last**, **Sun.** and type 02 in the **hr** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Oct.**, **Last**, **Sun.** The time you type in the **hr** field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel.	

Resetting the Time

The Contivity 221 resets the time in three instances:

- On leaving menu 24.10 after making changes.
- When the Contivity 221 starts up, if there is a timeserver configured in menu 24.10.
- 24-hour intervals after starting.

Chapter 40
Remote Management

This chapter covers remote management found in SMT menu 24.11.

Remote Management

Remote management allows you to determine which services/protocols can access which Contivity 221 interface (if any) from which computers.

You may manage your Contivity 221 from a remote location via:

- `Internet (`WAN only`)`
- ALL `(LAN and WAN)`
- LAN only
- `Neither (`Disable`)`



Note: When you Choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

Figure 274 Menu 24.11 – Remote Management Control

```
                Menu 24.11 - Remote Management Control

TELNET Server:     Port = 23         Access = LAN only
                   Secure Client IP = 0.0.0.0
FTP Server:        Port = 21         Access = LAN only
                   Secure Client IP = 0.0.0.0
SSH Server:        Certificate = auto_generated_self_signed_cert
                   Port = 22         Access = ALL
                   Secure Client IP = 0.0.0.0
HTTPS Server:      Certificate = auto_generated_self_signed_cert
                   Authenticate Client Certificates = No
                   Port = 443        Access = ALL
                   Secure Client IP = 0.0.0.0
HTTP Server:       Port = 80         Access = LAN only
                   Secure Client IP = 0.0.0.0
SNMP Service:      Port = 161        Access = LAN only
                   Secure Client IP = 0.0.0.0
DNS Service:       Port = 53         Access = LAN only
                   Secure Client IP = 0.0.0.0
               Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 157 Menu 24.11 – Remote Management Control

Field	Description
Telnet Server FTP Server SSH Server HTTPS Server HTTP Server SNMP Service DNS Service	Each of these read-only labels denotes a service that you may use to remotely manage the Contivity 221.
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the Contivity 221.
Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**.
Secure Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the Contivity 221. Enter an IP address to restrict access to a client with a matching IP address.

Table 157 Menu 24.11 – Remote Management Control

Field	Description
Certificate	Press [SPACE BAR] and then [ENTER] to select the certificate that the Contivity 221 will use to identify itself. The Contivity 221 is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Contivity 221).
Authenticate Client Certificates	Select **Yes** by pressing [SPACE BAR], then [ENTER] to require the SSL client to authenticate itself to the Contivity 221 by sending the Contivity 221 a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the Contivity 221 (see Appendix D, “Importing Certificates for details).
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.1.4 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Contivity 221 will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
6. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.
7. There is a firewall rule that blocks it.

Chapter 41
Call Scheduling

Call scheduling (applicable for PPPoA or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

Introduction

The call scheduling feature allows the Contivity 221 to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a video cassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 — Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

Figure 275 Menu 26 Schedule Setup

```
                        Menu 26 - Schedule Setup

Schedule                                  Schedule
Set #          Name                       Set #          Name
------  ----------------                  ------  ----------------
  1      AlwaysOn                           7      ________________
  2      ________________                   8      ________________
  3      ________________                   9      ________________
  4      ________________                  10      ________________
  5      ________________                  11      ________________
  6      ________________                  12      ________________

                Enter Schedule Set Number to Configure= 0
                Edit Name= N/A
                Press ENTER to Confirm or ESC to Cancel:
```

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Contivity 221, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.



Note: To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] (or delete) in the Edit Name field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

Figure 276 Menu 26.1 Schedule Set Setup

```
                    Menu 26.1 - Schedule Set Setup


Active= Yes
Start Date(yyyy/mm/dd) = 2000 - 01 - 01
How Often= Once
Once:
  Date(yyyy/mm/dd)= 2000 - 01 - 01
Weekdays:
  Sunday= N/A
  Monday= N/A
  Tuesday= N/A
  Wednesday= N/A
  Thursday= N/A
  Friday= N/A
  Saturday= N/A
Start Time (hh:mm)= 00 : 00
Duration (hh:mm)= 00 : 00
Action= Forced On

                 Press ENTER to Confirm or ESC to Cancel
```

If a connection has been already established, your Contivity 221 will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 158 Menu 26.1 Schedule Set Setup

Field	Description	Example
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.	Yes
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.	2000-01-01
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.	Once
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.	2000-01-01
Weekday: Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].	Yes No N/A
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	09:00
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	08:00
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.	**Forced On**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

Figure 277 Applying Schedule Set(s) to a Remote Node (PPPoE)

```
                    Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe          Route= IP
   Active= Yes                   Bridge= No
Encapsulation= PPPoE             Edit IP/Bridge= No
   Multiplexing=VC-based         Edit ATM Options= No
   Service Name=                 Telco Option:
   Incoming                        Allocated Budget(min)= 0
     Rem Login=                    Period(hr)= 0
     Rem Password= ********        Schedules=
 Outgoing=                         Nailed-Up Connection= No
     My Login=?                  Session Options:
     My Password= ********         Edit Filter Sets= No
     Authen= CHAP/PAP              Idle Timeout(sec)= 100


              Press ENTER to Confirm or ESC to Cancel:
```

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Appendix A Troubleshooting

This chapter covers potential problems and the corresponding remedies.

Problems Starting Up the Contivity 221

Table 159 Troubleshooting the Start-Up of Your Contivity 221

Problem	Corrective Action	
None of the LEDs turn on when I turn on the Contivity 221.	Make sure that the Contivity 221's power adaptor is connected to the Contivity 221 and plugged in to an appropriate power source. Check that the Contivity 221 and the power source are both turned on. Turn the Contivity 221 off and on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.	
I cannot access the Contivity 221 via the console port.	1. Make sure the Contivity 221 is connected to your computer's serial port.	
	2. Make sure the communications program is configured correctly. The communications software should be configured as follows:	• VT100 terminal emulation • 9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed. • No parity, 8 data bits, 1 stop bit, data flow set to none.

Problems with the LAN LED

Table 160 Troubleshooting the LAN LED

Problem	Corrective Action
The LAN LEDs do not turn on.	Check your Ethernet cable connections. Check for faulty Ethernet cables.
	Make sure your computer's Ethernet Card is working properly.

Problems with the LAN Interface

Table 161 Troubleshooting the LAN Interface

Problem	Corrective Action
I cannot access the Contivity 221 from the LAN.	Check your Ethernet cable type and connections. Refer to the *Quick Start Guide* for LAN connection instructions. Make sure the computer's Ethernet adapter is installed and functioning properly.
I cannot ping any computer on the LAN.	Check the 10M/100M LAN LEDs on the front panel. One of these LEDs should be on. If they are all off, check the cables between your Contivity 221 and hub or the station. Verify that the IP address and the subnet mask of the Contivity 221 and the computers are on the same subnet.

Problems with the WAN Interface

Table 162 Troubleshooting the WAN Interface

Problem	Corrective Action
Cannot get WAN IP address from the ISP.	The ISP provides the WAN IP address after authentication. Authentication may be through the user name and password, the MAC address or the host name. Use the following corrective actions to make sure the ISP can authenticate your connection.
	You need a user name and password if you're using PPPoE or PPTP encapsulation. Make sure that you have entered the correct Service Type, User Name and Password (the user name and password are case sensitive). Use the WAN screens in the WebGUI.

Table 162 Troubleshooting the WAN Interface

Problem	Corrective Action
	If your ISP requires MAC address authentication, you should clone the MAC address from your computer on the LAN as the Contivity 221's WAN MAC address. Use the WAN screens in the WebGUI. It is recommended that you clone your computer's MAC address, even if your ISP presently does not require MAC address authentication.
	If your ISP requires host name authentication, configure your computer's name as the Contivity 221's system name (use the WebGUI's wizard or **System General** screen to configure the system name).

Problems with Internet Access

Table 163 Troubleshooting Internet Access

Problem	Corrective Action
Cannot access the Internet.	Connect your cable/DSL modem with the Contivity 221 using the appropriate cable.Check with the manufacturer of your cable/DSL device about your cable requirement because some devices may require crossover cable and others a regular straight-through cable.
	Verify your settings in the WAN screens.
Internet connection disconnects.	Check the call scheduling rules. If you use PPPoA or PPPoE encapsulation, check the idle time-out setting in the WAN screens. Contact your ISP.

Problems Accessing an Internet Web Site

Table 164 Troubleshooting Web Site Internet Access

Problem	Corrective Action
Cannot connect to a web site on the Internet.	Disable content filtering and clear your browser cache. Try connecting to the web site again. If you can now connect to this site, then the content filter may have blocked original access. Check your content filter settings if this was not your intention.
	If you cannot connect to the site even after you disable content filtering, then please check your device connections and Internet access settings. Your user name and password may be case-sensitive. If device connections and Internet access settings are correct, then please contact your ISP.

Problems with the Password

Table 165 Troubleshooting the Password

Problem	Corrective Action
I cannot access the Contivity 221.	The username is “admin”. The default password is “setup”. The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to reset the Contivity 221to the default configuration file. This restores all of the factory defaults including the password.

Problems with the WebGUI

Table 166 Troubleshooting the WebGUI

Problem	Corrective Action
I cannot access the WebGUI.	Make sure that there is not an SMT console session running. Check that you have enabled web service access. If you have configured a remote management secured client IP address, your computer's IP address must match it. For WAN access, you must configure remote management to allow server access from the Wan (or all). You must also configure a firewall rule to allow access from the WAN. Your computer's and the Contivity 221's IP addresses must be on the same subnet for LAN access. If you changed the Contivity 221's LAN IP address, then enter the new one as the URL. Remove any filters in SMT menu 3.1 (LAN) or menu 11.1.4 (WAN) that block web service.

Problems with Remote Management

Table 167 Troubleshooting Remote Management

Problem	Corrective Action
I cannot remotely manage the Contivity 221 from the LAN or the WAN.	Check your remote management and firewall configuration.
	Use the Contivity 221's WAN IP address when configuring from the WAN. Use the Contivity 221's LAN IP address when configuring from the LAN.
	Refer to "Problems with the LAN Interface for instructions on checking your LAN connection.
	Refer to the "Problems with the WAN Interface section for instructions on checking your WAN connection.
	See also the "Problems with the WebGUI section.

Allowing Pop-up Windows, JavaScript and Java Permissions

In order to use the WebGUI you need to allow:

- Web browser pop-up windows from your device
- JavaScript
- Java permissions

Internet Explorer Pop-up Blockers

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

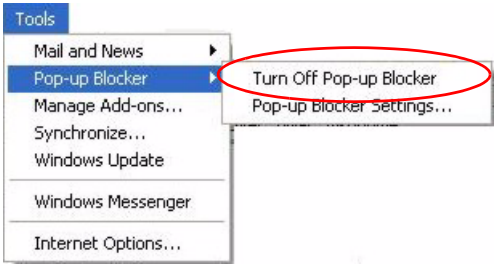
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or enable pop-up blocking and create an exception for your device's IP address.

Allowing Pop-ups

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 278 Pop-up Blocker

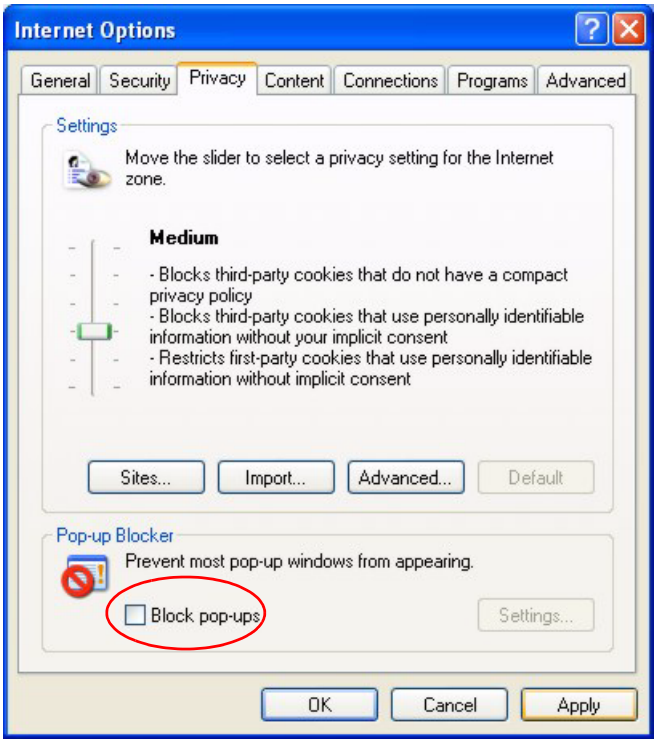


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen.

Figure 279 Internet Options



3 Click **Apply** to save this setting.

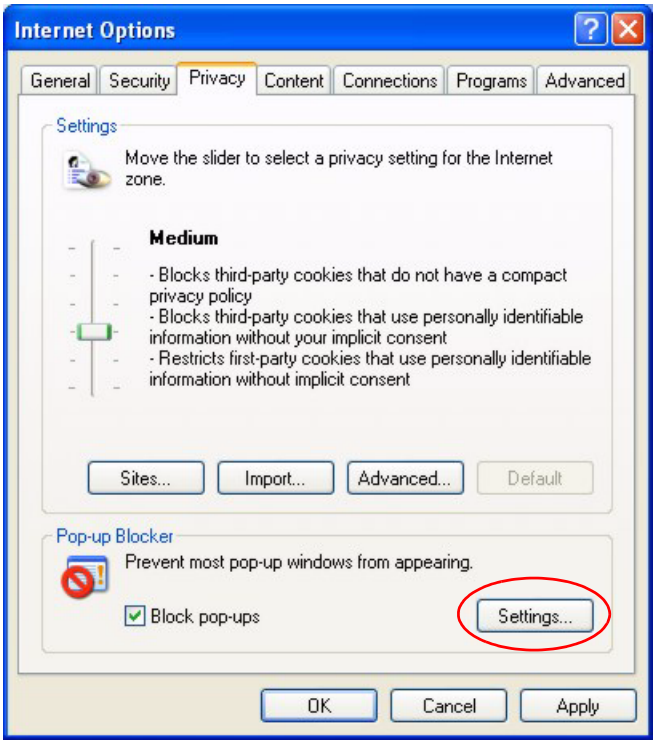
Enabling Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 280 Internet Options



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 281 Pop-up Blocker Settings



5 Click **Close** to return to the **Internet Options** screen.

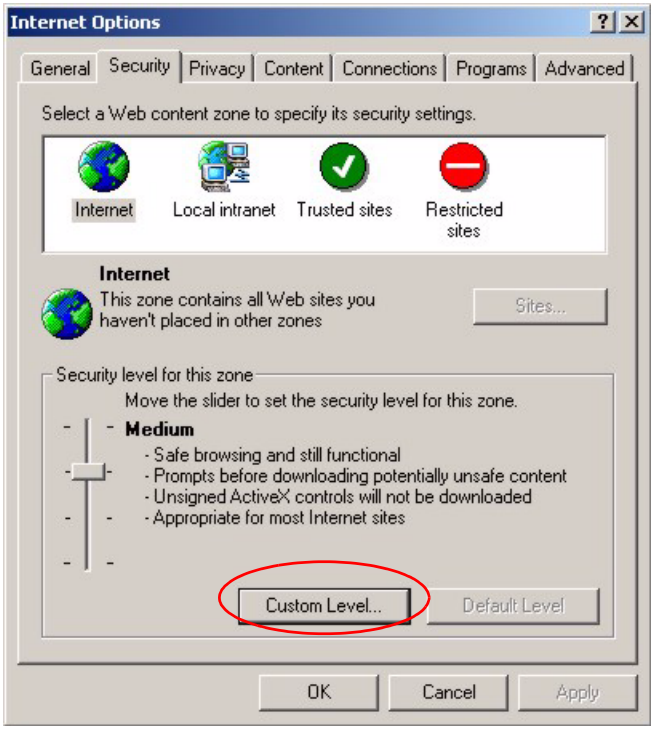
6 Click **Apply** to save this setting.

Internet Explorer JavaScript

If pages of the WebGUI do not display properly in Internet Explorer, check that JavaScript and Java permissions are enabled.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 282 Internet Options



2 Click the **Custom Level...** button.

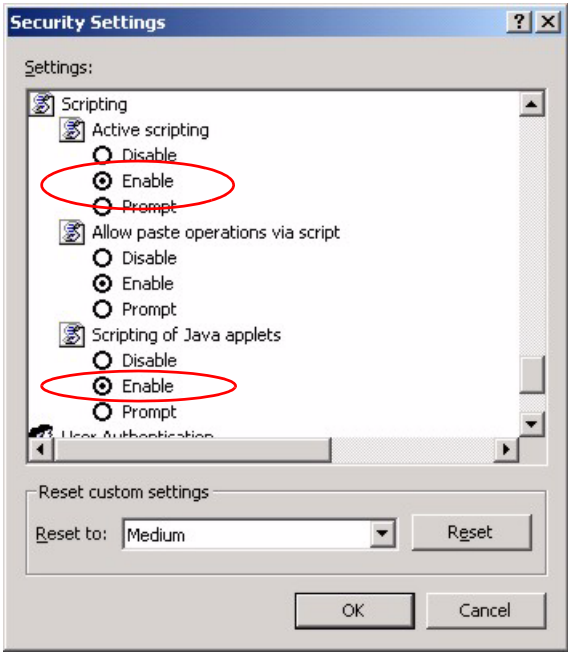
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

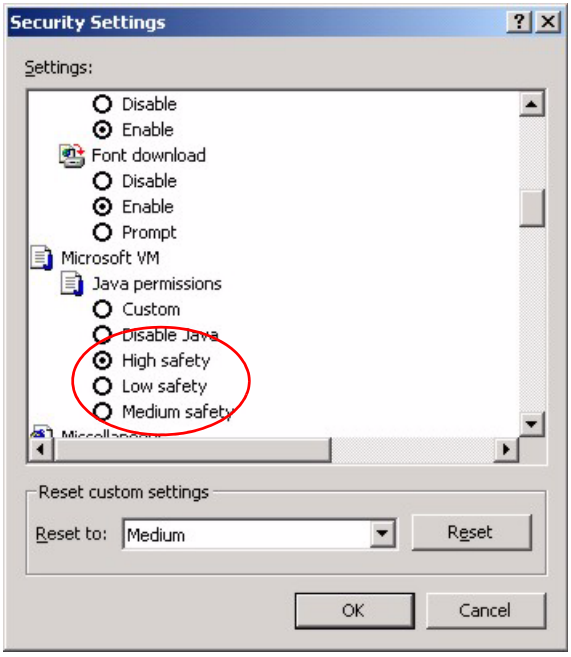
Figure 283 Security Settings - Java Scripting



Internet Explorer Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

Figure 284 Security Settings - Java



JAVA (Sun)

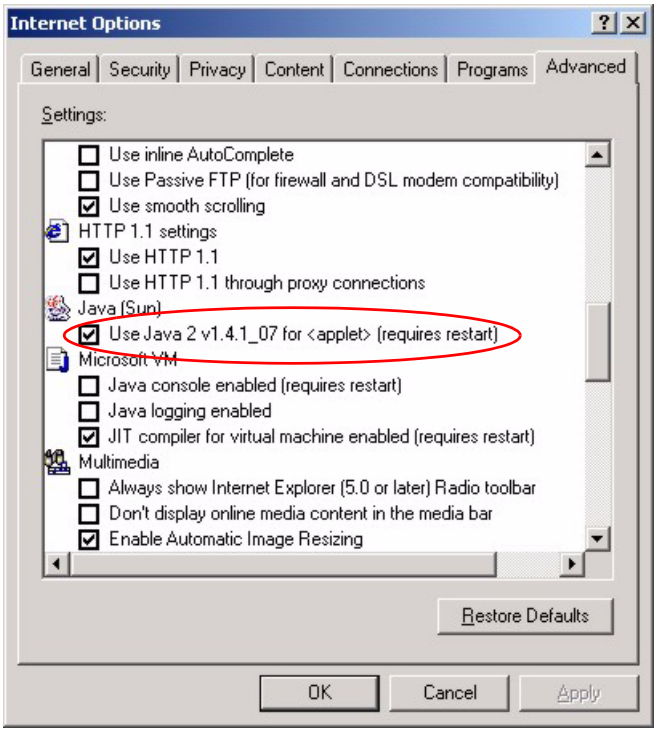
1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

4 Close your existing browser session and open a new browser.

Figure 285 Java (Sun)



Netscape Pop-up Blockers

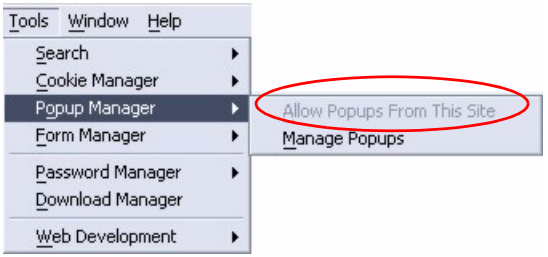
Note: Netscape 7.2 screens are used here. Screens for other Netscape versions may vary.

Either disable the blocking of unrequested pop-up windows (enabled by default in Netscape) or allow pop-ups from websites by creating an exception for your device's IP address.

Allowing Pop-ups

1 In Netscape, click **Tools**, **Popup Manager** and then select **Allow Popups From This Site**.

Figure 286 Allow Popups From This Site



2 In the Netscape search toolbar, you can enable and disable pop-up blockers for web sites.

Figure 287 Netscape Search Toolbar



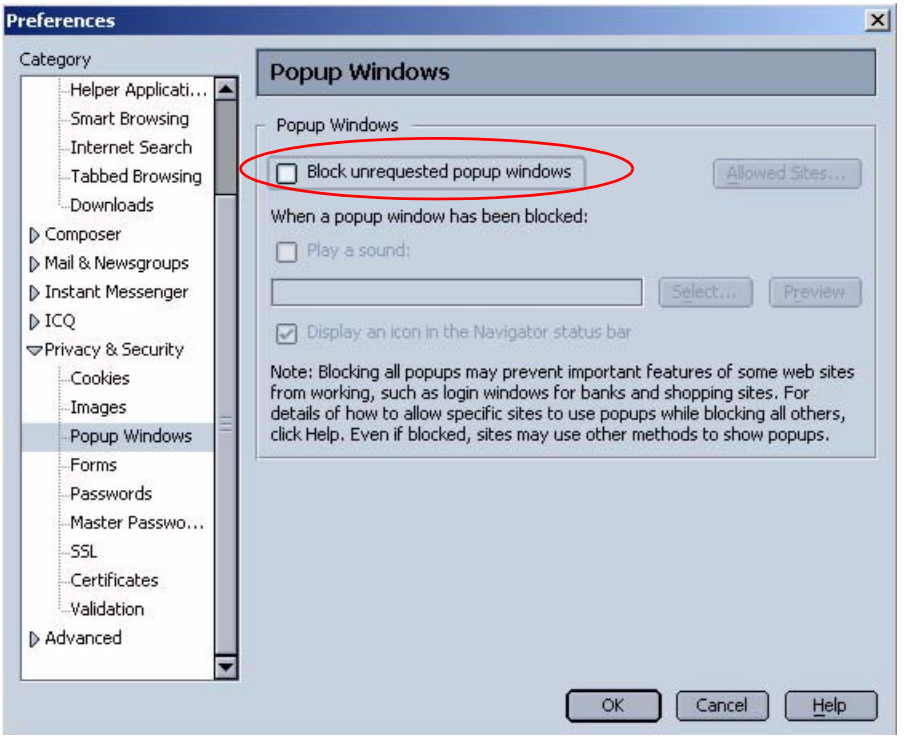
You can also check if pop-up blocking is disabled in the **Popup Windows** screen in the **Privacy & Security** directory.

1 In Netscape, click **Edit** and then **Preferences**.

2 Click the **Privacy & Security** directory and then select **Popup Windows**.

3 Clear the **Block unrequested popup windows** check box.

Figure 288 Popup Windows



4 Click **OK** to save this setting.

Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

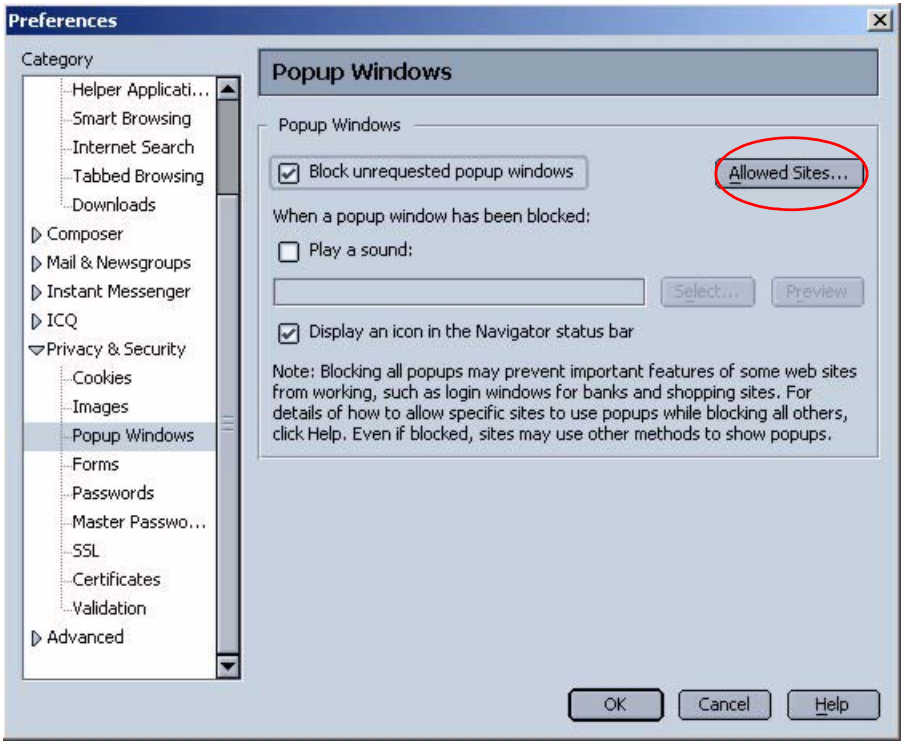
1 In Netscape, click **Edit** and then **Preferences**.

2 In the **Privacy & Security** directory, select **Popup Windows**.

3 Make sure the **Block unrequested popup windows** check box is selected.

4 Click the **Allowed Sites...** button.

Figure 289 Popup Windows



5 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.1.1.

6 Click **Add** to move the IP address to the **Site** list.

Figure 290 Allowed Sites



7 Click **OK** to return to the **Popup Windows** screen.

8 Click **OK** to save this setting.

Netscape Java Permissions and JavaScript

If pages of the WebGUI do not display properly in Netscape, check that JavaScript and Java permissions are enabled.

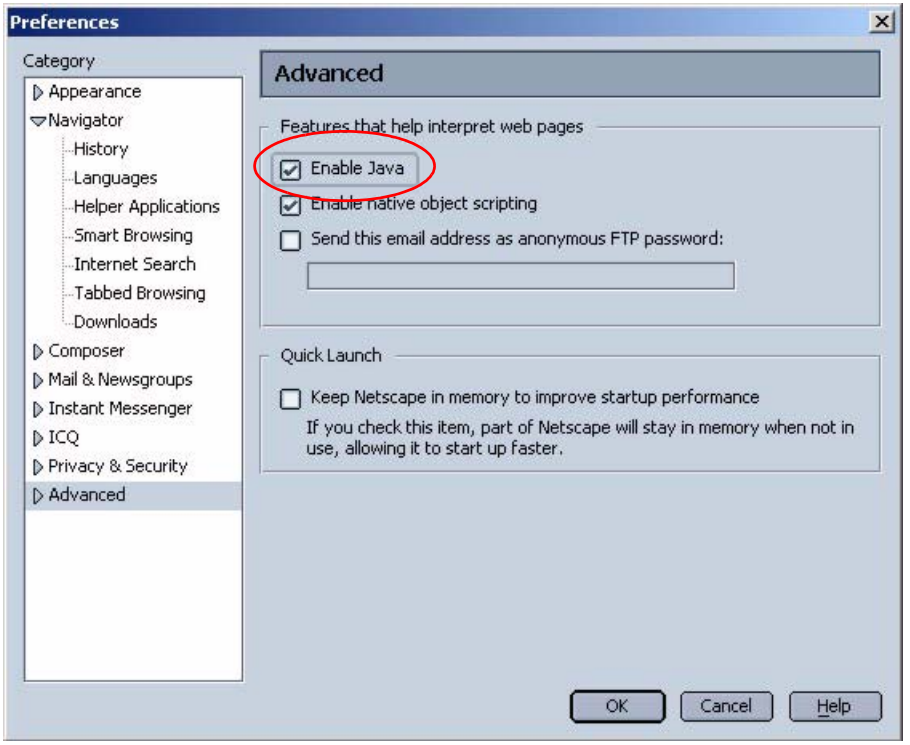
1 In Netscape, click **Edit** and then **Preferences**.

2 Click the **Advanced** directory.

3 In the **Advanced** screen, make sure the **Enable Java** check box is selected.

4 Click **OK** to close the window.

Figure 291 Advanced

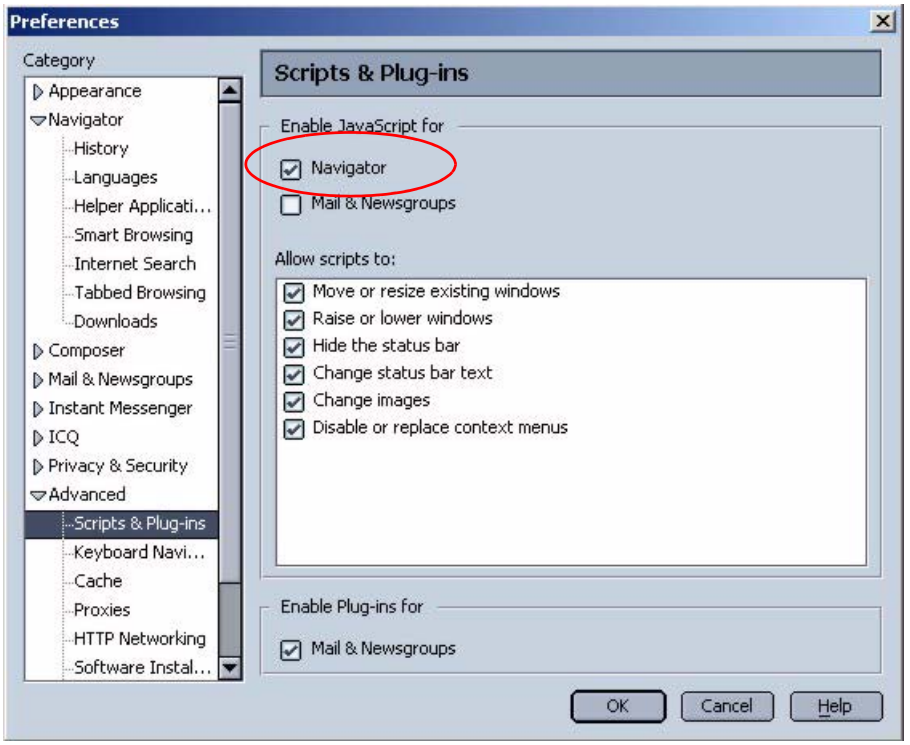


5 Click the **Advanced** directory and then select **Scripts & Plug-ins**.

6 Make sure the **Navigator** check box is selected in the enable JavaScript section.

7 Click **OK** to close the window.

Figure 292 Scripts & Plug-ins



Appendix B
Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

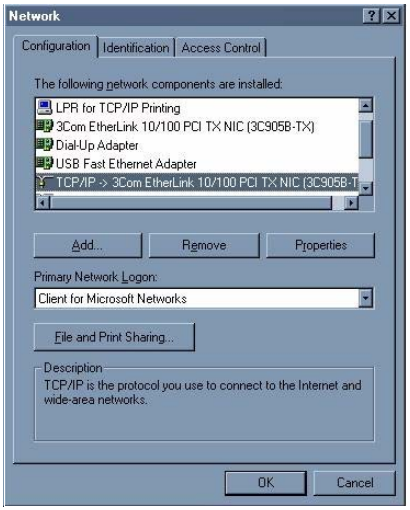
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Contivity 221's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

Figure 293 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

a In the **Network** window, click **Add**.

b Select **Adapter** and then click **Add**.

c Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

a In the **Network** window, click **Add**.

b Select **Protocol** and then click **Add**.

c Select **Microsoft** from the list of **manufacturers**.

d Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

a Click **Add**.

b Select **Client** and then click **Add**.

c Select **Microsoft** from the list of manufacturers.

d Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

e Restart your computer so the changes you made take effect.

Configuring

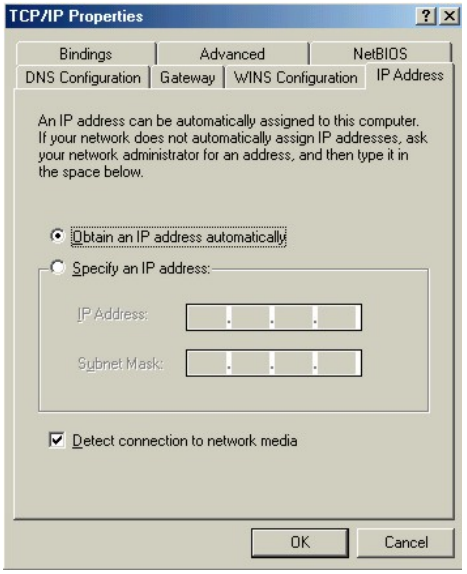
1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

— If your IP address is dynamic, select **Obtain an IP address automatically**.

— If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 294 Windows 95/98/Me: TCP/IP Properties: IP Address

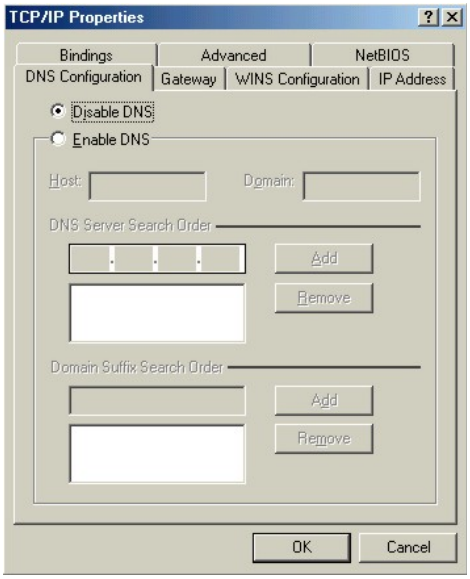


3 Click the **DNS** Configuration tab.

— If you do not know your DNS information, select **Disable DNS**.

— If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 295 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

   — If you do not know your gateway's IP address, remove previously installed gateways.

   — If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your Contivity 221 and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

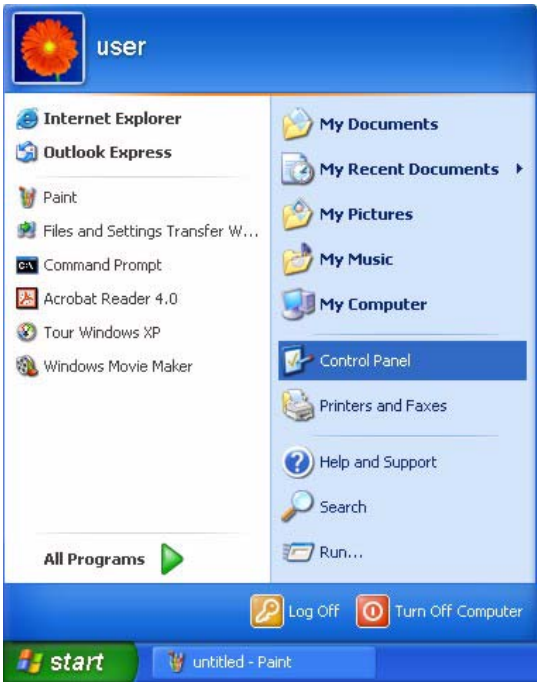
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

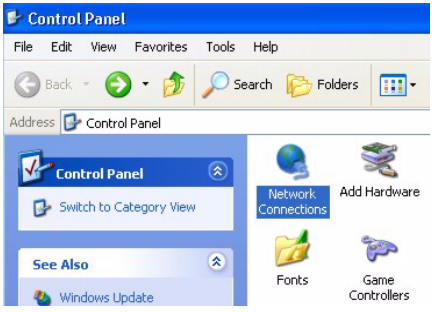
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 296 Windows XP: Start Menu



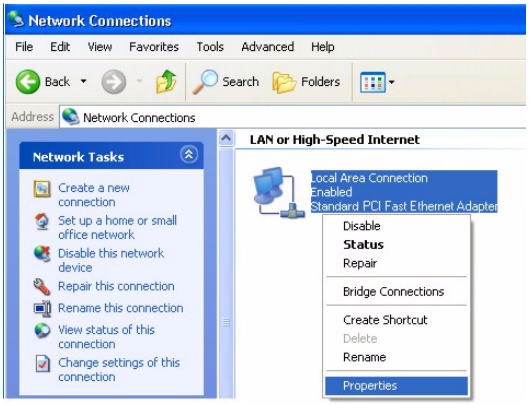
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 297 Windows XP: Control Panel



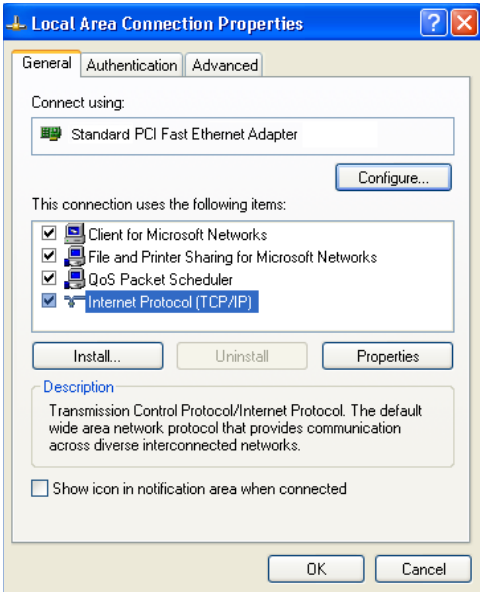
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 298 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

Figure 299 Windows XP: Local Area Connection Properties

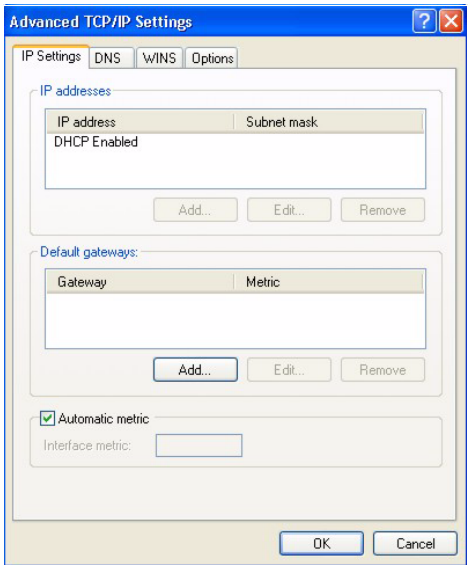


5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

— If you have a dynamic IP address click **Obtain an IP address automatically**.

— If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

Figure 300 Windows XP: Advanced TCP/IP Settings



6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Setting**s tab and click **OK**.

› Do one or more of the following if you want to configure additional IP addresses:

— In the **IP Settings** tab, in IP addresses, click **Add**.

— In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

— Repeat the above two steps for each IP address you want to add.

— Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

— In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

— Click **Add**.

— Repeat the previous three steps for each default gateway you want to add.

— Click **OK** when finished.

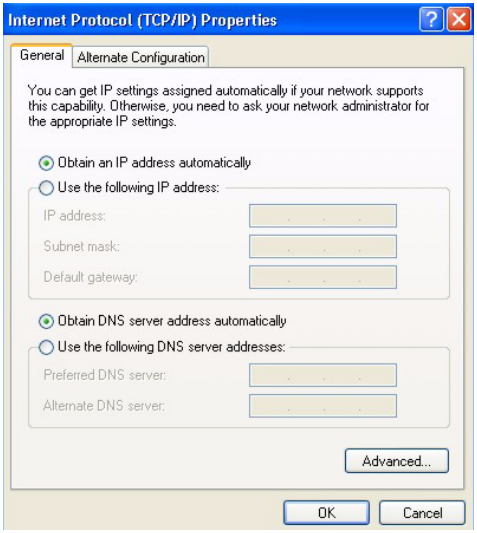
7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

— Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

— If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 301 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

10 Turn on your Contivity 221 and restart your computer (if prompted).

Verifying Settings

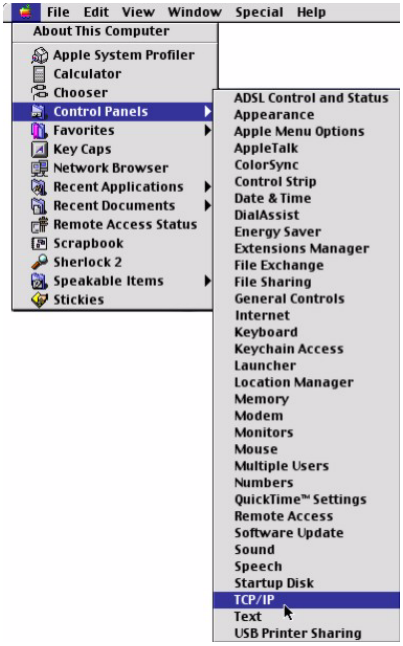
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

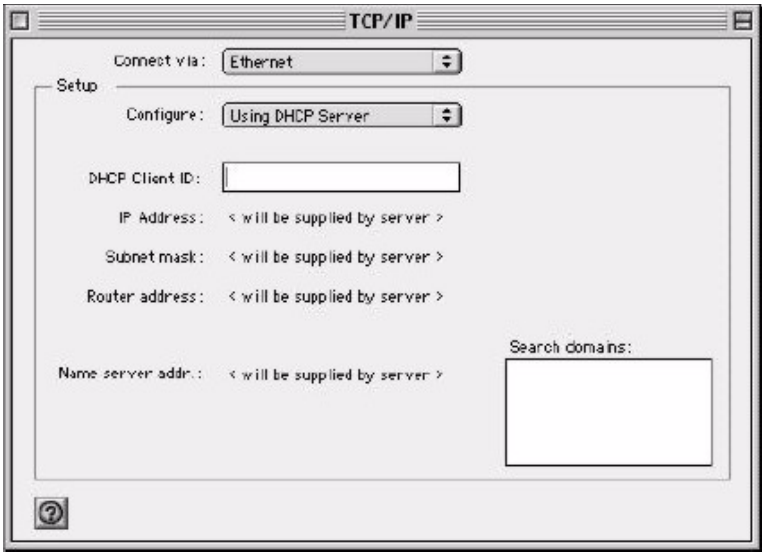
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 302 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 303 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

— From the **Configure** box, select **Manually**.

— Type your IP address in the **IP Address** box.

— Type your subnet mask in the **Subnet mask** box.

— Type the IP address of your Contivity 221 in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your Contivity 221 and restart your computer (if prompted).

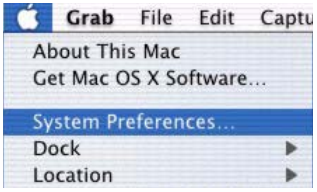
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 304 Macintosh OS X: Apple Menu



2 Click **Network** in the icon bar.

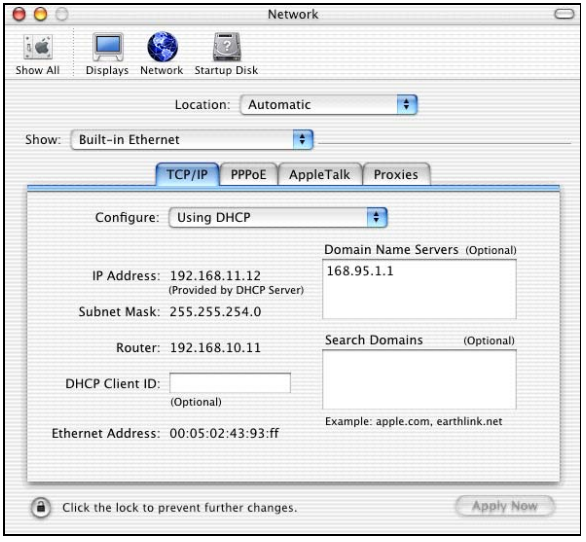
— Select **Automatic** from the **Location** list.

— Select **Built-in Ethernet** from the **Show** list.

— Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 305 Macintosh OS X: Network



4 For statically assigned settings, do the following:

— From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Contivity 221 in the **Router address** box.

5. Click **Apply Now** and close the window.
6. Turn on your Contivity 221 and restart your computer (if prompted).

Verifying Settings

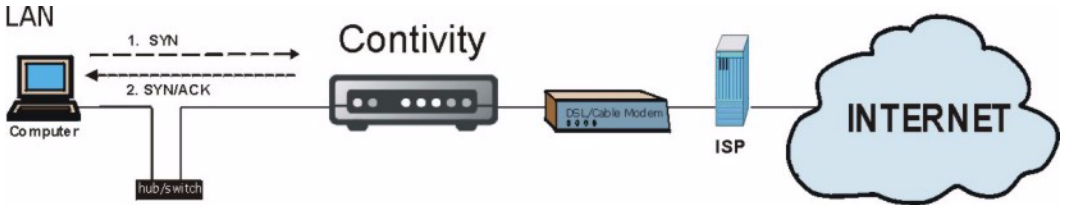
Check your TCP/IP properties in the **Network** window.

Appendix C
Triangle Route

The Ideal Setup

When the firewall is on, your Contivity 221 acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the Contivity 221 to protect your LAN against attacks.

Figure 306 Ideal Setup



The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the “triangle route” problem may occur. The steps below describe the “triangle route” problem.

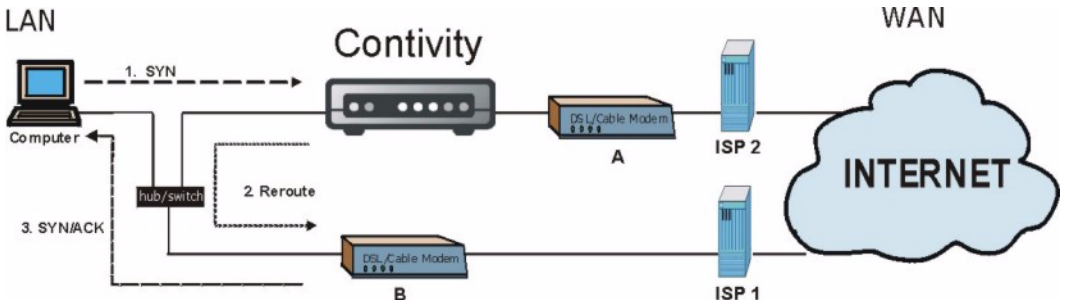
1 A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.

2 The Contivity 221 reroutes the SYN packet through Gateway **B** on the LAN to the WAN.

3 The reply from the WAN goes directly to the computer on the LAN without going through the Contivity 221.

As a result, the Contivity 221 resets the connection, as the connection has not been acknowledged.

Figure 307 "Triangle Route" Problem



The "Triangle Route" Solutions

This section presents you two solutions to the "triangle route" problem.

IP Aliasing

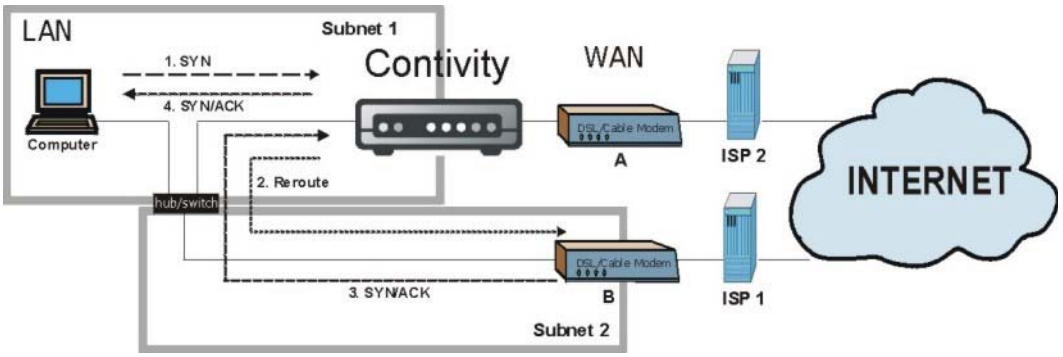
IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your Contivity 221 supports up to three logical LAN interfaces with the Contivity 221 being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning network traffic must pass through the Contivity 221 to your LAN. The following steps describe such a scenario.

1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.

2 The Contivity 221 reroutes the packet to Gateway B, which is in Subnet 2.

3 The reply from WAN goes through the Contivity 221 to the computer on the LAN in Subnet 1.

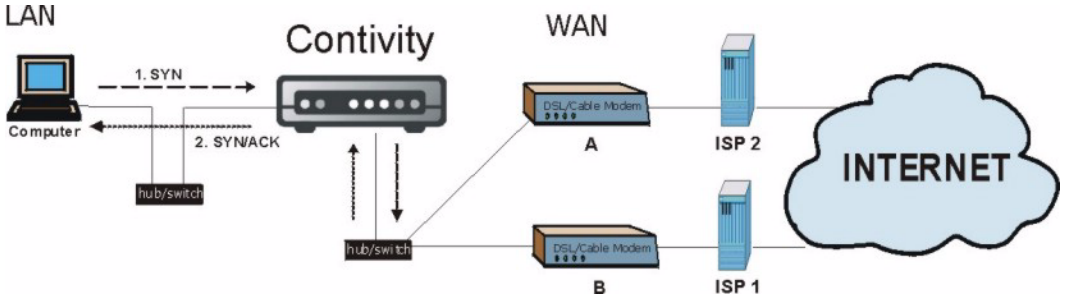
Figure 308 IP Alias



Gateways on the WAN Side

A second solution to the “triangle route” problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your Contivity 221 to your LAN. Therefore your LAN is protected.

Figure 309 Gateways on the WAN Side



Appendix D
Importing Certificates

This appendix shows importing certificates examples using Internet Explorer 5.

Import Contivity 221 Certificates into Netscape Navigator

In Netscape Navigator, you can permanently trust the Contivity 221's server certificate by importing it into your operating system as a trusted certification authority.

Select **Accept This Certificate Permanently** in the following screen to do this.

Figure 310 Security Certificate



Importing the Contivity 221's Certificate into Internet Explorer

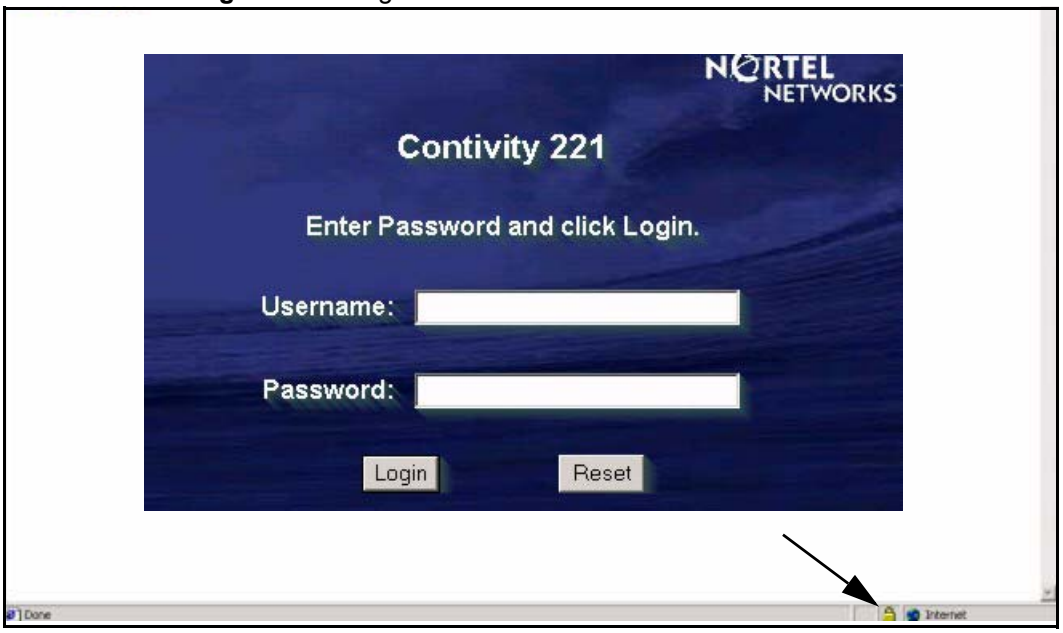
For Internet Explorer to trust a self-signed certificate from the Contivity 221, simply import the self-signed certificate into your operating system as a trusted certification authority.

To have Internet Explorer trust a Contivity 221 certificate issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certification authority.

The following example procedure shows how to import the Contivity 221's (self-signed) server certificate into your operating system as a trusted certification authority.

1 In Internet Explorer, double click the lock shown in the following screen.

Figure 311 Login Screen



2 Click **Install Certificate** to open the **Install Certificate** wizard.

Figure 312 Certificate General Information before Import



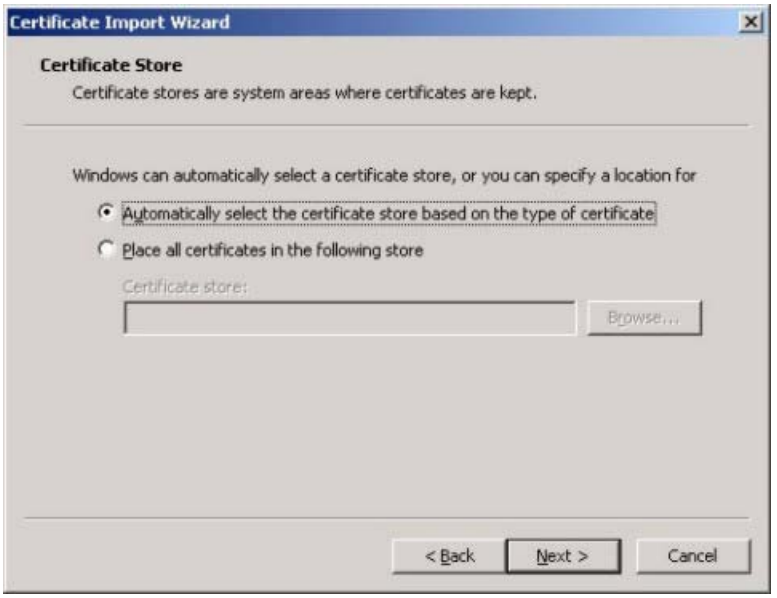
3 Click **Next** to begin the **Install Certificate** wizard.

Figure 313 Certificate Import Wizard 1



4 Select where you would like to store the certificate and then click **Next**.

Figure 314 Certificate Import Wizard 2



5 Click **Finish** to complete the **Import Certificate** wizard.

Figure 315 Certificate Import Wizard 3



6 Click **Yes** to add the Contivity 221 certificate to the root store.

Figure 316 Root Certificate Store

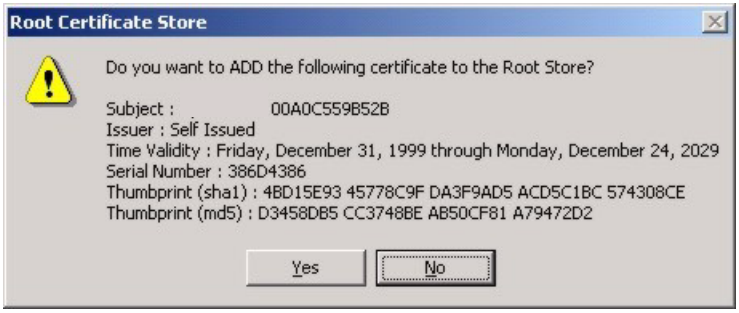


Figure 317 Certificate General Information after Import



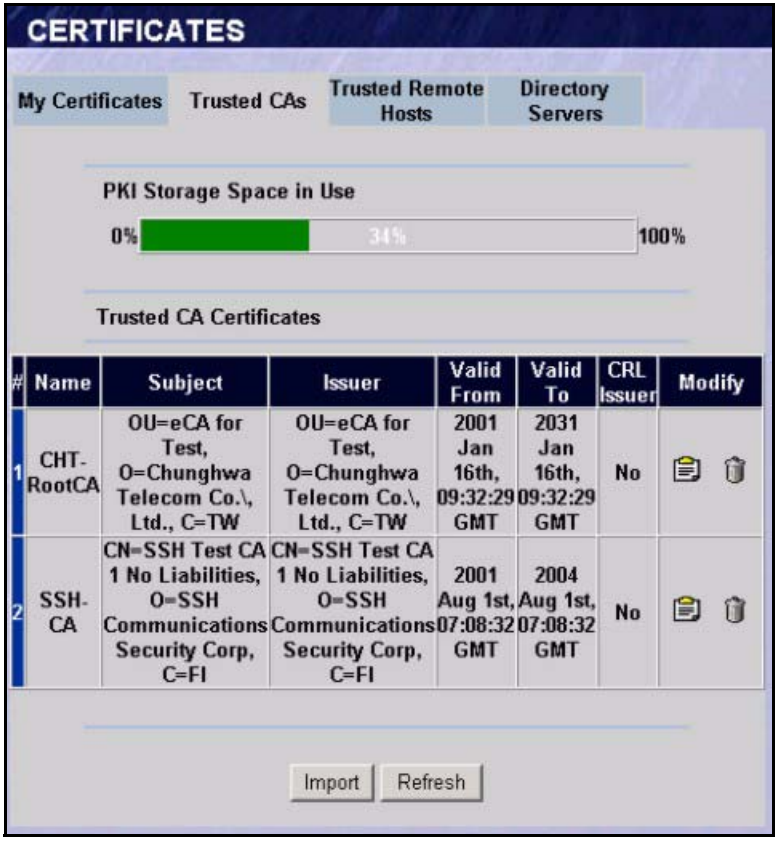
Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the Contivity 221.

You must have imported at least one trusted CA to the Contivity 221 in order for the **Authenticate Client Certificates** to be active (see Chapter 14 Certificates for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the Contivity 221 (see the Contivity 221's **Trusted CA** WebGUI screen).

Figure 318 Contivity 221 Trusted CA Screen

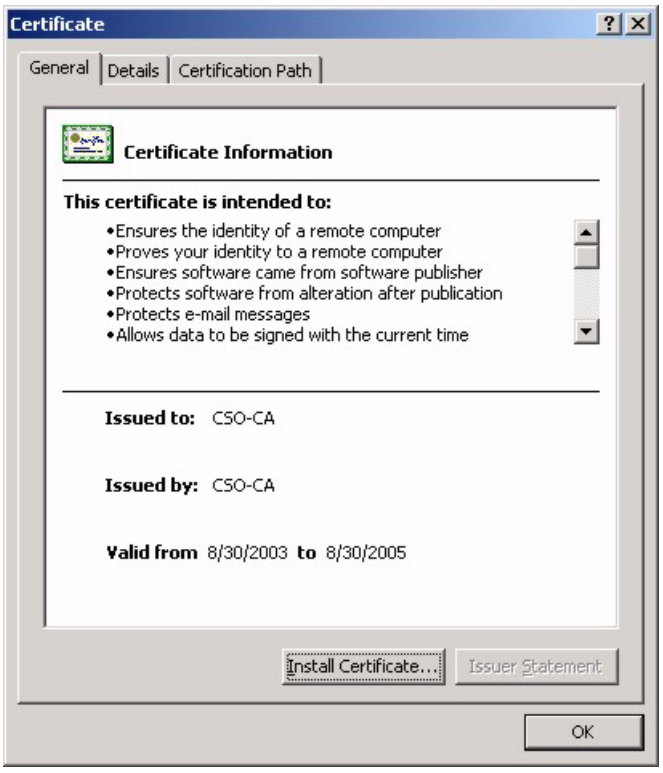


The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

Figure 319 CA Certificate Example



2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

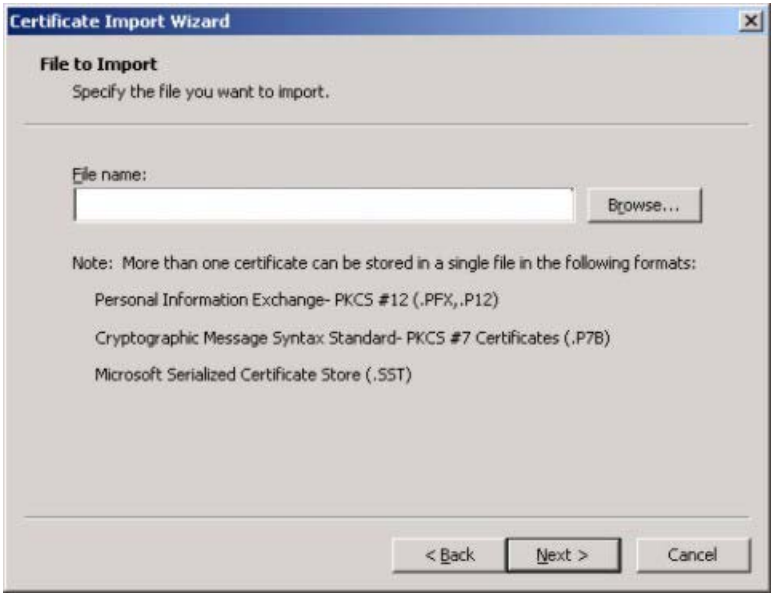
1 Click **Next** to begin the wizard.

Figure 320 Personal Certificate Import Wizard 1



2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

Figure 321 Personal Certificate Import Wizard 2



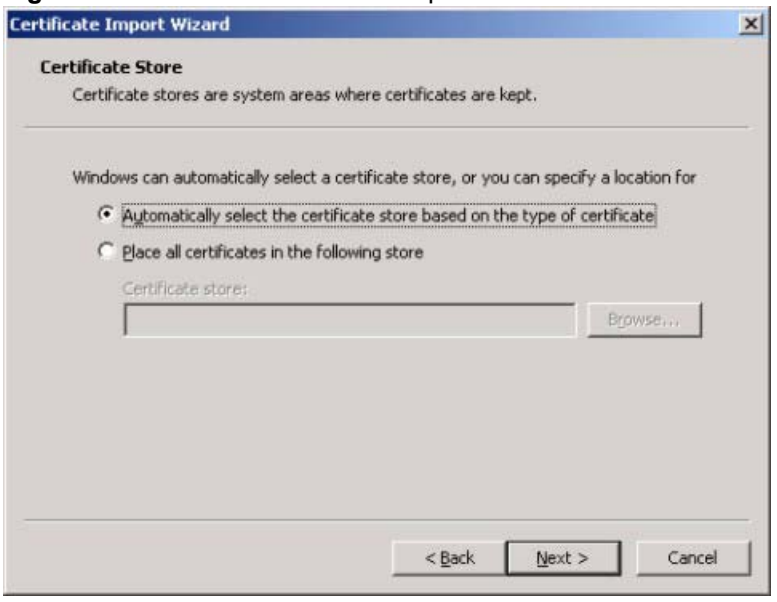
3 Enter the password given to you by the CA.

Figure 322 Personal Certificate Import Wizard 3



4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

Figure 323 Personal Certificate Import Wizard 4



5 Click **Finish** to complete the wizard and begin the import process.

Figure 324 Personal Certificate Import Wizard 5



6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 325 Personal Certificate Import Wizard 6



Using a Certificate When Accessing the Contivity 221 Example

Use the following procedure to access the Contivity 221 via HTTPS.

1 Enter ‘https://Contivity 221 IP Address/ in your browser’s web address field.

Figure 326 Access the Contivity 221 Via HTTPS



2 When **Authenticate Client Certificates** is selected on the Contivity 221, the following screen asks you to select a personal certificate to send to the Contivity 221. This screen displays even if you only have a single certificate as in the example.

Figure 327 SSL Client Authentication



3 You next see the Contivity 221 login screen.

Figure 328 Contivity 221 Secure Login Screen



Appendix E
PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

It provides you with a familiar dial-up networking (DUN) user interface.

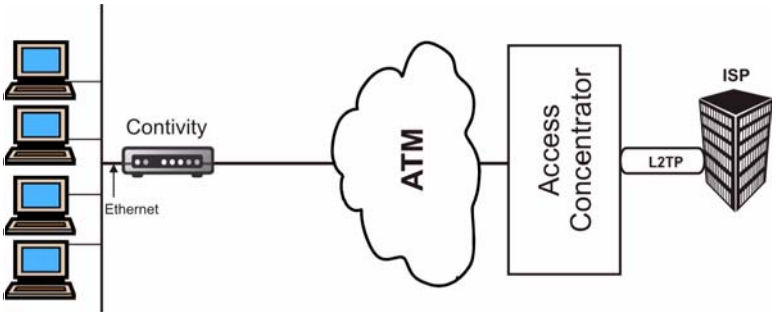
It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

Figure 329 Single-PC per Router Hardware Configuration



How PPPoE Works

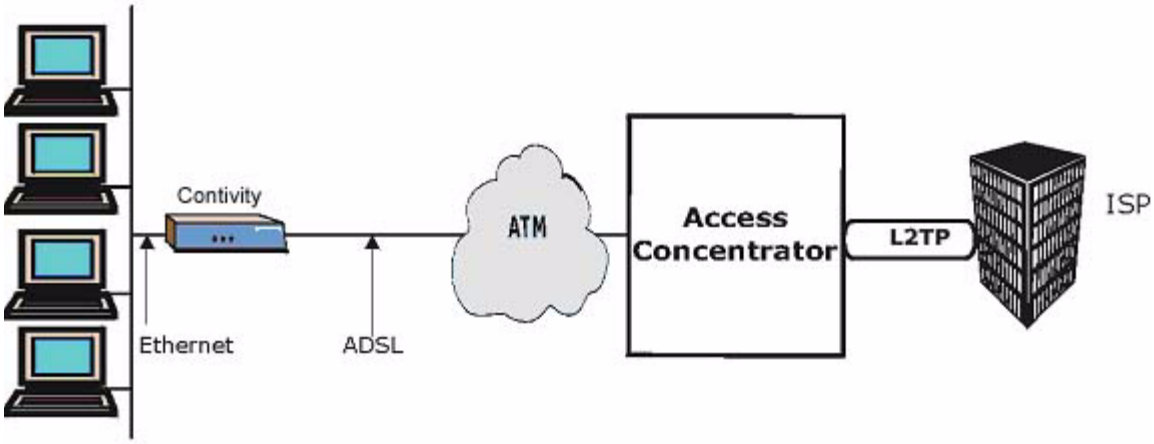
The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

Contivity 221 as a PPPoE Client

When using the Contivity 221 as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

Figure 330 Contivity 221 as a PPPoE Client



Appendix F
PPTP

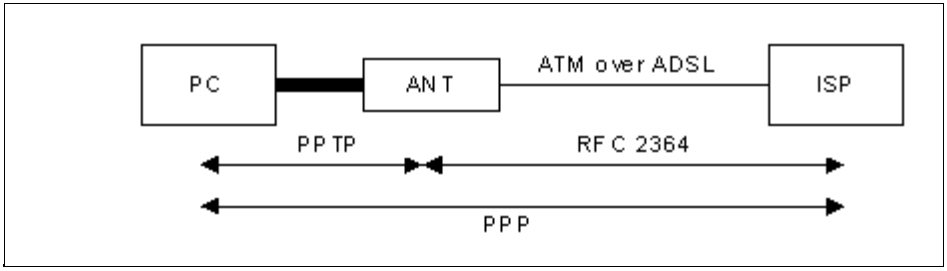
What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364) The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

Figure 331 Transport PPP frames over Ethernet



PPTP and the Contivity 221

When the Contivity 221 is deployed in such a setup, it appears as a PC to the ANT.

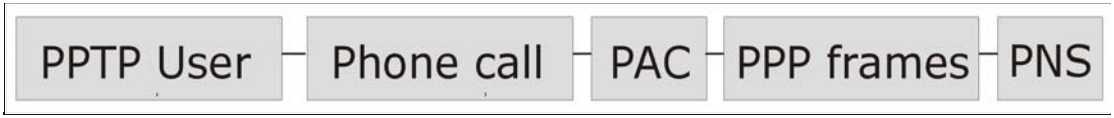
In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the Contivity 221's Internet connection. In SUA/NAT mode, the Contivity 221 is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. You need to configure port forwarding for port 1723 to have the Contivity 221 forward PPTP packets to the server. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The Contivity 221 initializes the PPTP connection hence; there is no need to configure the remote PPTP clients.

PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco’s Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to

the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

Figure 332 PPTP Protocol Overview



Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the PC, and hence the Contivity 221, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

Control & PPP connections

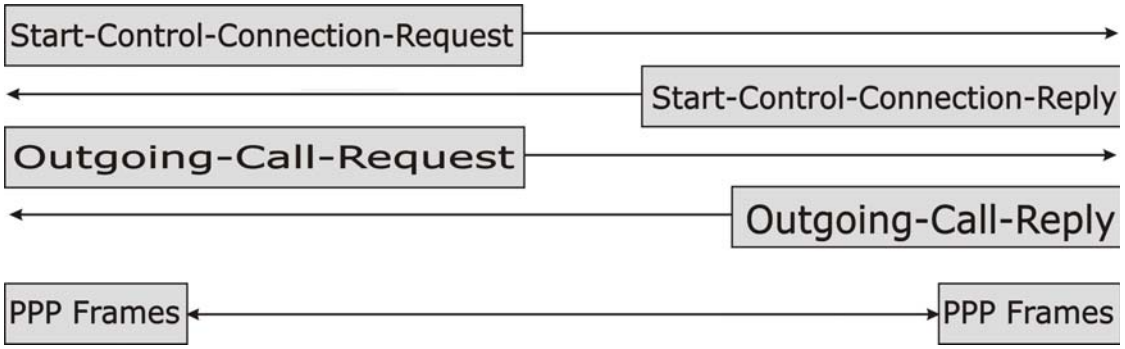
Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a PC and an ANT.

Figure 333 Example Message Exchange between PC and an ANT



PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

Appendix G
Hardware Specifications

Table 168 General Specifications

Power Specification	I/P AC 120V / 60Hz; O/P DC 12V 1200 mA
MTBF	100000 hrs (Mean Time Between Failures)
Operation Temperature	0º C ~ 40º C
Ethernet Specification for WAN	10/100Mbps Half / Full Auto-negotiation
Ethernet Specification for LAN/ VPN Ports	10/100Mbps Half / Full Auto-negotiation, Auto-sensing

Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (DataTerminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The Contivity 221 is DCE when you connect a computer to the console port. The Contivity 221 is DTE when you connect a modem to the dial backup port.

Figure 334 Console/Dial Backup Port Pin Layouts [1]

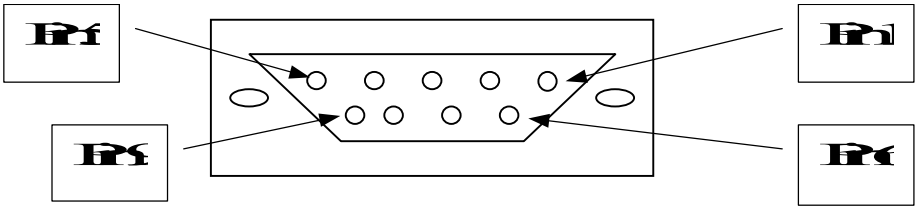
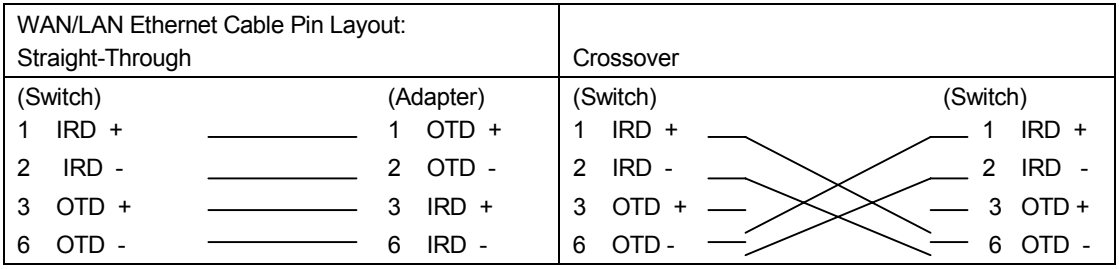


Table 169 Console/Dial Backup Port Pin Assignments

CONSOLE Port RS – 232 (Female) DB-9F	DIAL BACKUP RS – 232 (Male) DB-9M
Pin 1 = NON Pin 2 = DCE-TXD Pin 3 = DCE –RXD Pin 4 = DCE –DSR Pin 5 = GND Pin 6 = DCE –DTR Pin 7 = DCE –CTS Pin 8 = DCE –RTS PIN 9 = NON	Pin 1 = NON Pin 2 = DTE-RXD Pin 3 = DTE-TXD Pin 4 = DTE-DTR Pin 5 = GND Pin 6 = DTE-DSR Pin 7 = DTE-RTS Pin 8 = DTE-CTS PIN 9 = NON.
The CON/AUX port also has these pin assignments. The CON/AUX switch changes the setting in the firmware only and does not change the CON/AUX port's pin assignments.	Contivity 221s with a CON/AUX port also have a 9-pin adaptor for the console cable with these pin assignments on the male end.

[1] Products without flow control only use pins 2,3 and 5.

Figure 335 Ethernet Cable Pin Assignments



Power Adaptor Specifications

Table 170 North American AC Power Adaptor Specifications

AC Power Adapter model AD48-1201200DUY
Input power: AC120Volts/60Hz/0.25A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: North American standards
Safety standards: UL, CUL (UL 1950, CSA C22.2 No.234-M90)
AC Power Adapter model AD48-1201200DUY
Input power: AC120Volts/60Hz
Output power: DC12Volts/1.2A
Power consumption: 9 W
Plug: North American standards
Safety standards: UL, CUL (UL1950, CSA C22.2 NO. 234-M90)

Table 171 European Union AC Power Adaptor Specifications

AC Power Adapter model AD-1201200DV
Input power: AC230Volts/50Hz/0.2A
Output power: DC12Volts/1.2A

Table 171 European Union AC Power Adaptor Specifications

Power consumption: 10 W
Plug: European Union standards
Safety standards: TUV, CE (EN 60950)
AC Power Adapter model JAD-121200E
Input power: AC230Volts/50Hz,
Output power: DC12Volts/1.2A
Power consumption: 9 W
Plug: European Union standards
Safety standards: TUV, CE (EN 60950)

Table 172 UK AC Power Adaptor Specifications

AC Power Adapter model AD-1201200DK
Input power: AC230Volts/50Hz/0.2A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: United Kingdom standards
Safety standards: TUV, CE (EN 60950, BS7002)

Table 173 Japan AC Power Adaptor Specifications

AC Power Adapter model JOD-48-1124
Input power: AC100Volts/ 50/60Hz/ 27VA
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: Japan standards
Safety standards: T-Mark

Table 174 Australia and New Zealand AC Power Adaptor Specification

AC Power Adapter model AD-1201200Ds or AD-121200DS
Input power: AC240Volts/50Hz/0.2A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: Australia and New Zealand standards
Safety standards: NATA (AS 3260)

Appendix H
IP Subnetting

IP Addressing

Routers “route” based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class “A” addresses have a 0 in the left most bit. In a class “A” address the first octet is the network number and the remaining three octets make up the host ID.
- Class “B” addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class “B” address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class “C” addresses begin (starting from the left) with 1 1 0. In a class “C” address the first three octets make up the network number and the last octet is the host ID.

- Class “D” addresses begin with 1 1 1 0. Class “D” addresses are used for multicasting. (There is also a class “E” address. It is reserved for future use.)

Table 175 Classes of IP Addresses

IP Address:		Octet 1	Octet 2	Octet 3	Octet 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID



Note: Host IDs of all zeros or all ones are not allowed.

Therefore:

A class “C” network (8 host bits) can have 2^8 –2 or 254 hosts.

A class “B” address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class “A” address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

Table 176 Allowed IP Address Range By Class

Class	Allowed Range of First Octet (Binary)	Allowed Range of First Octet (decimal)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191

Table 176 Allowed IP Address Range By Class

Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

Table 177 "Natural" Masks

Class	Natural Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class "C" address using both notations.

Table 178 Alternative Subnet Mask Notation

Subnet Mask IP Address	Subnet Mask "1" Bits	Last Octet Bit Value
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

	Network number	Host ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000

Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.



Note: In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to form network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

Table 179 Subnet 1

	Network number	**Last Octet Bit Value**
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 180 Subnet 2

	Network number	**Last Octet Bit Value**
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000

Table 180 Subnet 2

Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 – 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0’s is the subnet itself, all 1’s is the broadcast address on the subnet).

Table 181 Subnet 1

	Network number	**Last Octet Bit Value**
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000

Table 181 Subnet 1

Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62

Table 182 Subnet 2

	Network number	**Last Octet Bit Value**
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 183 Subnet 3

	Network number	**Last Octet Bit Value**
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 184 Subnet 4

	Network number	**Last Octet Bit Value**
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Table 185 Eight Subnets

Subnet	Subnet Address	First Address	Last Address	Broadcast Address
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

The following table is a summary for class “C” subnet planning.

Table 186 Class C Subnet Planning

No. “Borrowed” Host Bits	Subnet Mask	No. Subnets	No. Hosts per Subnet
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class “A” and class “B” addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets (see Table 175) available for subnetting.

The following table is a summary for class “B” subnet planning.

Table 187 Class B Subnet Planning

No. “Borrowed” Host Bits	Subnet Mask	No. Subnets	No. Hosts per Subnet
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix I
Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or nortelnetworks.com for more detailed information on these commands.



Note: Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.

  For example,

  ```
  sys filter netbios config <type> <on|off>
  ```

  means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Sys Commands

The following table lists and describes the system commands. Each of these commands must be preceded by `sys` when you use them. For example, type `sys stdio 60` to set the management session inactivity timeout to 60 minutes.

Table 188 Sys Commands

Command			Description
atsh			Displays the MRD field.
callhist			
	display		Displays the call history.
	remove	<index>	Removes an entry from the call history.
client			
	name	[name]	Sets or displays the client login name.
	password	[password]	Sets or displays the client login password.
countrycode		[countrycode]	Sets or displays the country code.
datetime			
	date	[year month date]	Sets or displays the system's current date.
	time	[hour [min [sec]]]	Sets or displays the system time.
	period	[day]	Sets how often the Contivity 221 gets the date and time from the time server.
	sync		Has the Contivity 221 get the date and time from the time server.
domainname			Displays the domain name that the device sends to the LAN DHCP clients.
edit		<filename>	Edits the system preset text file such as autoexec.net.
extraphnum			Maintains extra phone numbers for outgoing (dial backup) calls.
	add	<set 1-3> <1st phone num> [2nd phone num]	Add extra phone numbers.
	display		Display the extra phone numbers.

Table 188 Sys Commands

Command			**Description**
	node	<num>	Sets all extend phone numbers to remote node <num>.
	remove	<set 1-3>	Remove extra phone numbers.
	reset		Resets node and mask.
feature			Displays a list of the device's major features.
firewall			See "Sys Firewall Commands for information on the system firewall commands.
hostname		[hostname]	Sets or displays the system name.
logs			
	category		
		access [0:none/1:log/ 2:alert/3:both]	Record and/or send alerts for access control logs.
		attack [0:none/1:log/ 2:alert/3:both]	Record and/or send alerts for firewall attack logs.
		cdr [0:none/1:log]	Records Call Detail Record logs.
		display	Displays the category settings.
		error [0:none/1:log/ 2:alert/3:both]	Record and/or send alerts for system error logs.
		icmp [0:none/1:log]	Records ICMP logs.
		ipsec [0:none/1:log/ 2:alert/3:both]	Record the access control logs
		ike [0:none/1:log/ 2:alert/3:both]	Records and/or sends alerts for access control logs.
		javablocked [0:none/ 1:log]	Record the java etc. blocked logs.
		mten [0:none/1:log]	Record the system maintenance logs.
		packetfilter [0:none/ 1:log]	Records the packet filter logs.
		ppp [0:none/1:log]	Records the PPP logs.
		remote [0:none/1:log]	Records the remote management logs.
		tcpreset [0:none/1:log]	Records the TCP reset logs.
		upnp [0:none/1:log]	Record the UPnP logs.

Table 188 Sys Commands

Command			Description
		urlblocked [0:none/ 1:log/2:alert/3:both]	Records and/or sends alerts for web access blocked logs.
		urlforward [0:none/ 1:log]	Records web access forward logs.
	clear		Clear the log.
	display	[access|attack|error|ike|ipsec|javablocked|mten|packetfilter|pki|tcpreset|tls|upnp|urlblocked|urlforward]	Display all logs or specify a category of logs.
	errlog		
		clear	Clears the error log.
		disp	Displays the error log.
		online	Turns the error log online display on/ off.
	load		Loads the log settings buffer. Use this command before you configure the log settings. Use sys logs save after you configure the log settings.
	mail		
		alertAddr [mail address]	Send alerts to this e-mail address.
		clearLog [0:no/1:yes]	Enable the switch to clear the log after sending logs via e-mail.
		display	Displays the logs and alerts mail settings.
		logAddr [mail address]	Send logs to this e-mail address.
		schedule display	Displays the mail schedule.
		schedule hour [0-23]	Sets the hour to send logs.
		schedule minute [0-59]	Sets the minute to send the logs.
		schedule policy [0:full/ 1:hourly/2:daily/ 3:weekly/4:none]	Sets the mail schedule policy.
		schedule week [0:sun/ 1:mon/2:tue/3:wed/ 4:thu/5:fri/6:sat]	Sets the day of the wee for sending weekly logs.

Table 188 Sys Commands

Command			Description
		server [domainName/IP]	Sets the domain name or IP address of the mail server to which to send the logs.
		subject [mail subject]	Sets the log e-mail's subject.
	save		Save the log settings from the buffer.
	syslog		
		active [0:no/1:yes]	Enables/disables syslog logging.
		display	Displays the syslog settings.
		facility [Local ID(1-7)]	Specifies the file to which the device logs the syslog messages.
		server [domainName/IP]	Specifies the IP address of the syslog server to which to send the syslogs.
	consolidate		
		switch <0:on|1:off>	Turns log consolidation on or off.
		period	Sets the consolidation period (in seconds).
		msglist	Displays the consolidated messages.
	updateSvrIP	<minute>	Sets how often to resolve the mail and/ or syslog server domain name to an IP address.
	switch		
		bmlog <0:no|1:yes>	Turns the broadcast/multicast log on or off.
		display	Displays switch settings.
		trilog <0:no|1:yes>	Turns triangle route logging on or off.
mbuf			These commands are for troubleshooting the memory buffer for leakage or corruption.
	link	link	Displays the link list (chain of connections) of the mbufs (data structures representing packets queued in the system).
	pool	[id] [type] <state> <qid> <num>	Displays the mbufs in the specified pool.
	status		Displays the system memory buffer's general status.

Table 188 Sys Commands

Command			Description
	disp	[addr]<0|1>	Displays the contents of the specified mbuf.
	cnt	disp	Displays the mbuf count.
		clear	Clears the mbuf count.
	debug	[on|off]	Turns the system memory buffer debug flag on/off.
rn			
	accessblock		Blocks access to a remote node.
	load	<entry no.>	Loads remote node information.
	disp	<entry no.>(0:working buffer)	Displays remote node information.
	nat	<none|sua|full_feature>	Configure remote node NAT.
	nailup	<no|yes>	Configure a remote node connection to be nailed up (always on).
	mtu	<value>	Sets the remote node Maximum Transmission Unit.
	save	[entry no.]	Save remote node information.
stdio		[minute]	Sets or displays the management terminal idle timeout value.
tos			
	display		Shows all runtime Temporarily Open Sessions
	debug		Turn TOS debug message on or off.
	listPerHost		Displays all hosts session counts.
	sessPerHost		Sets the session per host limit.
	timeout		
		display	Displays all TOS (Temporarily Open Session) timeout information.
		icmp	Sets the ICMP session idle timeout value.
		igmp	Sets the IGMP session idle timeout value.
		tcpsyn	Sets the SYN TCP session idle timeout value.

Table 188 Sys Commands

Command			**Description**
		tcp	Sets the TCP session idle timeout value.
		tcpfin	Sets the TCP FIN session idle timeout value.
		udp	Sets the UDP session idle timeout value.
		gre	Sets the GRE session idle timeout value.
		esp	Sets the ESP session idle timeout value.
		ah	Sets the AH session idle timeout value.
		others	Sets the idle timeout value for other sessions.
trcdisp		parse, brief, disp	Sets the level of detail that should be displayed. “parse” displays the most detail and “disp” displays the least.
trclog			
	switch	[on|off]	Enables/disables the system trace log or displays the current setting.
	online	[on|off]	Enables/disables the trace log onscreen display (for example in the telnet management window).
	level	[level]	Sets the level (1-10) of trace logs (1 shows the least) to display.
	type	<bitmap>	Use hexadecimal characters to set the type of trace logs to record.
	disp		Shows the trace log.
	clear		Erases the trace log.
	call		Shows call events.
	encapmask	[mask]	Shows which type of encapsulation the trace log records or sets it if you specify the encapsulation’s hexadecimal character.
trcpacket			Use trace packet to capture parts of packets in order to see the packet flow from one interface to another.
	create	<entry> <size>	Creates a packet trace buffer.

Table 188 Sys Commands

Command			Description
	destroy		Removes the packet trace buffer.
	channel	<name> [none|incoming|outgoing|bothway]	Sets the packet trace direction for a given channel.
	string	[on|off]	Enables/disables the sending of a log to the trace packet buffer when configuration changes are made or displays the current setting.
	switch	[on|off]	Enables/disables packet trace or displays the current setting.
	disp		Displays the trace packets.
	udp		Sends the trace packets to another system using UDP.
	udp switch	[on|off]	Enables/disables the sending of the trace packets to another system using UDP or displays the current setting.
	udp addr	<addr>	Sets the target IP address for sending trace packets using UDP.
	udp port	<port>	Sets the UDP port (should match that of the target IP address) for sending trace packets using UDP.
	parse	[[start_idx], end_idx]	Displays detailed packet details of the packet range specified.
	brief		Displays a brief listing of packet contents.
version			Displays the RAS code and driver versions.
view		<filename>	Displays the specified text file.
wdog			
	switch	[on|off]	Turns the watchdog firmware protection feature on or off.
	cnt	[value]	Sets (0-34463) or displays the current watchdog count (in 1.6 sec units).
romreset			Restores the factory default configuration file.
	server		Use these commands to configure remote server management.

Table 188 Sys Commands

Command			**Description**
		access <telnet|ftp|web|icmp|snmp|dns> <value>	Sets the server access type.
		load	Loads server information.
		disp	Displays server information.
		port <telnet|ftp|web|snmp> <port>	Sets the server port.
		save	Saves server information.
		secureip <telnet|ftp|web|icmp|snmp|dns> <ip>	Sets server secure IP address.
pwderrtm		[minute]	Sets or displays the password error blocking timeout value.
upnp			
	active	[0:no/1:yes]	Activates or deactivates the saved UPnP settings.
	config	[0:deny/1:permit]	Allow users to make configuration changes through UPnP.
	display		Displays UPnP information
	firewall	[0:deny/1:pass]	Allow UPnP to pass through the firewall.
	load		Saves UPnP information.
	reserve	[0:deny/1:permit]	
	save		Saves UPnP information.
cmgr			The connection monitor controls dial-up services (PPPoE and PPTP).
	trace	disp <ch-name>	Shows a channel's connection trace.
		clear <ch-name>	Clears a channel's connection trace.
	cnt	<ch-name>	Shows the channel connection related counter.
socket			Displays the system socket's ID #, type, control block address (PCB), IP address and port number of peer device connected to the socket (Remote Socket) and task control block (Owner).

Table 188 Sys Commands

Command			Description
filter			
	netbios		
		disp	Displays the current NetBIOS filter modes.
		config <0:Between LAN and WAN/ 3: IPSec Pass through/4: Trigger Dial> <on|off>	Sets NetBIOS filters.
roadrunner			
	debug	<level>	Enables/disables roadrunner service. 0: disable (default)1: enable
	display	<iface name>	Displays roadrunner information iface-name: enif0, wanif0
	restart	<iface name>	Restarts roadrunner.
ddns			
	debug	<level>	Enables/disables DDNS service.
	display	<iface name>	Displays DDNS information.
	restart		Restarts DDNS.
	logout		This command has no effect.
cpu			
	display		Displays the CPU's utilization.

Device Commands

The following table lists and describes the device commands. Each of these commands must be preceded by `dev` when you use them. For example, type `dev dial 3` to dial remote node 3.

Table 189 Device Commands

Command			Description
dev			
	channel		

Table 189 Device Commands

		drop <channel_name>	Drops a dial-up connection's channel.
	dial	<node#>	Dials a dial up (i.e. PPPoE or PPTP) remote node.

Exit Command

Table 190 Exit Command

Command	Description
exit	Ends the command interpreter session.

Ethernet Commands

The following table lists and describes the Ethernet commands. Each of these commands must be preceded by `ether` when you use them. For example, type `ether config` to display information on the LAN configuration.

Table 191 Ether Commands

Command			Description
config			Displays LAN configuration information.
driver			
	cnt		
		disp <name>	Displays the Ethernet driver counters.
	status	<ch_name>	Shows the LAN status.
version			Displays the Ethernet device type.
pkttest			These commands test an interface by sending packets and waiting for a reply.
	arp	<ch_name> <ip-addr>	Sends an ARP packet to the specified IP address.

Table 191 Ether Commands

edit			
	load	<1:LAN>	Loads Ethernet (1:LAN) data from the System Parameters Table.
	mtu	<value>	Sets the Ethernet data Maximum Transmission Unit.
	accessblock	<0:disable 1:enable>	Blocks Internet access.
	speed	<auto|10/half|10/full|100/half|100/full>	Sets the Ethernet data speed and duplex.
	save		Saves Ethernet data to the System Parameters Table.
dynamic Port			
	dump		Displays the relationship between physical port and channel.
	set	<port> <type>	Sets physical port belongs to which channel.
	spt		display channel setting stored in SPT.

IP Commands

The following table lists and describes the IP commands. Each of these commands must be preceded by `ip` when you use them. For example, type `ip address` to display the host IP address.

Table 192 IP Commands

Command			**Description**
address		[addr]	Displays the host IP address.
alias		<iface>	Sets an alias for the specified interface.
aliasdis		<0|1>	Disables/enables the alias for the specified interface.
arp			
	status	<iface>	Displays an interface's IP Address Resolution Protocol status.
dhcp		<iface>	

Table 192 IP Commands

Command			Description
	client		
		release	Releases the DHCP client IP address.
		renew	Renews the DHCP client IP address.
	status	[option]	Displays the DHCP status.
dns			
	query	address <ip address>	Displays the domain name of an IP address.
		name <host name>	Displays the IP address of a domain name.
	stats		
		clear	Clears the DNS statistics.
		disp	Displays DNS statistics.
	system		Configures the system DNS server settings.
		display	Shows the system DNS server settings.
		edit <0: first|1: second|2: third> <0:from ISP|1:usr-def|2 :none> [IP addr ess if choosing 1]	Configures the system DNS server settings.
	lan	edit <0: first|1: second|2: third> <0:from ISP|1:usr-def|2 :DNS Relay|3: n one> [IP address if choosing 1]	Configures the LAN DNS server settings.
		display	Shows the LAN DNS server settings.
httpd		debug [on|off]	Enables or disables the HTTP debug flag. This command does not work currently.
icmp			

Table 192 IP Commands

Command			Description
	status		Displays the ICMP statistics counter.
	discovery	<iface> [on|off]	Sets the ICMP router discovery flag.
ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	Configures a network interface.
ping		<hostid>	Pings a remote host.
route			
	status	[if]	Displays the routing table.
	add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	Adds a route.
	addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	Adds an entry to the routing table for the specified interface.
	addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	Adds a private route.
	drop	<host addr> [/ <bits>]	Drops a route.
status			Displays IP statistic counters.
udp			
	status		Displays the UDP status.
rip			These are the Routing Information Protocol commands.
	accept	<gateway>	Drops an entry from the RIP refuse list.
	activate		Enables RIP.
	merge	[on|off]	Sets the RIP merge flag.
	refuse	<gateway>	Adds an entry to the RIP refuse list.

Table 192 IP Commands

Command			Description
	request	<addr> [port]	Sends a RIP request to the specified address and port.
	reverse	[on|off]	RIP Poisoned Reverse.
	status		Displays RIP statistic counters.
	trace		Enables the RIP debug trace.
	mode		
		<iface> in [mode]	Sets the Contivity 221 to use the RIP information it receives.
		<iface> out [mode]	Sets the Contivity 221 to broadcast its routing table.
	dialin_user	[show|in|out|both|none]	Shows the dial-in user RIP direction.
tcp	status		Displays the TCP statistic counters.
telnet		<host>	Telnets to the specified host.
tftp			
	support		Displays whether or not TFTP is supported.
	stats		Displays the TFTP statistics.
traceroute		<host> [ttl] [wait] [queries]	Sends ICMP packets to trace the route of a remote host.
xparent		<join|break>	This command is not in use.
urlfilter			
	enable	[0:no/1:yes]	Enables/disables content filtering.
	dropIcmp	<?>	
	exemptZone		
		display	Displays content filtering exempt zone information.
		actionFlags [type(1-3)][enable/disable]	Enables/disables content filtering exempt zone action flags that determine to which IP addresses to apply content filtering.
		add [ip1] [ip2]	Sets a range of IP addresses to be in the exempt zone.
		delete [ip1] [ip2]	Removes a range of IP addresses from the exempt zone.

Table 192 IP Commands

Command			Description
		reset	Returns the exempt zone settings to the previous configuration.
	customize		Use the customize commands to configure content filtering for trusted web sites, forbidden web sites and keyword blocking.
		display	Displays the content filtering customize action flags.
		actionFlags [act(1-7)] [enable/ disable]	Sets the content filtering customize action flags.
		logFlags [type(1-3)][ena ble/disable]	Sets the content filtering customize log flags.
		add [string] [trust/untrust/ keyword]	Adds a trusted web site, forbidden web site or keyword blocking string.
		delete [string] [trust/untrust/ keyword]	Deletes a trusted web site, forbidden web site or keyword blocking string.
		reset	Return to the default configuration.
tredir			
	failcount	<count>	Sets the number of times that the device may ping the target without a response before forwarding traffic to the backup gateway.
	partner	<ipaddr>	Sets the traffic redirect backup gateway IP address.
	target	<ipaddr>	Sets the IP address that the device uses to test WAN accessibility.
	timeout	<timeout>	Sets the number of seconds the device waits for a response from the target.
	checktime	<period>	Sets the number of seconds the device waits between attempts to connect to the target.
	active	<on|off>	Enables/disables traffic redirect.
	save		Saves traffic redirect configuration.
	disp		Displays the traffic redirect configuration.
	debug	<value>	Sets the traffic redirect debug value.

Table 192 IP Commands

Command			**Description**
rpt			
	start		Start recording reports data.
	stop		Stop recording reports data.
	url		Record the most visited web sites.
	ip		Record the LAN IP addresses that sent and received the most traffic.
	srv		Record the most heavily used protocols or service ports.
stroute			
	display	[rule # | buf]	Displays the list of static routes or detailed information on a specified rule.
	load	<rule #>	Load the specified static route rule into the buffer.
	save		Saves a rule from the buffer to the System Parameters Table.
	config		
		name <site name>	Sets the name for a static route.
		destination <dest addr>[/<bits>] <gateway> [<metric>]	Sets a static route's destination IP address and gateway.
		mask <IP subnet mask>	Sets a static route's subnet mask.
		gateway <IP address>	Sets a static route's gateway IP address.
		metric <metric #>	Sets a static route's metric number.
		private <yes|no>	Turns private mode on or off.
		active <yes|no>	Enables/disables a static route rule.
dropIcmp		[0|1]	Sets whether or not the device allows ICMP fragment packets.
nat			
	loopback	[on|off]	Turns on/off the NAT loopback flag.

Table 192 IP Commands

Command			Description
	reset	<enifX|wanifX>	Resets the NAT table of an interface.
	session	[1-1024]	Sets/displays the number of NAT sessions per host.
	server		
		disp	Displays the NAT server table.
		load <set id>	Loads NAT server information from ROM.
		save	Saves NAT server information to ROM.
		clear <set id>	Clears NAT server information.
		edit active <yes|no>	Sets the NAT server edit active flag.
		edit svrport <start port> [end port]	Sets the server port of the NAT server.
		edit intport <start port> [end port]	Sets the NAT server forward port.
		edit remotehost <start ip> [end ip]	Sets the NAT server remote host IP address.
		edit leasetime [time]	Sets the NAT server lease time.
		edit rulename [name]	Sets the NAT server rule name.
		edit forwardip [ip]	Sets the server IP address of the NAT server.
		edit protocol [protocol id]	Sets the NAT server protocol.
	service		
		irc [on|off]	Turns on/off the irc flag.
	resetport		Resets all NAT server table entries.
	incikeport	[on|off]	Turns on/off the increase ike port flag.
	hashTable	<iface#>	Displays the NAT table information of an interface. X=0, 1.
	natTable	<iface#>	Displays the NAT session table of an interface. X=0, 1, 2.

Table 192 IP Commands

Command			Description
	vpnnat		Displays the virtual IP address information assigned by the remote Contivity VPN switch.
	routing	[0:no|1:yes]	Enables or disables routing (without NAT) between the LAN and WAN interfaces.
igmp			
	debug	[level]	Sets IGMP debug level.
	forwardall	[on|off]	Activates/deactivates IGMP forwarding to all interfaces flag.
	querier	[on|off]	Turns on/off IGMP stop query flag.
	iface		
		<iface> grouptm <timeout>	Sets IGMP group timeout for the specified interface.
		<iface> interval <interval>	Sets IGMP query interval for the specified interface.
		<iface> join <group>	Adds an interface to a group.
		<iface> leave <group>	Removes an interface from a group.
		<iface> query	Sends an IGMP query on the specified interface.
		<iface> rsptime [time]	Sets the IGMP response time.
		<iface> start	Turns on IGMP on the specified interface.
		<iface> stop	Turns off IGMP on the specified interface.
		<iface> ttl <threshold>	Sets the IGMP Time To Live threshold.
		<iface> v1compat [on|off]	Turns on/off IGMP version 1 compatibility on the specified interface.
	robustness	<num>	Sets the IGMP robustness variable.
	status		Displays the IGMP status.
alg			
	display		Shows whether the Application Layer Gateway is enabled or disabled.

Table 192 IP Commands

Command			Description
	siptimeout	<timeout in second> or 0 for no timeout	Sets the SIP timeout period.
	enable	<ALG_FTP|ALG_H323|ALG_SIP>	Turns on the ALG.
	disable	<ALG_FTP|ALG_H323|ALG_SIP>	Turns off the ALG.

PPPoE Commands

The following table lists and describes the PPPoE commands. Each of these commands must be preceded by `poe` when you use them. For example, type `poe status` to display the PPPoE status.

Table 193 PPPoE Commands

Command			Description
poe			
	status	[ch_name]	Displays the PPPoE status.
	dial	<node>	Dials a (PPPoE) remote node.
	drop	<node>	Drops a PPPoE call.
	ether	[rfc|3com]	Sets /displays the PPPoE ether type.

PPTP Commands

The following table lists and describes the PPTP commands. Each of these commands must be preceded by `pptp` when you use them. For example, type `pptp dial myisp` to dial the "myisp" remote node.

Table 194 PPTP Commands

Command			Description
pptp			
	dial	<rn-name>	Dials a (PPTP) remote node.
	drop	<rn-name>	Drops a (PPTP) remote node call.
	tunnel	<tunnel id>	Displays PPTP tunnel information.
	enque	[size]	Sets or displays the PPTP send buffer size.

Configuration Commands

The following table lists and describes the configuration commands. Use these commands to configure the firewall. Each of these commands must be preceded by `config` when you use them. For example, type `config display firewall` to display the firewall settings.

Table 195 Config Commands

Command					Description
display	firewall				Displays all the firewall settings.
		set <set#>			Displays current entries of a set configuration; including timeout values, name, default-permit, and number of rules in the set.
		set <set#>	rule <rule#>		Displays current entries of a rule in a set.
		attack			Displays all the attack alert settings.

Table 195 Config Commands

Command					Description
		e-mail			Displays all the e-mail settings.
		?			Displays all the available sub commands.
		e-mail	mail-server <mail server IP>		Edits the mail server IP to send alerts.
			return-addr <e-mail address>		Edits the mail address for returning an e-mail alert.
			e-mail-to <e-mail address>		Edits the mail address to send the alert.
			policy <full | hourly |daily | weekly>		Edits e-mail schedule when log is full or per hour, day, week.
			day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>		Edits the day to send the log when the e-mail policy is set to weekly.
			hour <0~23>		Edits the hour to send the log when the e-mail policy is set to daily or weekly.
			minute <0~59>		Edits the minute to send to log when the e-mail policy is set to daily or weekly.
			Subject <mail subject>		Edits the e-mail subject.
		attack	send-alert <yes|no>		Activates or deactivates the sending of firewall DoS attacks notification e-mails.

Table 195 Config Commands

Command					Description
			block <yes|no>		Yes: Blocks traffic when the tcp-max-incomplete threshold is exceeded. No: Delete the oldest half-open session when the tcp-max-incomplete threshold is exceeded.
			block-minute <0~255>		Only valid when 'Block' is set to yes. The unit is minutes.
			minute-high <0~255>		Sets the threshold to start deleting old half-opened sessions until reaching the minute-low.
			minute-low <0~255>		Sets the threshold to stop deleting old half-opened session.
			max-incomplete-high <0~255>		Sets the threshold to start to delete old half-opened sessions until reaching the max-incomplete-low.
			max-incomplete-low <0~255>		Sets the threshold to stop deleting the half-opened sessions.
			tcp-max-incomplete <0~255>		Sets the threshold to start executing the block field.
		set <set#>	name <desired name>		Edits the name for a set.
			default-permit <forward|block>		Edits whether a packet is dropped or allowed when it does not match the default set.
			icmp-timeout <seconds>		Edits the timeout for an idle ICMP session before it is terminated.
			udp-idle-timeout <seconds>		Edits the timeout for an idle UDP session before it is terminated.

Table 195 Config Commands

Command					Description
			connection-timeout <seconds>		Edits the wait time for an SYN TCP session before it is terminated.
			fin-wait-timeout <seconds>		Edits the wait time for FIN in concluding a TCP session before it is terminated.
			tcp-idle-timeout <seconds>		Edits the timeout for an idle TCP session before it is terminated.
			log <yes|no>		Turns on/off the sending of a log when the default permit is matched.
			rule <rule#>	permit <forward|block>	Edits whether packets matching this rule are dropped or allowed.
				active <yes|no>	Edits whether a rule is enabled or not.
				protocol <0~255>	Edits the protocol number for a rule. 1=ICMP, 6=TCP, 17=UDP...
				log <none|match|not-match|both>	Sends a log for a rule when the packet none|matches|not match|both the rule.
				alert <yes|no>	Activates or deactivates the notification when a DoS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an e-mail to the SMTP destination address and log an alert.
				srcaddr-single <ip address>	Sets the rule to check for packets with the specified source IP address.

Table 195 Config Commands

Command					Description
				`srcaddr-subnet <ip address> <subnet mask>`	Sets the rule to check for packets with the specified source IP address and subnet mask.
				`srcaddr-range <start ip address> <end ip address>`	Sets the rule to check for packets with a source IP address in the specified range.
				`destaddr-single <ip address>`	Sets the rule to check for packets with the specified destination IP address.
				`destaddr-subnet <ip address> <subnet mask>`	Sets the rule to check for packets with the specified destination IP address and subnet mask.
				`destaddr-range <start ip address> <end ip address>`	Sets the rule to check for packets with a destination IP address in the specified range.
				`tcp destport-single <port#>`	Sets the rule to check for TCP packets with the specified destination port. Repeat this command for non-consecutive port numbers.
				`tcp destport-range <start port#> <end port#>`	Sets the rule to check for TCP packets with a destination port in the specified range.

Table 195 Config Commands

Command					Description
				udp destport-single <port#>	Sets the rule to check for UDP packets with the specified destination port. Repeat this command for non-consecutive port numbers.
				udp destport-range <start port#> <end port#>	Sets the rule to check for UDP packets with a destination port in the specified range.
				desport-custom <desired custom port name>	Sets the custom port name.
delete	firewall	e-mail			Removes all e-mail alert settings.
		attack			Resets all alert settings to defaults.
		set <set#>			Removes a specified set from the firewall configuration.
		set <set#>	rule <rule#>		Removes a specified rule in a set from the firewall configuration.
edit	firewall	active <yes|no>			Activates or deactivates the saved firewall settings.
insert	firewall	e-mail			Inserts e-mail alert settings.
		attack			Inserts attack alert settings.
		set <set#>			Inserts a specified rule set in the firewall configuration.
		set <set#>	rule <rule#>		Inserts a specified rule in a set in the firewall configuration

Table 195 Config Commands

Command					Description
retrieve	firewall				Retrieves the current saved firewall settings.
save	firewall				Saves the current firewall settings.
cli					Displays the command list.
debug	<1|0>				Turns on|off the trace for firewall debug information.

IPSec Commands

The following table lists and describes the IP Sec commands. Each of these commands must be preceded by `ipsec` when you use them. For example, type `ipsec display 3` to display the third IPSec rule if you have it configured.

Table 196 IPSec Commands

Command			Description
debug	<type> <level>		Sets the trace for IPsec debug information type (IKE, IPSec or PKI) and level (1~3 with 3 giving the most detail).
switch	<on|off>		As long as there is one active IPSec rule, all packets will go into the IPSec process to check against the SPD. When this switch is turned on packets will not be put through the IPSec process, even if there are active IPSec rules.
timer			
	chk_input		Adjust auto-timer to check if any inbound IPsec traffic has passed during the specified period. If not, the Contivity 221 will disconnect the tunnel.
	dpdtime		Sets the idle timeout for IPSec connections where the Contivity 221 is waiting for a response from the peer.

Table 196 IPSec Commands

Command			Description
	chk_conn.		Sets the idle timeout for IPSec connections. The system disconnects an IPSec connection with no traffic for the timeout period. The interval is in minutes (2 default) and 0 means the connection never times out.
	update_peer		Sets the auto-timer for updating IPSec rules that use a domain name as the secure gateway IP address. The interval is in minutes (30 default) and 0 means it never updates.
show_runtime	sa		Displays runtime phase 1 and phase 2 SA information.
	spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to the peer's local IP address. This command displays these runtime SPDs.
updatePeerIp			Forces the system to immediately update IPSec rules which use a domain name as the secure gateway IP address.
display	<rule index>		Displays the specified IPSec rule.
policyDisplay	<rule index>		Displays the specified IPSec rule's IP policies.
dial	<rule index>	<policy index>	Triggers the specified phase two connection.
route	lan	<on|off>	After IPSec has processed a packet and sent it to the LAN side, this switch controls whether or not IPSec can be applied to the packet again.
	wan	<on|off>	After IPSec has processed a packet and sent it to the WAN side, this switch controls whether or not IPSec can be applied to the packet again.
load	<rule index>		Edit an IPSec branch office rule with the specified rule number.
save			Saves the IPSec branch office rule.
config			Use these commands to configure the IPSec rule.
	name	<name>	Sets the name of the rule.

Table 196 IPSec Commands

Command			Description
	active	<Yes|No>	Turns the rule on or off.
	negotiationMode	<0:Main | 1:Aggressive>	Sets the negotiation mode.
	natTraversal	<Yes|No>	Turns NAT traversal on or off.
	p1MultiPro	<Yes|No>	Turns phase 1 multiple proposal on or off.
	lcIdType	<0:IP | 1:DNS | 2:Email>	Sets the local ID type.
	lcIdContent	<content>	Sets the local ID content.
	myIpAddr	<IP address>	Sets the My IP Address.
	peerIdType	<0:IP | 1:DNS | 2:Email>	Sets the peer ID type.
	peerIdContent	<content>	Sets the peer ID content.
	secureGwAddr	<IP address | Domain name>	Sets the secure gateway address.
	authMethod	<0:PreSharedKey |1: RSASignature>	Sets the authentication method.
	certificate	<certificate name>	Specifies the certificate to use for authentication.
	preShareKey	<ASCII | 0xHEX>	Type from 8 to 32 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters (preceded by"0x" (zero x), which is not counted as part of the 16 to 62 characters.
	p1EncryAlgo	<0:DES | 1:3DES | 2:AES>	Sets the phase 1 encryption algorithm.
	p1AuthAlgo	<0:MD5 | 1:SHA1>	Sets the phase 1 authentication algorithm.
	p1SaLifeTime	<seconds>	Sets the phase 1 SA lifetime.
	keyGroup	<0:DH1 | 1:DH2>	Sets the key group for phase 1 IKE setup.
	nailUp	<Yes|No>	Turns nailed up on or off.
	activeProtocol	<0:AH | 1:ESP>	Sets the protocol.
	p2MultiPro	<Yes|No>	Turns phase 2 multiple proposal on or off.

Table 196 IPSec Commands

Command			Description
	p2EncryAlgo	<0:Null | 1:DES | 2:3DES | 3:AES>	Sets the phase 2 encryption algorithm.
	p2EncryKeyLen	<0:128 | 1:192 | 2:256>	Sets the phase 2 encryption key length (with AES encryption).
	p2AuthAlgo	<0:MD5 | 1:SHA1>	Sets the phase 2 authentication algorithm.
	p2SaLifeTime	<seconds>	Sets the phase 2 SA lifetime.
	encap	<0:Tunnel | 1:Transport>	Sets the encapsulation mode.
	pfs	<0:None | 1:DH1 | 2:DH2>	Sets Perfect Forward Secrecy.
	antiReplay	<Yes | No>	Turns replay detection on or off.
	connType	<0:Branch Office | 1:Contivity Client>	Specifies whether the rule is for a branch office or Contivity Client VPN connection.
	authOptions	<0:Username Password | 1:Group ID & Password	Sets the Contivity 221 to either send just the user name and password to the remote Contivity VPN switch, or a group ID and password as well.
	onDemand	<on | off>	Sets whether or not outgoing packets can automatically trigger a VPN connection to the remote Contivity VPN switch.
	ODService	[netbios] [ntp] [none]...	Sets which specific services can automatically trigger a VPN connection to the remote Contivity VPN switch.
	groupID	<group ID>	Sets the Contivity Client tunnel's user's group ID.
	groupPasswd	<group password>	Sets the Contivity Client tunnel's user's group password.
	username	<name>	Sets the Contivity Client tunnel's user's user name.
	password	<password>	Sets the Contivity Client tunnel's user's password.
	exUseMode	[enable|disable]	Turns the exclusive use mode for the Contivity Client tunnel on or off.

Table 196 IPSec Commands

Command			Description
	exUseMac	[MAC address]	Specifies which MAC address is allowed to use the Contivity Client tunnel with exclusive use mode.
	clientFailOver	<IP address> <IP address> <IP address>	Sets the Contivity Client fail over IP addresses (of back up remote Contivity VPN switches).
	keepAlive	<Yes|No>	Turns the Keep Alive feature on or off.
ikeList			Displays a summary of the IKE (phase 1) rules.
ikeDelete	<rule index>		Deletes the specified IPSec rule.
policyEdit	<rule index>		Edit the specified IP policy.
policySave			Saves the IP policy.
ipsecList			Displays a summary of the IPSec (phase 2) rules.
policyList			Displays the IP policies.
policyDelete	<rule index>		Deletes the specified IP policy.
policyConfig			Use these commands to configure an IP policy for an IPSec office tunnel rule.
	saIndex	<rule index>	Binds the IP policy to an IPSec rule.
	active	<Yes|No>	Turns the IP policy on or off.
	lcAddrStart	<IP>	Sets the local starting IP address.
	protocol	<1:ICMP | 6:TCP | 17:UDP>	Sets the IP policy's protocol.
	controlPing	<Yes|No>	Turns control ping on or off.
	controlPingAddr	<IP>	Sets the control ping IP address.
	lcAddrType	<0:single | 1:range | 2:subnet>	Sets the local address type.
	lcAddrEndMask	<IP>	Sets the local ending IP address or subnet mask.
	lcPortStart	<port>	Sets the local starting port number.
	lcPortEnd	<port>	Sets the local ending port number.

Table 196 IPSec Commands

Command			Description
	rmAddrType	<0:single | 1:range | 2:subnet>	Sets the remote address type.
	rmAddrStart	<IP>	Sets the remote starting IP address.
	rmAddrEndMask	<IP>	Sets the remote ending IP address or subnet mask.
	rmPortStart	<port>	Sets the remote starting port number.
	rmPortEnd	<port>	Sets the remote ending port number.
	btNatActive	<Yes | No>	Turns branch tunnel NAT address mapping on or off.
	btNatType	<0:single | 1:range | 2:all>	Sets the type of NAT address mapping.
	btNatAddrStart	<IP address>	Sets the branch tunnel NAT starting IP address.
	btNatArEnd	<IP address>	Sets the branch tunnel NAT ending IP address or subnet mask.
swSkipOverlapIP	<on|off>		Turn this on to have the device allow rules with overlapping source and destination IP addresses.
adjTcpMss	<off|auto|user defined value>		Sets the adjust TCP Maximum Segment Size.
contivityDial			Initiates the Contivity Client VPN connection.
contivityDrop			Ends the Contivity Client VPN connection.
contivityState			Displays information about the Contivity Client VPN connection.
contivitySplit			
contivityTimecnt	<0~65535>		Sets the Contivity Client keep alive interval (in seconds).
exemptHost			Use the exemptHost commands to configure specific IP addresses that are not to be part of a VPN tunnel.
	display		Displays the exempt host settings.
	load	<index>	Loads an exempt host.

Table 196 IPSec Commands

Command			Description
	active	<Yes|No>	Enables/disables an exempt host.
	sourceStart	<IP address>	Sets the exempt host's source start IP address.
	sourceEnd	<IP address>	Sets the exempt host's source end IP address.
	destStart	<IP address>	Sets the exempt host's destination start IP address.
	destEnd	<IP address>	Sets the exempt host's destination end IP address.
	save		Saves an exempt host.
btNatList			Displays the branch tunnel NAT entries.

Sys Firewall Commands

The following table lists and describes the system firewall commands. Each of these commands must be preceded by `sys firewall` when you use them. For example, type `sys firewall active yes` to turn on the firewall.

Table 197 Sys Firewall Commands

Command		Description
acl		
	disp	Displays ACLs or a specific ACL set # and rule #.
active	<yes|no>	Active firewall or deactivate firewall Enables/disables the firewall.
cnt		
	disp	Displays the firewall log type and count.
	clear	Clears the firewall log count.
dynamicrule	display	Displays the firewall's dynamic rules.
tcprst		
	rst	Turns TCP reset sending on/off.
	rst113	Turns TCP reset sending for port 113 on/off.

Table 197 Sys Firewall Commands

Command		Description
	display	Displays the TCP reset sending settings.
dos		
	smtp	Enables/disables the SMTP DoS defender.
	display	Displays the SMTP DoS defender setting.
	ignore	Sets if the firewall will ignore DoS attacks on the lan/wan.
ignore		
	dos	Sets if the firewall will ignore DoS attacks on the lan/wan.
	triangle	Sets if the firewall will ignore triangle route packets on the lan/wan.

Bandwidth Management Commands

The following table lists and describes the bandwidth management commands. Each of these commands must be preceded by `bm` when you use them. For example, type `bm show lan` to display the LAN port's bandwidth management settings.

Table 198 Bandwidth Management Commands

Command				Description
interface				
	iface	enable [bandwidth bps]		Turns on bandwidth management on the specified interface (LAN or WAN) and set its bandwidth (default 100 Mbps).
		disable		Disable bandwidth management on the specified interface.
class	iface	add/mod <class name>	<bandwidth bps>	Adds, deletes or modifies a class with specified name. You can set the bandwidth.
	iface	del	<class name>	Deletes the specified class.

Table 198 Bandwidth Management Commands

Command				Description
filter	iface	add class [service xxx] <dst> [mask xx] <dport> <src> [mask xx]	<sport> <proto>	Adds a filter for the specified class on the specified interface. The filter can contain destination address (netmask), destination port, source address (netmask), source port and protocol. Use 0 for any.
		del class		Deletes a filter for the specified class on the specified interface.
show				
	interface	iface		Displays the specified interface's settings.
	class	iface		Displays the specified interface's classes.
	filter	iface		Displays the specified interface's filter settings.
	statistics iface	iface		Displays the statistics of the specified interface's classes.
monitor	iface	[class]		Monitors the bandwidth usage of an interface or a specific class on an interface. Use the command once to turn on the monitor and again to turn it off.
moveFilter	iface	from to		Moves a bandwidth management filter from number in the filter list to another.
config				
	save			Save the bandwidth management configuration.
	load			Load the bandwidth management configuration.
	clear			Clear the bandwidth management configuration.

Certificates Commands

The table describes the certificate commands. Each of these commands must be preceded by `certificates` when you use them (or `cert` for short). For example, type `cert my_cert list` to display all my certificate names and basic information.

All of these commands start with certificates.

Table 199 Certificates Commands

Command			Description
`my_cert`			
	`create`		
	`create`	`selfsigned <name> <subject> [key size]`	Create a self-signed local host certificate. <name> specifies a descriptive name for the generated certificate. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	`create`	`request <name> <subject> [key size]`	Create a certificate request and save it to the router for later manual enrollment. <name> specifies a descriptive name for the generated certification request. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	`create`	`scep_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]`	Create a certificate request and enroll for a certificate immediately online using SCEP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the key used for user authentication. If the key contains spaces, please put it in quotes. To leave it blank, type "". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.

Table 199 Certificates Commands

Command			Description
	`create`	`cmp_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]`	Create a certificate request and enroll for a certificate immediately online using CMP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the id and key used for user authentication. The format is "id:key". To leave the id and key blank, type ":". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	`import`	`[name]`	Import the PEM-encoded certificate from stdin. [name] specifies the descriptive name (optional) as which the imported certificate is to be saved. For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on Contivity 221. After the importation, the certification request will automatically be deleted. If a descriptive name is not specified for the imported certificate, the certificate will adopt the descriptive name of the certification request.
	`export`	`<name>`	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	`view`	`<name>`	View the information of the specified local host certificate. <name> specifies the name of the certificate to be viewed.
	`verify`	`<name> [timeout]`	Verify the certification path of the specified local host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
	`delete`	`<name>`	Delete the specified local host certificate. <name> specifies the name of the certificate to be deleted.
	`list`		List all my certificate names and basic information.
	`rename`	`<old name> <new name>`	Rename the specified my certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.

Table 199 Certificates Commands

Command			Description
	def_self_signed	[name]	Set the specified self-signed certificate as the default self-signed certificate. [name] specifies the name of the certificate to be set as the default self-signed certificate. If [name] is not specified, the name of the current self-signed certificate is displayed.
	replace_factory		Create a certificate using your device MAC address that will be specific to this device. The factory default certificate is a common default certificate for all Contivity 221 models.
ca_trusted			
	import	<name>	Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported CA certificate is to be saved.
	export	<name>	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	view	<name>	View the information of the specified trusted CA certificate. <name> specifies the name of the certificate to be viewed.
	verify	<name> [timeout]	Verify the certification path of the specified trusted CA certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
	delete	<name>	Delete the specified trusted CA certificate. <name> specifies the name of the certificate to be deleted.
	list		List all trusted CA certificate names and basic information.
	rename	<old name> <new name>	Rename the specified trusted CA certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
	crl_issuer	<name> [on|off]	Specify whether or not the specified CA issues CRL. <name> specifies the name of the CA certificate. [on|off] specifies whether or not the CA issues CRL. If [on|off] is not specified, the current crl_issuer status of the CA.
remote_trusted			
	import	<name>	Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported remote host certificate is to be saved.

Table 199 Certificates Commands

Command			Description
	export	<name>	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	view	<name>	View the information of the specified trusted remote host certificate. <name> specifies the name of the certificate to be viewed.
	verify	<name> [timeout]	Verify the certification path of the specified trusted remote host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
	delete	<name>	Delete the specified trusted remote host certificate. <name> specifies the name of the certificate to be deleted.
	list		List all trusted remote host certificate names and basic information.
	rename	<old name> <new name>	Rename the specified trusted remote host certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
dir_server			
	add	<name> <addr[:port]> [login:pswd]	Add a new directory service. <name> specifies a descriptive name as which the added directory server is to be saved. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
	delete	<name>	Delete the specified directory service. <name> specifies the name of the directory server to be deleted.
	view	<name>	View the specified directory service. <name> specifies the name of the directory server to be viewed.
	list		List all directory service names and basic information.

Table 199 Certificates Commands

Command			Description
	rename	<old name> <new name>	Rename the specified directory service. <old name> specifies the name of the directory server to be renamed. <new name> specifies the new name as which the directory server is to be saved.
	edit	<name> <addr[:port]> [login:pswd]	Edit the specified directory service. <name> specifies the name of the directory server to be edited. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".

RADIUS Commands

The following table lists and describes the RADIUS commands. Each of these commands must be preceded by `radius` when you use them. For example, type `radius auth` to display the authentication server settings.

Table 200 RADIUS Commands

Command	Description
auth	Displays the current RADIUS authentication server configuration.
acct	Displays the current RADIUS accounting server configuration.
checkRadID	Checks the RADIUS ID pool.
debug	Enables radius debug messages.

IEEE 802.1X Commands

The following table lists and describes the IEEE 802.1x commands. Each of these commands must be preceded by `8021x` when you use them. For example, type `8021x debug level 1` to set the IEEE 802.1X debug messages to the first level.

Table 201 IEEE 802.1X Commands

Command		Description
`debug`		
	`level`	Sets the IEEE 802.1x debug message level
	`trace`	Displays all supplicants information in the supplicant table.
	`user`	Displays all supplicants information related to the username.

Appendix J
NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands.

Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

You can configure NetBIOS filters to do the following:

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN and from the WAN to the LAN.
- Allow or disallow the sending of NetBIOS packets through VPN connections.
- Allow or disallow NetBIOS packets to initiate calls.

Display NetBIOS Filter Settings

Figure 336 NetBIOS Display Filter Settings Command Example

```
============== NetBIOS Filter Status ===============
        Between LAN and WAN: Block
        IPSec Packets: Forward
        Trigger Dial: Disabled
```

Syntax:

```
sys filter netbios disp
```

This command gives a read-only list of the current NetBIOS filter modes.

The filter types and their default settings are as follows.

Table 202 NetBIOS Filter Default Settings

Name	Description	Example
`Between LAN and WAN`	This field displays whether NetBIOS packets are blocked or forwarded from the LAN to the WAN or from the WAN to the LAN.	Forward
`IPSec Packets`	This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.	Forward
`Trigger dial`	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

NetBIOS Filter Configuration

Syntax:

```
sys filter netbios config <type> <on|off>
```

where

<type> =Identify which NetBIOS filter (numbered 0-3) to configure.

- 0 = LAN to WAN and WAN to LAN
- 3 = IPSec packet pass through
- 4 = Trigger Dial

<on|off> =For type 0, use on to enable the filter and block NetBIOS packets. Use off to disable the filter and forward NetBIOS packets.

For type 3, use on to block NetBIOS packets from being sent through a VPN connection. Use off to allow NetBIOS packets to be sent through a VPN connection.

For type 4, use on to allow NetBIOS packets to initiate dial backup calls. Use off to block NetBIOS packets from initiating dial backup calls.

Example commands

Command:

```
sys filter netbios config 0 on
```

This command blocks LAN to WAN and WAN to LAN NetBIOS packets

Command:

```
sys filter netbios config 1 off
```

This command forwards WAN to LAN and WAN to LAN NetBIOS packets

Command:

```
sys filter netbios config 3 on
```

This command blocks IPSec NetBIOS packets

Command:

```
sys filter netbios config 4 off
```

This command stops NetBIOS commands from initiating calls.

Appendix K
Boot Commands

The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main router firmware is started. When you start up your Contivity 221, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example ATUR (for uploading firmware) and ATLC (for uploading the configuration file). These are already discussed in the Firmware and Configuration File Maintenance chapter.

Figure 337 Option to Enter Debug Mode

```
Bootbase Version: V1.02 | 08/08/2001 15:40:50
RAM: Size = 16384 Kbytes
DRAM Post: Testing:  16384K OK
FLASH: Intel 16M

RAS Version: V3.50(WB.0)b3 | 08/08/2001 16:21:27

Press any key to enter debug mode within 3 seconds.
.............................................
```

Enter ATHE to view all available Contivity 221 boot module commands as shown in the next screen. ATBAx allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; for example ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product related

information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.

Figure 338 Boot Module Commands

```
AT              just answer OK
ATHE            print help
ATBAx           change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx,(y)       set BootExtension Debug Flag (y=password)
ATSE            show the seed of password generator
ATTI(h,m,s)     change system time to hour:min:sec or show current time
ATDA(y,m,d)     change system date to year/month/day or show current date
ATDS            dump RAS stack
ATDT            dump Boot Module Common Area
ATDUx,y         dump memory contents from address x for length y
ATRBx           display the  8-bit value of address x
ATRWx           display the 16-bit value of address x
ATRLx           display the 32-bit value of address x
ATGO(x)         run program at addr x or boot router
ATGR            boot router
ATGT            run Hardware Test Program
ATRTw,x,y(,z)   RAM test level w, from address x to y (z iterations)
ATSH            dump manufacturer related data in ROM
ATDOx,y         download from address x for length y to PC via XMODEM
ATTD            download router configuration to PC via XMODEM
ATUR            upload router firmware to flash ROM
ATLC            upload router configuration file to flash ROM
ATXSx           xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATSR            system reboot
```

Appendix L
Log Descriptions

This appendix provides descriptions of example log messages.

Table 203 System Error Logs

Log Message	Description
`%s exceeds the max. number of session per host!`	This attempt to create a SUA/NAT session exceeds the maximum number of SUA/NAT session table entries allowed to be created per host.

Table 204 System Maintenance Logs

Log Message	Description
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`DHCP client gets %s`	A DHCP client got a new IP address from the DHCP server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`SMT Login Successfully`	Someone has logged on to the router's SMT interface.
`SMT Login Fail`	Someone has failed to log on to the router's SMT interface.
`WEB Login Successfully`	Someone has logged on to the router's WebGUI interface.
`WEB Login Fail`	Someone has failed to log on to the router's WebGUI interface.

Table 204 System Maintenance Logs

Log Message	Description
TELNET Login Successfully	Someone has logged on to the router via telnet.
TELNET Login Fail	Someone has failed to log on to the router via telnet.
FTP Login Successfully	Someone has logged on to the router via FTP.
FTP Login Fail	Someone has failed to log on to the router via FTP.
NAT Session Table is Full!	The maximum number of SUA/NAT session table entries has been exceeded and the table is full.

Table 205 UPnP Logs

Log Message	Description
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 206 Content Filtering Logs

Category	Log Message	Description
URLFOR	IP/Domain Name	The Contivity 221 allows access to this IP address or domain name and forwarded traffic addressed to the IP address or domain name.
URLBLK	IP/Domain Name	The Contivity 221 blocked access to this IP address or domain name due to a forbidden keyword. All web traffic is disabled except for trusted domains, untrusted domains, or the cybernot list.
JAVBLK	IP/Domain Name	The Contivity 221 blocked access to this IP address or domain name because of a forbidden service such as: ActiveX, a Java applet, a cookie, or a proxy.

Table 207 Attack Logs

Log Message	Description
`attack TCP`	The firewall detected a TCP attack.
`attack UDP`	The firewall detected an UDP attack.
`attack IGMP`	The firewall detected an IGMP attack.
`attack ESP`	The firewall detected an ESP attack.
`attack GRE`	The firewall detected a GRE attack.
`attack OSPF`	The firewall detected an OSPF attack.
`attack ICMP (type:%d, code:%d)`	The firewall detected an ICMP attack; see the section on ICMP messages for type and code details.
`land TCP`	The firewall detected a TCP land attack.
`land UDP`	The firewall detected an UDP land attack.
`land IGMP`	The firewall detected an IGMP land attack.
`land ESP`	The firewall detected an ESP land attack.
`land GRE`	The firewall detected a GRE land attack.
`land OSPF`	The firewall detected an OSPF land attack.
`land ICMP (type:%d, code:%d)`	The firewall detected an ICMP land attack; see the section on ICMP messages for type and code details.
`ip spoofing - WAN TCP`	The firewall detected a TCP IP spoofing attack on the WAN port.
`ip spoofing - WAN UDP`	The firewall detected an UDP IP spoofing attack on the WAN port.
`ip spoofing - WAN IGMP`	The firewall detected an IGMP IP spoofing attack on the WAN port.
`ip spoofing - WAN ESP`	The firewall detected an ESP IP spoofing attack on the WAN port.
`ip spoofing - WAN GRE`	The firewall detected a GRE IP spoofing attack on the WAN port.
`ip spoofing - WAN OSPF`	The firewall detected an OSPF IP spoofing attack on the WAN port.
`ip spoofing - WAN ICMP (type:%d, code:%d)`	The firewall detected an ICMP IP spoofing attack on the WAN port.

Table 207 Attack Logs

Log Message	Description
`icmp echo ICMP (type:%d, code:%d)`	The firewall detected an ICMP echo attack.
`syn flood TCP`	The firewall detected a TCP syn flood attack.
`ports scan TCP`	The firewall detected a TCP port scan attack.
`teardrop TCP`	The firewall detected a TCP teardrop attack.
`teardrop UDP`	The firewall detected an UDP teardrop attack.
`teardrop ICMP (type:%d, code:%d)`	The firewall detected an ICMP teardrop attack.
`illegal command TCP`	The firewall detected a TCP illegal command attack.
`NetBIOS TCP`	The firewall detected a TCP NetBIOS attack.
`ip spoofing - no routing entry TCP`	The firewall detected a TCP IP spoofing attack while the Contivity 221 did not have a default route.
`ip spoofing - no routing entry UDP`	The firewall detected an UDP IP spoofing attack while the Contivity 221 did not have a default route.
`ip spoofing - no routing entry IGMP`	The firewall detected an IGMP IP spoofing attack while the Contivity 221 did not have a default route.
`ip spoofing - no routing entry ESP`	The firewall detected an ESP IP spoofing attack while the Contivity 221 did not have a default route.
`ip spoofing - no routing entry GRE`	The firewall detected a GRE IP spoofing attack while the Contivity 221 did not have a default route.
`ip spoofing - no routing entry OSPF`	The firewall detected an OSPF IP spoofing attack while the Contivity 221 did not have a default route.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	The firewall detected an ICMP IP spoofing attack while the Contivity 221 did not have a default route.
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack.

Please see Table 210 for type and code details.

Table 208 Access Logs

Log Message	Description
`Firewall default policy: TCP (set:%d)`	TCP access matched the default policy of the listed ACL set and the Contivity 221 blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: UDP (set:%d)`	UDP access matched the default policy of the listed ACL set and the Contivity 221 blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: ICMP (set:%d, type:%d, code:%d)`	ICMP access matched the default policy of the listed ACL set and the Contivity 221 blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: IGMP (set:%d)`	IGMP access matched the default policy of the listed ACL set and the Contivity 221 blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: ESP (set:%d)`	ESP access matched the default policy of the listed ACL set and the Contivity 221 blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: GRE (set:%d)`	GRE access matched the default policy of the listed ACL set and the Contivity 221 blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: OSPF (set:%d)`	OSPF access matched the default policy of the listed ACL set and the Contivity 221 blocked or forwarded it according to the ACL set's configuration.
`Firewall default policy: (set:%d)`	Access matched the default policy of the listed ACL set and the Contivity 221 blocked or forwarded it according to the ACL set's configuration.
`Firewall rule match: TCP (set:%d, rule:%d)`	TCP access matched the listed firewall rule and the Contivity 221 blocked or forwarded it according to the rule's configuration.
`Firewall rule match: UDP (set:%d, rule:%d)`	UDP access matched the listed firewall rule and the Contivity 221 blocked or forwarded it according to the rule's configuration.
`Firewall rule match: ICMP (set:%d, rule:%d, type:%d, code:%d)`	ICMP access matched the listed firewall rule and the Contivity 221 blocked or forwarded it according to the rule's configuration.
`Firewall rule match: IGMP (set:%d, rule:%d)`	IGMP access matched the listed firewall rule and the Contivity 221 blocked or forwarded it according to the rule's configuration.

Table 208 Access Logs

Log Message	Description
`Firewall rule match: ESP (set:%d, rule:%d)`	ESP access matched the listed firewall rule and the Contivity 221 blocked or forwarded it according to the rule's configuration.
`Firewall rule match: GRE (set:%d, rule:%d)`	GRE access matched the listed firewall rule and the Contivity 221 blocked or forwarded it according to the rule's configuration.
`Firewall rule match: OSPF (set:%d, rule:%d)`	OSPF access matched the listed a firewall rule and the Contivity 221 blocked or forwarded it according to the rule's configuration.
`Firewall rule match: (set:%d, rule:%d)`	Access matched the listed firewall rule and the Contivity 221 blocked or forwarded it according to the rule's configuration.
`Firewall rule NOT match: TCP (set:%d, rule:%d)`	TCP access did not match the listed firewall rule and the Contivity 221 logged it.
`Firewall rule NOT match: UDP (set:%d, rule:%d)`	UDP access did not match the listed firewall rule and the Contivity 221 logged it.
`Firewall rule NOT match: ICMP (set:%d, rule:%d, type:%d, code:%d)`	ICMP access did not match the listed firewall rule and the Contivity 221 logged it.
`Firewall rule NOT match: IGMP (set:%d, rule:%d)`	IGMP access did not match the listed firewall rule and the Contivity 221 logged it.
`Firewall rule NOT match: ESP (set:%d, rule:%d)`	ESP access did not match the listed firewall rule and the Contivity 221 logged it.
`Firewall rule NOT match: GRE (set:%d, rule:%d)`	GRE ac access did not match the listed firewall rule and the Contivity 221 logged it.
`Firewall rule NOT match: OSPF (set:%d, rule:%d)`	OSPF access did not match the listed firewall rule and the Contivity 221 logged it.
`Firewall rule NOT match: (set:%d, rule:%d)`	Access did not match the listed firewall rule and the Contivity 221 logged it.
`Filter default policy DROP!`	TCP access matched a default filter policy and the Contivity 221 dropped the packet to block access.

Table 208 Access Logs

Log Message	Description
`Filter default policy DROP!`	UDP access matched a default filter policy and the Contivity 221 dropped the packet to block access.
`Filter default policy DROP!`	ICMP access matched a default filter policy and the Contivity 221 dropped the packet to block access.
`Filter default policy DROP!`	Access matched a default filter policy and the Contivity 221 dropped the packet to block access.
`Filter default policy DROP!`	Access matched a default filter policy (denied LAN IP) and the Contivity 221 dropped the packet to block access.
`Filter default policy FORWARD!`	TCP access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	UDP access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	ICMP access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	Access matched a default filter policy. Access was allowed and the router forwarded the packet.
`Filter default policy FORWARD!`	Access matched a default filter policy (denied LAN IP). Access was allowed and the router forwarded the packet.
`Filter match DROP <set %d/rule %d>`	TCP access matched the listed filter rule and the Contivity 221 dropped the packet to block access.
`Filter match DROP <set %d/rule %d>`	UDP access matched the listed filter rule and the Contivity 221 dropped the packet to block access.
`Filter match DROP <set %d/rule %d>`	ICMP access matched the listed filter rule and the Contivity 221 dropped the packet to block access.
`Filter match DROP <set %d/rule %d>`	Access matched the listed filter rule and the Contivity 221 dropped the packet to block access.
`Filter match DROP <set %d/rule %d>`	Access matched the listed filter rule (denied LAN IP) and the Contivity 221 dropped the packet to block access.
`Filter match FORWARD <set %d/rule %d>`	TCP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
`Filter match FORWARD <set %d/rule %d>`	UDP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
`Filter match FORWARD <set %d/rule %d>`	ICMP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
`Filter match FORWARD <set %d/rule %d>`	Access matched the listed filter rule. Access was allowed and the router forwarded the packet.

Table 208 Access Logs

Log Message	Description
`Filter match FORWARD <set %d/rule %d>`	Access matched the listed filter rule (denied LAN IP). Access was allowed and the router forwarded the packet.
`(set:%d)`	With firewall messages, this is the number of the ACL policy set and denotes the packet's direction (see Table 209). With filter messages, this is the number of the filter set.
`(rule:%d)`	With firewall messages, the firewall rule number denotes the number of a firewall rule within an ACL policy set.With filter messages, this is the number of an individual filter rule.
`Router sent blocked web site message`	
`Triangle route packet forwarded`	The firewall allowed a triangle route session to pass through.
`Firewall sent TCP packet in response to DoS attack`	The firewall detected a DoS attack and sent a TCP packet(s) in response.
`Firewall sent TCP reset packets`	The firewall sent out TCP reset packets.
`Packet without a NAT table entry blocked`	The router blocked a packet that did not have a corresponding SUA/NAT table entry.
`Out of order TCP handshake packet blocked`	The router blocked a TCP handshake packet that came out of the proper order
`Drop unsupported/ out-of-order ICMP`	The Contivity 221 generates this log after it drops an ICMP packet due to one of the following two reasons:1. The Contivity 221 does not support the ICMP packet's protocol.2. The ICMP packet is an echo reply for which there was no corresponding echo request.
`Router sent ICMP response packet (type:%d, code:%d)`	The router sent an ICMP response packet. This packet automatically bypasses the firewall.

Please see Table 210 for type and code details.

Table 209 ACL Setting Notes

ACL Set Number	Direction	Description
1	LAN to WAN	ACL set 1 for packets traveling from the LAN to the WAN.
2	WAN to LAN	ACL set 2 for packets traveling from the WAN to the LAN.
7	LAN to LAN/Contivity 221	ACL set 7 for packets traveling from the LAN to the LAN or the Contivity 221.
8	WAN to WAN/Contivity 221	ACL set 8 for packets traveling from the WAN to the WAN or the Contivity 221.

Table 210 ICMP Notes

Type	Code	Description
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host

Table 210 ICMP Notes

Type	Code	Description
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 211 Sys log

LOG MESSAGE	DESCRIPTION
Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>	"This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix's other charts.

VPN/IPSec Logs

To view the IPSec and IKE connection log, type 3 in menu 27 and press [ENTER] to display the IPSec log as shown next. The following figure shows a typical log from the initiator of a VPN connection.

Figure 339 Example VPN Initiator IPSec Log

```
Index:    Date/Time:              Log:
------------------------------------------------------------
 001    01 Jan 08:02:22    Send Main Mode request to <192.168.100.101>
 002    01 Jan 08:02:22    Send:<SA>
 003    01 Jan 08:02:22    Recv:<SA>
 004    01 Jan 08:02:24    Send:<KE><NONCE>
 005    01 Jan 08:02:24    Recv:<KE><NONCE>
 006    01 Jan 08:02:26    Send:<ID><HASH>
 007    01 Jan 08:02:26    Recv:<ID><HASH>
 008    01 Jan 08:02:26    Phase 1 IKE SA process done
 009    01 Jan 08:02:26    Start Phase 2: Quick Mode
 010    01 Jan 08:02:26    Send:<HASH><SA><NONCE><ID><ID>
 011    01 Jan 08:02:26    Recv:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:02:26    Send:<HASH>
 Clear IPSec Log (y/n):
```

VPN Responder IPSec Log

The following figure shows a typical log from the VPN connection peer.

Figure 340 Example VPN Responder IPSec Log

```
Index:    Date/Time:              Log:
------------------------------------------------------------
 001    01 Jan 08:08:07    Recv Main Mode request from <192.168.100.100>
 002    01 Jan 08:08:07    Recv:<SA>
 003    01 Jan 08:08:08    Send:<SA>
 004    01 Jan 08:08:08    Recv:<KE><NONCE>
 005    01 Jan 08:08:10    Send:<KE><NONCE>
 006    01 Jan 08:08:10    Recv:<ID><HASH>
 007    01 Jan 08:08:10    Send:<ID><HASH>
 008    01 Jan 08:08:10    Phase 1 IKE SA process done
 009    01 Jan 08:08:10    Recv:<HASH><SA><NONCE><ID><ID>
 010    01 Jan 08:08:10    Start Phase 2: Quick Mode
 011    01 Jan 08:08:10    Send:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:08:10    Recv:<HASH>
 Clear IPSec Log (y/n):
```

This menu is useful for troubleshooting. A log index number, the date and time the log was created and a log message are displayed.

Note: Double exclamation marks (!!) denote an error or warning message.

The following table shows sample log messages during IKE key exchange.

Note: A PYLD_MALFORMED packet usually means that the two ends of the VPN tunnel are not using the same pre-shared key.

Table 212 Sample IKE Key Exchange Logs

Log Message	Description
`Send <Symbol> Mode request to <IP>Send <Symbol> Mode request to <IP>`	The Contivity 221 has started negotiation with the peer.
`Recv <Symbol> Mode request from <IP>Recv <Symbol> Mode request from <IP>`	The Contivity 221 has received an IKE negotiation request from the peer.
`Recv:<Symbol>`	IKE uses the ISAKMP protocol (refer to RFC2408 – ISAKMP) to transmit data. Each ISAKMP packet contains payloads of different types that show in the log (see Table 214).
`Phase 1 IKE SA process done`	Phase 1 negotiation is finished.
`Start Phase 2: Quick Mode`	Phase 2 negotiation is beginning using Quick Mode.
`!! IKE Negotiation is in process`	The Contivity 221 has begun negotiation with the peer for the connection already, but the IKE key exchange has not finished yet.
`!! Duplicate requests with the same cookie`	The Contivity 221 has received multiple requests from the same peer but it is still processing the first IKE packet from that peer.
`!! No proposal chosen`	The parameters configured for Phase 1 or Phase 2 negotiations don't match. Please check all protocols and settings for these phases. For example, one party may be using 3DES encryption, but the other party is using DES encryption, so the connection will fail.
`!! Verifying Local ID failed!! Verifying Remote ID failed`	During IKE Phase 2 negotiation, both parties exchange policy details, including local and remote IP address ranges. If these ranges differ, then the connection fails.
`!! Local / remote IPs of incoming request conflict with rule <#d>`	If the security gateway is "0.0.0.0", the Contivity 221 will use the peer's "Local Addr" as its "Remote Addr". If this IP (range) conflicts with a previously configured rule then the connection is not allowed.
`!! Invalid IP <IP start>/ <IP end>`	The peer's "Local IP Addr" range is invalid.

Table 212 Sample IKE Key Exchange Logs

Log Message	Description
`!! Remote IP <IP start> / <IP end> conflicts`	If the security gateway is "0.0.0.0", the Contivity 221 will use the peer's "Local Addr" as its "Remote Addr". If a peer's "Local Addr" range conflicts with other connections, then the Contivity 221 will not accept VPN connection requests from this peer.
`!! Active connection allowed exceeded`	The Contivity 221 limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded.
`!! IKE Packet Retransmit`	The Contivity 221 did not receive a response from the peer and so retransmits the last packet sent.
`!! Failed to send IKE Packet`	The Contivity 221 cannot send IKE packets due to a network error.
`!! Too many errors! Deleting SA`	The Contivity 221 deletes an SA when too many errors occur.
`!! Phase 1 ID type mismatch`	The ID type of an incoming packet does not match the local's peer ID type.
`!! Phase 1 ID content mismatch`	The ID content of an incoming packet does not match the local's peer ID content.
`!! No known phase 1 ID type found`	The ID type of an incoming packet does not match any known ID type.
`Peer ID: IP address type <IP address>`	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays the IP address type and IP address of the incoming packet.
`vs. My Remote <IP address>`	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured remote IP address type or IP address that the incoming packet did not match.
`vs. My Local <IP address>`	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured local IP address type or IP address that the incoming packet did not match.

Table 212 Sample IKE Key Exchange Logs

Log Message	Description
-> <symbol>	The router sent a payload type of IKE packet.
Error ID Info	The parameters configured for Phase 1 ID content do not match or the parameters configured for the Phase 2 ID (IP address of single, range or subnet) do not match. Please check all protocols and settings for these phases.

The following table shows sample log messages during packet transmission.

Table 213 Sample IPSec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
!! WAN IP changed to <IP>	If the Contivity 221's WAN IP changes, all configured "My IP Addr" are changed to b "0.0.0.0". If this field is configured as 0.0.0.0, then the Contivity 221 will use the current Contivity 221 WAN IP address (static or dynamic) to set up the VPN tunnel.
!! Cannot find IPSec SA	The Contivity 221 cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped.
!! Cannot find outbound SA for rule <%d>	The packet matches the rule index number (#d), but Phase 1 or Phase 2 negotiation for outbound (from the VPN initiator) traffic is not finished yet.
!! Discard REPLAY packet	If the Contivity 221 receives a packet with the wrong sequence number it will discard it.
!! Inbound packet authentication failed	The authentication configuration settings are incorrect. Please check them.
!! Inbound packet decryption failed	The decryption configuration settings are incorrect. Please check them.
Rule <#d> idle time out, disconnect	If an SA has no packets transmitted for a period of time (configurable via CI command), the Contivity 221 drops the connection.

The following table shows RFC-2408 ISAKMP payload types that the log displays. lease refer to the RFC for detailed information on each type.

Table 214 RFC-2408 ISAKMP Payload Types

Log Display	Payload Type
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Table 215 PKI Logs

Log Message	Description
`Enrollment successful`	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
`Enrollment failed`	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <SCEP CA server url>`	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
`Enrollment successful`	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.

Table 215 PKI Logs

Log Message	Description
`Enrollment failed`	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <CMP CA server url>`	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
`Rcvd ca cert: <subject name>`	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd user cert: <subject name>`	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd CRL <size>: <issuer name>`	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd ARL <size>: <issuer name>`	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ca cert`	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received user cert`	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received CRL`	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ARL`	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Rcvd data <size> too large! Max size allowed: <max size>`	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
`Cert trusted: <subject name>`	The router has verified the path of the certificate with the listed subject name.
`Due to <reason codes>, cert not trusted: <subject name>`	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 216 for the corresponding descriptions of the codes.

Table 216 Certificate Path Verification Failure Reason Codes

Code	Description
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 217 IEEE 802.1X Logs

Log Message	Description
`Local User Database accepts user.`	A user was authenticated by the local user database.
`Local User Database reports user credential error.`	A user was not authenticated by the local user database because of an incorrect user password.
`Local User Database does not find user`s credential.`	A user was not authenticated by the local user database because the user is not listed in the local user database.
`RADIUS accepts user.`	A user was authenticated by the RADIUS Server.
`RADIUS rejects user. Pls check RADIUS Server.`	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
`Local User Database does not support authentication method.`	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
`User logout because of session timeout expired.`	The router logged out a user whose session expired.
`User logout because of user deassociation.`	The router logged out a user who ended the session.
`User logout because of no authentication response from user.`	The router logged out a user from which there was no authentication response.
`User logout because of idle timeout expired.`	The router logged out a user whose idle timeout period expired.
`User logout because of user request.`	A user logged out.
`Local User Database does not support authentication mothed.`	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
`No response from RADIUS. Pls check RADIUS Server.`	There is no response message from the RADIUS server, please check the RADIUS server.
`Use Local User Database to authenticate user.`	The local user database is operating as the authentication server.
`Use RADIUS to authenticate user.`	The RADIUS server is operating as the authentication server.

Table 217 IEEE 802.1X Logs

Log Message	Description
`No Server to authenticate user.`	There is no authentication server to authenticate a user.
`Local User Database does not find user`s credential.`	A user was not authenticated by the local user database because the user is not listed in the local user database.

Log Commands

Go to the command interpreter interface (the Command Interpreter Appendix explains how to access and use the commands).

Configuring What You Want the Contivity 221 to Log

Use the sys logs load command to load the log setting buffer that allows you to configure which logs the Contivity 221 is to record.

Use sys logs category followed by a log category and a parameter to decide what to record

Table 218 Log Categories and Available Settings

Log Categories	Available Parameters
access	0, 1, 2, 3
attack	0, 1, 2, 3
error	0, 1, 2, 3
ike	0, 1, 2, 3
ipsec	0, 1, 2, 3
javablocked	0, 1, 2, 3
mten	0, 1
upnp	0, 1
urlblocked	0, 1, 2, 3

Table 218 Log Categories and Available Settings

Log Categories	Available Parameters
urlforward	0, 1
	Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category.

Use the sys logs save command to store the settings in the Contivity 221 (you must do this in order to record logs).

Displaying Logs

Use the sys logs display command to show all of the logs in the Contivity 221's log.

Use the sys logs category display command to show the log settings for all of the log categories.

Use the sys logs display [log category] command to show the logs in an individual Contivity 221 log category.

Use the sys logs clear command to erase all of the Contivity 221's logs.

Log Command Example

This example shows how to set the Contivity 221 to record the access logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

#  .time                 source                 destination            notes
    message
  0|11/11/2002 15:10:12 |172.22.3.80:137       |172.22.255.255:137    |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
  1|11/11/2002 15:10:12 |172.21.4.17:138       |172.21.255.255:138    |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
  2|11/11/2002 15:10:11 |172.17.2.1           |224.0.1.60           |ACCESS BLOCK
    Firewall default policy: IGMP(set:8)
  3|11/11/2002 15:10:11 |172.22.3.80:137       |172.22.255.255:137    |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
  4|11/11/2002 15:10:10 |192.168.10.1:520      |192.168.10.255:520    |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
  5|11/11/2002 15:10:10 |172.21.4.67:137       |172.21.255.255:137    |ACCESS
BLOCK
```

Appendix M
Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password.

Table 219 Brute-Force Password Guessing Protection Commands

Command	Description
`sys pwderrtm`	This command displays the brute-force guessing password protection settings.
`sys pwderrtm 0`	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
`sys pwderrtm N`	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

Example

sys pwderrtm 5

This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

Appendix N
SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then “VoIP-provider.com” is the SIP service domain.

SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 220 SIP Call Progression

A		B
1. INVITE		
		2. Ringing
		3. OK
4. ACK		
	5.Dialogue (voice traffic)	
6. BYE		
		7. OK

1. A sends a SIP INVITE request to B. This message is an invitation for B to participate in a SIP telephone call.
2. B sends a response indicating that the telephone is ringing.
3. B sends an OK response after the call is answered.
4. A then sends an ACK message to acknowledge that B has answered the call.
5. Now A and B exchange voice media (talk).
6. After talking, A hangs up and sends a BYE request.
7. B replies with an OK response confirming receipt of the BYE request and the call is terminated.

SIP Servers

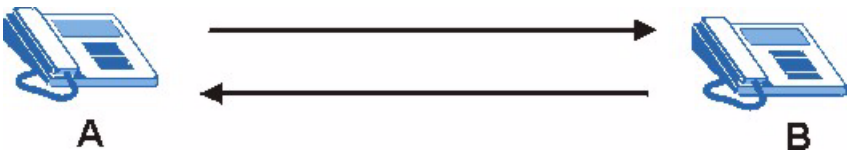
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent Server

A SIP user agent server can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either A or B can act as a SIP user agent client to initiate a call. A and B can also both act as a SIP user agent server to receive the call.

Figure 341 SIP User Agent Server



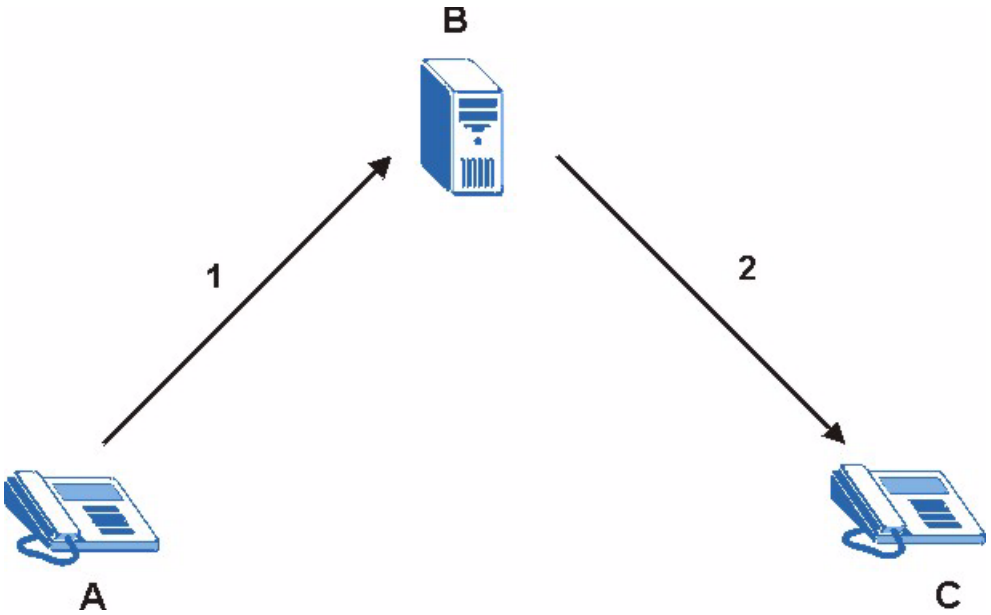
SIP Proxy Server

A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device A to call someone who is using client device C.

1. The client device (A in the figure) sends a call invitation to the SIP proxy server (B).
2. The SIP proxy server forwards the call invitation to C.

Figure 342 SIP Proxy Server



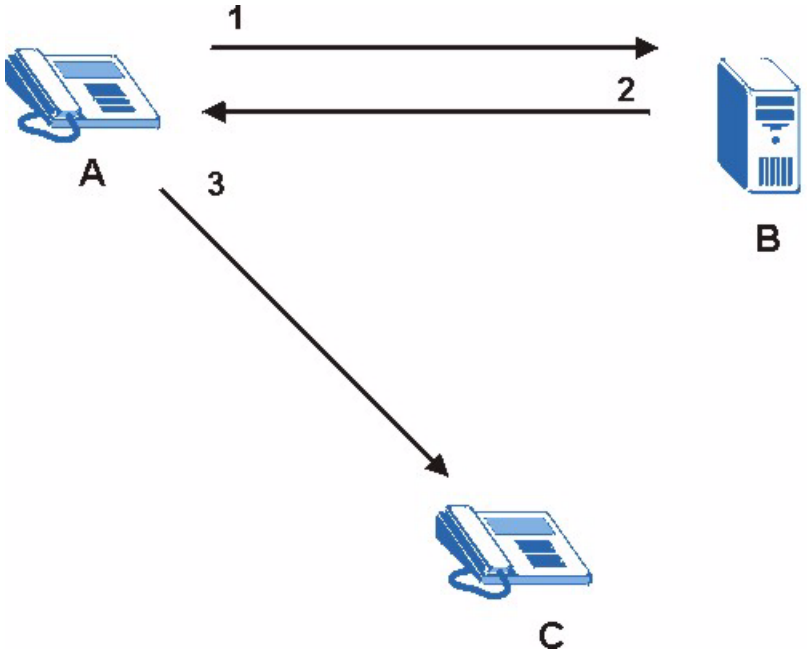
SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device A to call someone who is using client device C.

1. Client device A sends a call invitation for C to the SIP redirect server (B).
2. The SIP redirect server sends the invitation back to A with C's IP address (or domain name).
3. Client device A then sends the call invitation to client device C.

Figure 343 SIP Redirect Server



SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

SIP ALG

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows VoIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When a VoIP device (SIP client) behind the SIP ALG registers with the SIP register server, the SIP ALG translates the device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN if your VoIP device is behind the SIP ALG.

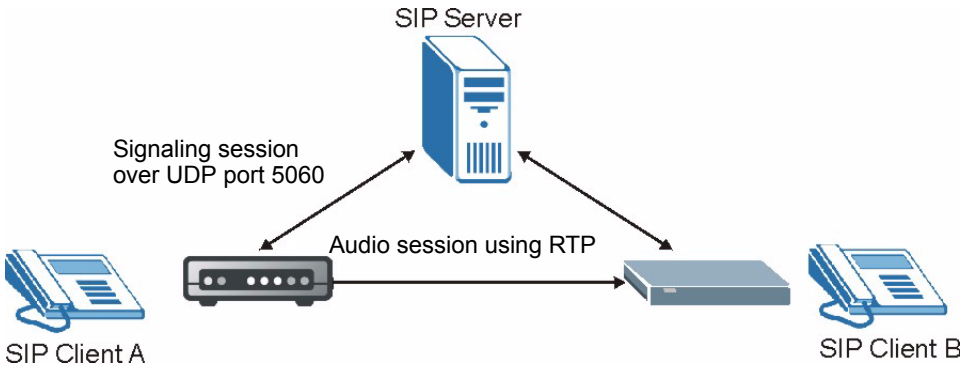
STUN

STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the VoIP device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the VoIP device to find the public IP address that NAT assigned, so the VoIP device can embed it in the SIP data stream. See RFC 3489 for details on STUN.

Contivity 221 SIP ALG

- SIP clients must be connected to the LAN. A SIP server must be on the WAN.
- You can make and receive calls between the LAN and the WAN. You cannot make a call between the LAN and the LAN.
- The SIP ALG allows UDP packets with a port 5060 destination to pass through.
- The Contivity 221 allows SIP audio connections.

Figure 344 Contivity 221 SIP ALG



SIP ALG and NAT

The Contivity 221 dynamically creates an implicit port forwarding rule for SIP traffic from the WAN to the LAN.

The SIP ALG on the Contivity 221 supports all NAT mapping types, including **One to One**, **Many to One**, **Many to Many Overload** and **Many One to One**.

SIP ALG and Firewall

The Contivity 221 creates an implicit temporary firewall rule for the dynamic RTP port on the WAN to the SIP client device on the LAN. The firewall rule is created for both directions to allow voice packets. The firewall rule is deleted when the call is terminated.

SIP ALG and Multiple WAN

When the Contivity 221 has two WAN ports and uses the second highest priority WAN port as a back up, it drops SIP connections when the primary WAN port connection fails. The Contivity 221 does not automatically change the SIP connection to the secondary WAN port.

If the primary WAN connection fails, the SIP client needs to re-register with the SIP server through the secondary WAN port to have the SIP connection go through the secondary WAN port.

When the Contivity 221 uses both of the WAN ports at the same time, you can configure a routing policy to have the voice traffic from any IP address with UDP port 5060 and the RTP ports go over a specified WAN port.

Enabling/Disabling the SIP ALG

The Contivity 221 SIP ALG is turned off by default to avoid retranslating the IP address of an existing SIP device that is using STUN. If you want to use a SIP client device (a SIP phone or IP phone for example) behind the Contivity 221 without STUN, use the `ip alg enable ALG_SIP` command to activate the SIP ALG.

Signaling Session Timeout

Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP UA sends registration packets to the SIP server periodically and keeps the session alive in the Contivity 221.

If the SIP client does not have this mechanism and makes no call during the Contivity 221 SIP timeout default (60 minutes), the Contivity 221 SIP ALG drops any incoming calls after the timeout period. You can use the `ip alg siptimeout` command to change the timeout value.

Audio Session Timeout

If no voice packets go through the SIP ALG before the timeout period default (5 minutes) expires, the SIP ALG does not drop the call but blocks all voice traffic and deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

Index

Numbers

10/100 Mbps Ethernet WAN 52
3DES 206
4-Port Switch 52

A

ACK Message 714
Action 176
Action for Matched Packets 179
Active 406, 409, 433
ActiveX 194
Address Assignment 74, 75
Administrator Inactivity Timer 84
AES 206
AH 205
AH Protocol 205
Alert 176
ALG 718
Allocated Budget 127, 407, 436
Allow Through IPSec Tunnel 246
Allow Trigger Dial 119
Alternative Subnet Mask Notation 634
Always On 127
Answer 130
Application Layer Gateway 718
Application-level Firewalls 154
Applications 58
AT command 402, 404, 526
AT Command Initial String 125
AT Command Strings 128, 129
AT Response Strings 130
ATDP 128
ATH 128
Attack Alert 189, 190, 191
Attack Types 160
Authen 407, 436
Authentication 407, 435, 436
Authentication Header 205
Authentication Protocol 435
Authentication Type 125
Auto-negotiating 10/100 Mbps Ethernet LAN 52
Auto-sensing 10/100 Mbps Ethernet LAN 52
Auxiliary 52

B

Backup 378, 526
Bandwidth Class 286
Bandwidth Filter 286, 293
Bandwidth Management 285
Bandwidth Management Statistics 294
Bandwidth Manager Class Configuration 291
Bandwidth Manager Class Setup 289
Bandwidth Manager Monitor 296
Bandwidth Manager Summary 288
Blocking Time 190, 192
Branch Office 221
Branch Tunnel NAT Address Mapping Rule 231
Broadcast Dial Backup Route 127

Brute-force Attack 159
Brute-Force Password Guessing Protection 54
Budget 127
Budget Management 548
BYE Request 714
Bypass Triangle Route 175

C

Cable Modem 155
Call Back Delay 130, 405
Call Control 130, 548
Call History 550
Call Scheduling 55, 363, 559
  Maximum Number of Schedule Sets 363, 559
  PPPoE 562
  Precedence 363, 560
  Precedence Example 363, 560
Called ID 130
Calling Line Identification 130
Call-Triggering Packet 519
Central Network Management 56
CHAP 125, 407, 436
Check WAN IP Address 122
CLID 130
Client-server Protocol 715
Command Interpreter Mode 545
Community 499
Conditions that prevent TFTP and FTP from working over WAN 529
Configuration 372
Connection ID/Name 114, 438
Console Port 512, 514, 626
Content Filtering 54, 193
  Days and Times 193
  Restrict Web Features 193
Contivity Client 217
Contivity VPN Client 209
conventions, text 47
Cookies 194
Custom Port 179
Custom Ports
  Creating/Editing 180
customer support 49

D

Data Terminal Ready 128
DDNS
  Configuration 394
DDNS Type 86, 395
Default 377
Default Policy Log 176
Default Server 140
Default Server IP Address 139
Denial of Service 155, 156, 189, 190, 477
DES 206
Destination Address 172, 178
DHCP 68, 75, 76, 85, 97, 98, 372, 419
DHCP (Dynamic Host Configuration Protocol) 57
DHCP Ethernet Setup 418
DHCP Server 100
Diagnostic 521
Dial 129
DIAL BACKUP 626
Dial Backup 123
Dial Backup Port Speed 125
Dial Timeout 130, 405
DNS 81, 333
DNS Server
  For VPN Host 81
DNS Servers 98
Domain Name 68, 75, 83, 138, 512, 514
DoS
  Basics 156

Types 157
DoS (Denial of Service) 54
Drop 130
Drop DTR When Hang Up 130
Drop Timeout 130, 405
DSL Modem 58, 434
DTE 128
DTR 128, 404
DTR Signal 128
Dynamic DNS 85
Dynamic DNS Service Provider 86
Dynamic DNS Support 55
Dynamic Host Configuration Protocol 97
DYNDNS Wildcard 85, 87

E

ECHO 138
Edit IP 407, 434
EMAIL 395
E-mail Address 395
Enable Wildcard 87, 396
Encapsulating Security Payload 206
Encapsulation 426, 433, 438
Entering Information 383
ESP 206
ESP Protocol 206
Ethernet 68, 71
Ethernet Encapsulation 109, 425, 432, 433, 438, 442
Ethernet Specification for WAN 625

F

F/W Version 526
Factory Default 400
Factory LAN Defaults 98
Fail Tolerance 123, 445
Features 51
Filename Conventions 525
Filter 415, 441
Applying 496
Configuration 479
Configuring 482
Example 492
Generic Filter Rule 489
Generic Rule 490
NAT 495
Remote Node 497
Structure 480
TCP/IP Rule 486
Filters
Executing a Filter Rule 480
IP Filter Logic Flow 488
Finger 138
Firewall 54
Access Methods 169
Activating 477
Address Type 180
Alerts 188
Connection Direction 172
Creating/Editing Rules 177
Custom Ports 180
Enabling 169
Firewall Vs. Filters 166
Guidelines For Enhancing Security 166
Introduction 155
LAN to WAN Rules 173
Policies 169
Rule Checklist 171
Rule Logic 170
Rule Security Ramifications 171
Services 185
SMT Menus 477
Types 153
When To Use 167
Firmware 514
First DNS Server 84
Flow Control 381

FTP 85, 137, 138, 308, 327, 557
FTP File Transfer 536
FTP Restrictions 308, 529, 557
FTP Server 58, 469
Full Feature 117
Full Network Management 57

G

Gateway IP Addr 440
Gateway IP Address 427, 449
General Setup 67, 82, 391
Global 132
Global End IP 142, 144
Global Start IP 142, 144
Group Authentication 220
Group ID 220
Group Password 220

H

Half-Open Sessions 189
Hardware Setup 59
Hidden Menus 383
Host 88, 395
Host IDs 632
Host Names 86
How SSH works 320
HTTP 138, 154, 156, 157
HTTPS 54, 309
HTTPS Example 312
HyperTerminal program 531, 534

I

ICMP Commands That Trigger Alerts 160
ICMP echo 159
ICMP Vulnerability 160
Idle Timeout 114, 127, 408, 436
IEEE 802.1x 54
IGMP 99, 118, 127
IGMP-V1 118
IGMP-v1 127
IGMP-V2 118
IGMP-v2 127
Illegal Commands 160
Incoming Protocol Filters 423
Initial Screen 381
Inside 132
Inside Global Address 132
Inside Local Address 132
Internet Access 425
  ISP's Name 426
Internet Access Setup 425, 426, 454
Internet Control Message Protocol (ICMP) 159
Internet Group Multicast Protocol 99, 118
Introduction to Filters 479
IP Address 74, 137, 372, 407, 410, 421, 422, 427, 439
  Remote 410
IP Address Assignment 410, 427, 439
IP Addressing 631
IP Alias 56, 104, 422
IP Alias Setup 421, 422
IP Classes 631
IP Multicast 56
  Internet Group Management Protocol (IGMP) 56
IP Pool 419, 420
IP Pool Setup 97
IP Ports 157
IP Spoofing 157, 161
IP Static Route 149, 447, 448, 449
  Active 449
  Destination IP Address 449

IP Subnet Mask 449
Name 449
Route Number 449
IP Subnet Mask 410, 422
Remote 410
IPSec VPN Capability 53
ISP's Name 426

J

Java 194

K

Key Fields For Configuring Rules 172

L

LAN IP Address 355, 359
LAN Port Filter Setup 417
LAN Setup 97, 107, 417, 418
LAN TCP/IP 98
LAN to WAN Rules 173
LAND 158, 159
Local 132
Local End IP 142, 144
Local Start IP 142, 144
Log 176, 514
Log Facility 516
Logging 57
Logging In to the SMT 382
Login Name 426
Login Screen 382
Logs 349

M

MAC Address 400
MAC Addresses 103
MAIN MENU 65
Main Menu 384
Management Information Base (MIB) 330
Many One-to-One 143, 144
Many to Many No Overload 135
Many to Many Overload 135
Many to One 135
Many-to-Many Ov 144
Many-to-Many Overload 143, 144
Many-to-On 144
Many-to-One 143
Maximum Incomplete High 192
Maximum Incomplete Low 192
Max-incomplete High 190
Max-incomplete Low 190, 192
MD5 207
Mean Time Between Failures 625
Media Access Control 103
Metric 107, 117, 122, 125, 152, 411, 436, 440, 449
MTBF 625
Multicast 99, 118, 127, 411, 421, 441
Multicast Version 127
Multimedia 713
My IP Addr 438
My Login 406, 434
My Login Name 426
My Password 303, 305, 406, 426, 427, 434
My Server IP Addr 438
My WAN Address 410

N

Nailed-Up Connection 408, 436
Nailed-up Connection 114, 436
Nailed-Up Connections 438
NAT 72, 75, 117, 126, 137, 138, 139, 140, 411, 440, 495
Application 134

Applying NAT in the SMT Menus 453
Configuring 456
Definitions 131
Examples 465
How NAT Works 133
Mapping Types 135
Ordering Rules 460
Port Restricted Cone 133
Restricted Cone 134
What NAT does 132
NAT Routers 718
NAT Traversal 337, 338, 339
NetBIOS commands 160
NetBIOS over TCP/IP 118, 246
Network Address Translation 117, 126, 427
Network Address Translation (NAT) 56, 453
Network Address Translators 718
Network Management 138
NNTP 138
Nortel Firmware Version 370

O

Off Line 87
Offline 396
OK Response 714
On Demand Client Tunnel 221
One Minute High 191
One Minute Low 191
One to One 135
One-Minute High 190
One-to-One 144
Operating Mode 126
Operation Temperature 625
Outgoing Protocol Filters 423
Outside 132

P

Packet Direction 176, 178
Packet Filtering 55, 166
Packet Filtering Firewalls 154
PAP 125, 407, 436
Password 62, 87, 303, 305, 382, 385, 426, 427, 499
PAT 144
Period(hr) 407, 436
Phone Number 125
Ping 522
Ping of Death 157
Point-to-Point Protocol over Ethernet 110
Point-to-Point Tunneling Protocol 70, 113, 138
POP3 138, 156, 157
Port Configuration 181
Port Forwarding 57
Port Restricted Cone NAT 133
Power Adaptor Specifications 627
PPP 408
PPPoE 55, 68, 71, 72, 617
PPPoE Encapsulation 110, 425, 429, 432, 434, 436, 442
PPTP 68, 70, 72, 138, 621
Client 427, 428
Configuring a Client 427, 428
PPTP Encapsulation 55, 113, 437
Pre-defined NTP Time Server List 89
Pre-Shared Key 217, 239
Primary Phone Number 125
Priority 107, 125
Private 117, 152, 411, 440, 450
Private IP Address 74
product support 49
Proportional Bandwidth Allocation 286
Protocol Filters 423

Incoming 423
Outgoing 423
Protocol/Port 355, 357
publications
hard copy 49
related 48

Q

Quick Start Guide 61

R

RADIUS 297
Shared Secret Key 298
RADIUS Message Types 297
RAS F/W Version 514
Real time Transport Protocol 717
Rem IP Address 410
Rem Node Name 406, 409, 433
Remote Management 555
Remote Management and NAT 308
Remote Management Limitations 308, 557
Remote Node 431
Profile (Traffic Redirect Field) 443
Remote Node Filter 415, 441
Reports 354
Required fields 383
Reset 63
Reset Button 53
Resetting the Time 554
Response Strings 128
Restore 378
Restore Configuration 532
Restrict Web Features 194
Retry Count 130
retry count 405
Retry Interval 130
retry interval 405
RFC 1889 717
RFC 3489 718
RIP 98, 99, 126, 411, 421, 423, 440
Direction 423
Version 423, 441
RIP Direction 99, 118
RIP Version 98, 118, 126
RIP-1 98, 118, 126
RIP-2 98
RIP-2B 99, 118, 126
RIP-2M 99, 118, 126
Roadrunner Manager 115
RoadRunner Support 57
RoadRunner Toshiba 115
Root Class 289
Route 434
Routing Information Protocol 98
RR- Service Type 114
RR-Telstra 115
RTP 717
Rule Summary 184
Rules 169, 173
Checklist 171
Creating Custom 169
Key Fields 172
LAN to WAN 173
Logic 170
Predefined Services 185
Source and Destination Addresses 179

S

SA Monitor 244
Saving the State 161
Schedule Sets
Duration 366, 561
Schedules 436, 438

Second DNS Server 84
Secondary Phone Number 125
Secure FTP Using SSH Example 325
Secure Telnet Using SSH Example 323
Security Ramifications 171
Server 92, 135, 136, 143, 144, 426, 427, 434, 456, 459, 462, 463, 464, 467, 469, 552
Server Auto Detect 87
Server IP 434
Service 172
Service Name 434
Service Type 114, 176, 181, 426, 433
Services 138
Session Initiation Protocol 713
setup a schedule 365, 560
SHA1 207
Single User Account 126, 144
SIP Account 713
SIP ALG 718
SIP Application Layer Gateway 718
SIP Client 715
SIP INVITE Request 714
SIP Redirect Server 716
SIP Register Server 717
SIP Servers 715
SIP URI 713
SIP User Agent Server 715
SMT 382
SMT Menus at a Glance 387
SMTP 138
Smurf 159, 160
SNMP 56, 138, 329
  Community 500
  Configuration 499
  Get 330
  Manager 330
  MIBs 330
  Trap 330
  Trusted Host 500
SNMP (Simple Network Management Protocol) 56
Source & Destination Addresses 179
Source Address 172, 178
SSH 53, 319
SSH Implementation 321
Start Port 148
Stateful Inspection 54, 153, 154, 161, 162, 163
  Process 162
Static DHCP 103
Static Route 149
SUA 137, 138, 140
SUA (Single User Account) 136, 453
SUA Only 117, 126
SUA Server 139
Sub-class Layers 289
Subnet Mask 74, 180, 410, 421, 427, 439, 449
Subnet Masks 633
Subnetting 633
support, Nortel Networks 49
SYN Flood 158, 159
SYN-ACK 158
Syslog 184, 515
Syslog IP Address 516
System DNS Servers 84
System General Setup 83
System Information 509, 512, 513
System Maintenance 350, 509, 510, 511, 512, 513, 514, 515, 521, 522, 526, 529, 539, 541, 545, 548, 550, 552
System Management Terminal 382
System Name 83, 392
System Screens 81

System Status 510
System Timeout 308

T

TA 128
TCP Maximum Incomplete 190, 192
TCP Security 164
TCP/IP 156, 157, 158, 326, 409, 418, 421, 438, 485, 486, 488, 491, 495
  Setup 421
TCP/IP and DHCP Setup 418
TCP/IP filter rule 485
Teardrop 157
technical publications 49
technical support 49
Telnet 325
Telnet Configuration 326
Terminal Emulation 381
text conventions 47
TFTP File Transfer 539
TFTP Restrictions 308, 529, 557
Third DNS Server 84
Threshold Values 189
Time and Date 53
Time and Date Setting 551, 552
Time Setting 90
Time Warner 115
Time Zone 553
Timeout 408, 428, 429, 436
Trace 514
Traceroute 161
Tracing 57
Traffic Redirect 57, 120, 121
  Setup 443
Triangle 597
Triangle Route Solutions 598
Trigger Port Forwarding 473
  Process 145

U

UDP/ICMP Security 165
Uniform Resource Identifier 713
Universal Plug and Play 55
Universal Plug and Play (UPnP) 337, 339
Upgradeable Firmware 58
Upload Firmware 536
Uploading a Configuration File Via Console Port 64
UPnP 55
UPnP Examples 341
UPnP Port Mapping 340
Upper Layer Protocols 165
URL Keyword Blocking 195
User Name 395
User Profiles 301, 451
Username 62, 382

V

VPN 113
VT100 381

W

WAN DHCP 522
WAN MAC 119
WAN Setup 76, 399, 400
WAN to LAN Rules 173
Web Proxy 195
Web Site Hits 355, 356
WebGUI 61, 65, 155, 166, 171, 478
Windows Networking 118, 246
Wizard Setup 67, 68, 74

WWW 310
www.dyndns.org 396

X

XMODEM protocol 527
Xmodem Upload 64