AudioCodes CPE & Access Gateway Products

MP-20x series

MediaPack™ Series Telephone Adapters with Integrated Router

MP-202 Telephone Adapter User's Manual

Version 2.6.0

Document #: LTRT-50605

AudioCodes

Notice

This document describes the MP-202 Telephone Adapter available from AudioCodes. Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed and downloaded by registered Technical Support customers at www.AudioCodes.com.

This document is subject to change without notice.

Refer to the current release notes that may be included with your documentation or hardware delivery.

Date Published: Apr-29-2008 Date Printed: May-01-2008

Tip: When viewing this manual on CD, Web site or on any other electronic copy, all cross-references are hyperlinked. Click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly. To return back to the point from where you accessed the cross-reference, press Alt + ← .

Trademarks

AC logo, Ardito, AudioCoded, AudioCodes, AudioCodes logo, CTI², CTI Squared, InTouch, IPmedia, Mediant, MediaPack, MP-MLQ, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, 3GX, TrunkPack, VoicePacketizer, VoIPerfect, What's Inside Matters, Your Gateway To VoIP, are trademarks or registered trademarks of AudioCodes Limited.

All other products or trademarks are the property of their respective owners.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@AudioCodes.com.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used. Only industry-standard terms are used throughout this manual. Hexadecimal notation is indicated by 0x preceding the number. When the term 'device' is used, it refers to the MP-202 Telephone Adapter.

Related Documentation

Document Title
MP-202 Telephone Adapter Quick Installation Guide
MP-202 Telephone Adapter Release Notes
AC494 VoIP SoC Data Book
AC494 VoIP SoC User’s Manual
AC494 VxWorks SDK Getting Started Guide
AC494 Linux SDK Getting Started Guide
AC494 SDK Release Notes for VxWorks
AC494 SDK Release Notes for Linux
AC494 SDK Installation Guide for VxWorks
AC494 SDK Installation Guide for Linux
AC494 VoIP SoC Product Overview
AC494 SoC Reference Design

Table of Contents

1 Introducing AudioCodes' MP-202 Telephone Adapter 15

2 Cabling the MP-202 Telephone Adapter 17

3 Setting up a Network Connection 19

3.1 Defining Your PC's Network Connection 19
3.1.1 Windows XP 20
3.1.2 Linux 20
3.2 Configuring the MP-202's Network Connection 21
3.2.1 Logging In 21
3.2.2 Configuring 'Quick Setup' Screen Parameters 22
3.2.2.1 Configuring Your Internet Connection 23

4 Using the MP-202's Web Interface 27

4.1 Your Home Network Map 27
4.2 Web Interface Left Sidebar Icons 29
4.3 Navigational Aids 29
4.4 Managing Tables 30

5 Configuring VoIP Parameters 31

5.1 Voice over IP Screen 31
5.1.1 Configuring Signaling Protocol Parameters 32
5.1.2 Configuring Dialing Parameters 39
5.1.3 Configuring Media Streaming Parameters 41
5.1.3.1 Configuring Codecs 43
5.1.3.2 Supported Codecs 43
5.1.3.3 Packetization Time 44
5.1.4 Configuring Voice and Fax Parameters 44
5.1.5 Configuring Services Parameters 47
5.1.6 Configuring Line Settings Screen 49
5.1.7 Configuring Speed Dial Settings 50
5.1.8 Configuring Telephone Interfaces 53

6 Connecting the MP-202 to a VoIP Service Provider 55

6.1 Opening a SIP Account 55
6.2 Configuring VoIP Parameters 55

7 Making VoIP Calls 57

7.1 Placing a Call 57
7.2 Answering a Waiting Call 57
7.3 Putting a Call on Hold 57
7.4 Performing a Call Transfer 58
7.5 Establishing a 3-Way Conference 58
7.6 Forwarding Calls to Another Phone 59

8 Quality of Service (QoS) 61
8.1 Traffic Shaping 61
8.1.1 Device Traffic Shaping 61
8.1.2 Shaping Classes 63
8.1.2.1 Class Rules 64
8.2 Traffic Priority 66
8.3 DSCP Mapping 70
8.4 802.1p Mapping 72
8.5 Class Statistics 73
8.6 Configuring Basic VoIP QoS 73
9 WAN Settings 77
9.1 WAN Ethernet 77
9.1.1 General 78
9.1.2 Internet Protocol Settings 79
9.1.3 DNS Server 80
9.1.4 Routing 80
9.1.5 Advanced Routing Properties 81
9.1.6 Internet Connection Firewall 81
9.2 WAN PPPoE 82
9.2.1 General 82
9.2.2 PPP Configuration 82
9.2.3 PPP Authentication 83
9.2.4 PPP Encryption 84
9.2.5 PPP Compression 85
9.2.6 Internet Protocol 86
9.2.7 DNS Server 86
9.2.8 Routing 86
9.2.9 Internet Connection Firewall 86
9.3 WAN PPTP 86
9.3.1 Creating a PPTP Connection with the Connection Wizard 86
9.3.2 Creating a PPTP VPN Connection with the Connection Wizard 89
9.3.3 General 91
9.3.4 PPP Configuration 91
9.3.5 PPP Authentication 91
9.3.6 PPP Encryption 92
9.3.7 Internet Protocol 92
9.3.8 DNS Server 92
9.3.9 Routing 92
9.3.10 Internet Connection Firewall 92
9.4 WAN L2TP 92
9.4.1 Creating an L2TP IPSec VPN Connection with the Connection Wizard 92
9.4.2 Creating an L2TP IPSec VPN Connection with the Connection Wizard 95
9.4.3 General 97
9.4.4 PPP Configuration 97
9.4.5 PPP Authentication 97
9.4.6 PPP Encryption 97
9.4.7 PPP Compression 98
9.4.8 Internet Protocol 98
9.4.9 DNS Server 98
9.4.10 Routing 98
9.4.11 Internet Connection Firewall 98

10 VLAN and Bridge Settings....99

10.1 Virtual LAN Interface (VLAN)....99

10.1.1 Creation with the Connection Wizard....99
10.1.2 General....100
10.1.3 IP Address Distribution....102
10.1.4 Routing....104
10.1.5 Internet Connection Firewall....106
10.1.6 Allow Unrestricted Administration....106
10.1.7 Additional IP Addresses....107
10.1.8 Example of Configuring 3 VLANs: VoIP, Data and Management....107

10.2 WAN-LAN Bridge....114

10.2.1 Creation with the Connection Wizard....114
10.2.2 General....116
10.2.3 Internet Protocol Settings....116
10.2.4 Bridge Settings....117
10.2.5 Examples of Configuring VLANs in Bridge Mode....118
10.2.5.1 Example 1 - Configuring 3 VLANs: VoIP, Data and Management....118
10.2.5.2 Example 2 - Configuring Tagged VoIP, Untagged Data Traffic....122
10.2.5.3 Example 3 - Configuring VoIP and Data in the Same VLAN....127

11 TR-069 CPE WAN Management Protocol....129

11.1 Overview....129

11.2 TR-069 Parameter List....129

11.2.1 Viewing, Changing TR-069 Parameters Using the CLI....132

12 Security....135

12.1 General Security Level Settings....136

12.2 Access Control....138

12.3 Port Forwarding....140

12.4 DMZ Host....144

12.5 Port Triggering....145

12.6 Website Restrictions....148

12.7 Advanced Filtering....151

12.8 Security Log....155

13 Advanced Settings....161

13.1 Remote Administration....163

13.2 About the MP-202....165

13.3 Configuration File....165

13.3.1 Loading From a Computer in the Network....167
13.3.2 Loading From a Remote Server....169

13.4 Restart....171

13.5 Restoring Default Settings....171

13.6 Diagnostics....172

13.6.1 Diagnosing Network Connectivity....172
13.6.2 Performing a Traceroute....173

13.7 MAC Cloning....174

13.8 Regional Settings 174
13.9 System Settings 175
13.10 SNMP 178
13.10.1 Configuring Your Gateway's SNMP Agent 178
13.11 Universal Plug and Play 179
13.12 Firmware Upgrade 179
13.12.1 Upgrading From a Computer in the Network 180
13.12.2 Upgrading From the Internet 181
13.13 Scheduler Rules 182
13.14 Date & Time 184
13.15 Configuring Users 185
13.15.1 Email Notification 186
13.16 Routing 187
13.16.1 Managing Routing Table Rules 187
13.16.2 Multicasting 188
13.17 Network Objects 188
13.18 Dynamic DNS 189
13.18.1 Opening a Dynamic DNS Account 189
13.19 IP Address Distribution 191
13.19.1 DHCP Server Parameters 192
13.19.2 DHCP Relay Parameters 194
13.19.3 DHCP Connections 195
13.20 DNS Server 196
13.20.1 Viewing and Modifying the DNS Table 197
13.21 Protocols 198
14 System Monitoring 201
14.1 Connections 201
14.2 Traffic 202
14.3 System Log 202
14.4 System Up Time 203
14.5 Voice over IP 204
15 Software and Hardware Specifications 205

List of Figures

Figure 2-1: Cabling the Device 17
Figure 3-1: IP and DNS Configuration....20
Figure 3-2: 'Welcome' Screen 21
Figure 3-3: Logging In 21
Figure 3-4: Quick Setup....22
Figure 3-5: Internet Connection - Automatic IP Address Ethernet Connection....23
Figure 3-6: Internet Connection - Manual IP Address Ethernet Connection....24
Figure 3-7: Internet Connection - PPPoE....25
Figure 3-8: Internet Connection - Point-to-Point Tunneling Protocol 25
Figure 3-9: Layer 2 Tunneling Protocol 26
Figure 3-10: Internet Connection - No Internet Connection 26
Figure 4-1: Network Map....27
Figure 4-2: Host Information....28
Figure 4-3: Typical Table Structure 30
Figure 5-1: VoIP - Signaling Protocol 32
Figure 5-2: VoIP - Signaling Protocol - SIP Proxy and Registrar....33
Figure 5-3: VoIP - Signaling Protocol - SIP Proxy and Registrar....36
Figure 5-4: VoIP - Signaling Protocol - SIP Outbound Proxy....37
Figure 5-5: VoIP - Signaling Protocol - NAT Traversal 38
Figure 5-6: VoIP - Dialing 39
Figure 5-7: VoIP - Media Streaming - Basic....41
Figure 5-8: VoIP - Media Streaming - Advanced....42
Figure 5-9: VoIP - Voice and Fax 44
Figure 5-10: VoIP - Services - Advanced 47
Figure 5-11: VoIP - Line Settings 49
Figure 5-12: VoIP - Line Settings - Defining a New Line....49
Figure 5-13: VoIP - Speed Dial 50
Figure 5-14: VoIP - Speed Dial Settings 50
Figure 5-15: VoIP - Speed Dial - Local Line....51
Figure 5-16: VoIP - Speed Dial Settings - Local Line....51
Figure 5-17: VoIP - Speed Dial - Direct Call....52
Figure 5-18: VoIP - Telephone Interface....53
Figure 5-19: VoIP - Telephone Interface - NW Map....53
Figure 6-1: VoIP - Line Settings 55
Figure 6-2: VoIP - Line Settings - Defining a New Line....56
Figure 8-1: QoS - Add Device Traffic Shaping....61
Figure 8-2: QoS - Edit Device Traffic Shaping 62
Figure 8-3: QoS - Edit Device Traffic Shaping - Add Class 63
Figure 8-4: QoS - Edit Device Traffic Shaping - Edit Class....63
Figure 8-5: QoS - Edit Device Traffic Shaping - Edit Class - Add Traffic Priority Rule 65
Figure 8-6: QoS - Traffic Shaping 68
Figure 8-7: QoS - Add Traffic Priority Rule....68
Figure 8-8: QoS - DSCP Settings....70
Figure 8-9: QoS - Edit DSCP Settings 71
Figure 8-10: QoS - 802.1p Settings....72
Figure 8-11: QoS - Class Statistics 73
Figure 8-12: QoS - Edit Device Traffic Shaping 74
Figure 8-13: QoS - Edit Device Traffic Shaping - Submitting the Configuration 75
Figure 9-1: WAN Ethernet Properties....77
Figure 9-2: WAN Ethernet Configuration....78
Figure 9-3: Internet Protocol Settings - No IP Address 79
Figure 9-4: Obtain DNS Server Address Automatically 80
Figure 9-5: DNS Server Settings....80
Figure 9-6: Internet Connection Firewall 81
Figure 9-7: Additional IP Addresses....81

Figure 9-8: General PPPoE Settings....82
Figure 9-9: PPP Configuration 83
Figure 9-10: PPP Authentication Settings....84
Figure 9-11: PPP Encryption....85
Figure 9-12: PPP Compression....85
Figure 9-13: Internet Cable Modem Connection 87
Figure 9-14: Point-to-Point Tunneling Protocol....88
Figure 9-15: Connection Summary 88
Figure 9-16: VPN Client or Point-To-Point....89
Figure 9-17: Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)....90
Figure 9-18: Connection Summary 90
Figure 9-19: General PPTP Settings....91
Figure 9-20: VPN Client or Point-To-Point....93
Figure 9-21: Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)....94
Figure 9-22: Connection Summary 94
Figure 9-23: VPN Client or Point-To-Point....95
Figure 9-24: Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)....96
Figure 9-25: Connection Summary 96
Figure 9-26: PPP Compression....98
Figure 10-1: VLAN Interface....99
Figure 10-2: Connection Summary 100
Figure 10-3: Internet Protocol Settings - No IP Address 102
Figure 10-4: Internet Protocol Settings - Automatic IP.... 102
Figure 10-5: Internet Protocol Settings . Static IP 102
Figure 10-6: IP Address Distribution - DHCP Server 103
Figure 10-7: IP Address Distribution - DHCP Relay.... 104
Figure 10-8: DHCP Relay Server Address.... 104
Figure 10-9: IP Address Distribution - Disable DHCP.... 104
Figure 10-10: Advanced Routing Properties 106
Figure 10-11: Internet Connection Firewall 106
Figure 10-12: Allow Unrestricted Administration 106
Figure 10-13: Additional IP Addresses.... 107
Figure 10-14: Using VLAN - Setup.... 107
Figure 10-15: Example of Using VLAN - VLAN Interface Screen 108
Figure 10-16: Verifying a New Interface on the WAN Side 109
Figure 10-17: Configuring WAN Ethernet.... 109
Figure 10-18: Use the Following IP Address.... 110
Figure 10-19: Routing - Advanced 110
Figure 10-20: Routing - Advanced - Extended Parameters 110
Figure 10-21: Route Settings 111
Figure 10-22: Input Rule Sets 111
Figure 10-23: Edit Advanced Filter.... 112
Figure 10-24: Testing the Setup.... 112
Figure 10-25: Testing the Setup.... 113
Figure 10-26: Testing the Setup.... 113
Figure 10-27: Bridge Options 114
Figure 10-28: Network Bridging.... 115
Figure 10-29: WLAN-LAN - Network Bridging.... 115
Figure 10-30: Connection Summary - Configure Existing Bridge 116
Figure 10-31: Bridge Settings.... 117
Figure 10-32: Example of Using Bridge Mode and Configuring VLANs 118
Figure 10-33: Network Connections.... 119
Figure 10-34: Configuring WAN Ethernet.... 119
Figure 10-35: Network Bridging.... 120
Figure 10-36: No IP Address.... 120
Figure 10-37: System Monitoring 121
Figure 10-38: Example of Tagging Voice and Untagging Data.... 122
Figure 10-39: WAN/LAN Bridge 123

Figure 10-40: VLAN Interface Screen 123
Figure 10-41: Bridge Section of the Screen 124
Figure 10-42: VLAN Settings..... 124
Figure 10-43: No IP Address..... 124
Figure 10-44: Configuring WAN Ethernet..... 125
Figure 10-45: System Monitoring 125
Figure 10-46: Testing the Setup..... 126
Figure 10-47: Testing the Setup..... 126
Figure 10-48: VoIP and Data on same VLAN 127
Figure 10-49: No IP Address..... 128
Figure 11-1: TR-069 CPE WAN Management Protocol..... 129
Figure 12-1: Firewall in Action..... 135
Figure 12-2: General Security Level Settings..... 136
Figure 12-3: Access Control..... 138
Figure 12-4: Add Access Control Rule 139
Figure 12-5: Port Forwarding..... 141
Figure 12-6: Add Port Forwarding Rule..... 141
Figure 12-7: Add a Specific Protocol..... 142
Figure 12-8: Forward to a Specific Port..... 142
Figure 12-9: Add a Specific Schedule..... 142
Figure 12-10: Port Forwarding Rule 142
Figure 12-11: DMZ Host..... 144
Figure 12-12: Port Triggering 145
Figure 12-13: Adding Port Triggering Rules..... 146
Figure 12-14: Edit Service Server Ports..... 146
Figure 12-15: Edit Service Server Ports..... 147
Figure 12-16: Edit Service Opened Ports..... 147
Figure 12-17: Edit Service Opened Ports..... 147
Figure 12-18: New Port Triggering Rule..... 148
Figure 12-19: Website Restrictions 149
Figure 12-20: Restricted Website..... 149
Figure 12-21: Add a Specific Host..... 150
Figure 12-22: Add a Specific Schedule 150
Figure 12-23: Advanced Filtering 151
Figure 12-24: Add Advanced Filter..... 152
Figure 12-25: Specify Source Address..... 153
Figure 12-26: Specify Protocol 153
Figure 12-27: Set Priority Rule 154
Figure 12-28: Set DSCP Rule 154
Figure 12-29: Security Log 155
Figure 12-30: Security Log Settings 156
Figure 13-1: Advanced Settings 161
Figure 13-2: Advanced - About the Gateway 165
Figure 13-3: Contents of the Configuration File 166
Figure 13-4: Load Configuration File..... 167
Figure 13-5: Advanced - Loading Configuration File from a PC on the Network..... 168
Figure 13-6: Successful Configuration File Loading 168
Figure 13-7: Reboot After Configuration File Load 168
Figure 13-8: Load Configuration File..... 169
Figure 13-9: Advanced - Restart 171
Figure 13-10: Restore Defaults 171
Figure 13-11: Advanced - Diagnostics 172
Figure 13-12: Advanced - Diagnostics - Statistics 173
Figure 13-13: Advanced - MAC Cloning Settings 174
Figure 13-14: Regional Settings..... 175
Figure 13-15: System Settings..... 177
Figure 13-16: Advanced - SNMP 178

Figure 13-17: Advanced - Universal Plug n Play 179
Figure 13-18: Advanced - Firmware and Configuration Upgrade 180
Figure 13-19: Advanced - Upgrading from a Computer in the Network 180
Figure 13-20: Upgrade in Progress 181
Figure 13-21: Remote Update Check 182
Figure 13-22: Advanced - Scheduler Rules 182
Figure 13-23: Advanced - Scheduler Rules - Edit Scheduler Rule 183
Figure 13-24: Advanced - Scheduler Rules - Time Segment Edit 183
Figure 13-25: Date & Time Settings 184
Figure 13-26: Managing Users 186
Figure 13-27: Routing Rules 187
Figure 13-28: Routing Rule Settings 188
Figure 13-29: Advanced - Dynamic DNS 190
Figure 13-30: Advanced - Dynamic DNS 190
Figure 13-31: DHCP Server Summary 192
Figure 13-32: Advanced - IP Address Distribution - DHCP Server 193
Figure 13-33: DHCP Server Relay 194
Figure 13-34: Advanced - IP Address Distribution - DHCP Relay 194
Figure 13-35: Advanced - IP Address Distribution - DHCP Relay - New IP Address 194
Figure 13-36: Advanced - IP Address Distribution - Connection List 195
Figure 13-37: Advanced - IP Address Distribution - Connection List - New Static Connection 195
Figure 13-38: DNS Server 197
Figure 13-39: DNS Entry 197
Figure 13-40: Advanced - Protocols 198
Figure 13-41: Advanced - Protocols - Edit Service 199
Figure 13-42: Advanced - Protocols - Edit Service - Server Ports 199
Figure 14-1: System Monitoring - Connections 201
Figure 14-2: System Monitoring - Traffic 202
Figure 14-3: System Monitoring - System Log 203
Figure 14-4: System Monitoring - System Up Time 203
Figure 14-5: Advanced - System Monitoring - VoIP 204

List of Tables

Table 4-1: Network Map Symbols 28
Table 4-2: Icons to Indicate the Interface Used for Connecting the PC 28
Table 4-3: Icons Indicating Web-Based Management Screens' Subject Areas 29
Table 4-4: Icons to Quickly Jump to Key Information About Your Home Network 29
Table 4-5: Managing Tables 30
Table 5-1: VoIP - Signaling Protocol 32
Table 5-2: VoIP - Signaling Protocol - Signaling Protocol 34
Table 5-3: VoIP - Signaling Protocol - SIP Proxy and Registrar 34
Table 5-4: VoIP - Signaling Protocol - SIP Timers 35
Table 5-5: VoIP - Signaling Protocol - SIP Registrar SIP 36
Table 5-6: VoIP - Signaling Protocol - SIP Outbound Proxy 37
Table 5-7: VoIP - Signaling Protocol - NAT Traversal 38
Table 5-8: VoIP - Dialing Parameters 39
Table 5-9: VoIP - Media Streaming Parameters - Codecs 42
Table 5-10: VoIP - Advanced - Media Streaming Parameters 43
Table 5-11: VoIP - Advanced - Quality of Service Parameters 43
Table 5-12: VoIP - Advanced - G.723 Bitrate 43
Table 5-13: VoIP - Voice and Fax 45
Table 5-14: VoIP - Services 48
Table 5-15: VoIP - Line Settings 49
Table 5-16: 'Speed Dial Settings' - via Proxy 51
Table 5-17: 'Speed Dial Settings' - Direct Call 52
Table 8-1: Edit Device Traffic Shaping - Parameter Descriptions 62
Table 8-2: Edit Class - Parameter Descriptions 64
Table 8-3: Add Traffic Priority Rule - Parameter Descriptions 66
Table 8-4: Add Traffic Priority Rule - Parameter Descriptions 69
Table 8-5: Edit DSCP Settings- Parameter Descriptions 71
Table 9-1: General Connection Settings 79
Table 9-2: Static or Dynamic Routing Parameters 80
Table 9-3: PPPoE Parameter Descriptions 82
Table 9-4: PPP Configuration Parameter Descriptions 83
Table 9-5: PPP Authentication Parameter Descriptions 84
Table 9-6: PPP Encryption Parameter Descriptions 85
Table 9-7: PPP Compression Parameter Descriptions 85
Table 9-8: General PPTP Settings 91
Table 9-9: General Settings 97
Table 9-10: PPTP Compression Parameters 98
Table 10-1: VLAN Interface - General Communication Parameters 101
Table 10-2: IP Address Distribution Parameters 103
Table 10-3: DHCP Relay 103
Table 10-4: Assigning Static IP Addresses to Network Computers 104
Table 10-5: Routing Parameters 105
Table 11-1: TR-069 Parameter Descriptions 133
Table 12-1: Behavior for the Three Security Levels 137
Table 13-1: Action Icons in the Advanced Screen 161
Table 13-2: Managing Users 185
Table 13-3: Adding a Routing Rule - Parameter Descriptions 187
Table 13-4: Dynamic DNS Parameter Descriptions 191
Table 13-5: DHCP Server Parameter Descriptions 193
Table 15-1: MP-202 Telephone Adapter Software Specifications 205
Table 15-2: MP-202 Telephone Adapter Hardware Specifications 206

Reader's Notes

1 Introducing AudioCodes' MP-202 Telephone Adapter

The MP-202 is a 2-line SIP gateway allowing residential and SOHO subscribers to connect ordinary POTS telephones or fax machines, and is interoperable with leading Softswitches and SIP Application Servers for enabling legacy phone services such as caller ID and call waiting. In addition, the MP-202 includes an internal router with DHCP, NAT, Firewall, PPPoE, PPTP and L2TP capabilities enabling subscribers to connect their home PC or LAN hub/switch to it.

Utilizing AudioCodes' VoIPerfect core architecture, and gaining from its accumulated experience in providing IP telephony solutions, the MP-20x series combines superior voice quality and state-of-the-art features for end users, such as T.38 Fax Relay and G.168-2004 compliant Echo Cancelation. Low bit-rate vocoders (voice coders) can be used simultaneously on both telephony ports to save valuable bandwidth. The Voice over Data prioritization algorithm prevents degradation in voice quality even during large data transfers.

The MP-20x Series is designed for full interoperability with leading Softswitches and SIP Servers for deployment in various network environments. Throughout the years, AudioCodes has invested significant effort in complying with the leading and evolving VoIP standards. Support of the Session Initiation Protocol (SIP), which is commonly found in Voice over Broadband (VoB) networks, assures seamless integration and rapid deployment.

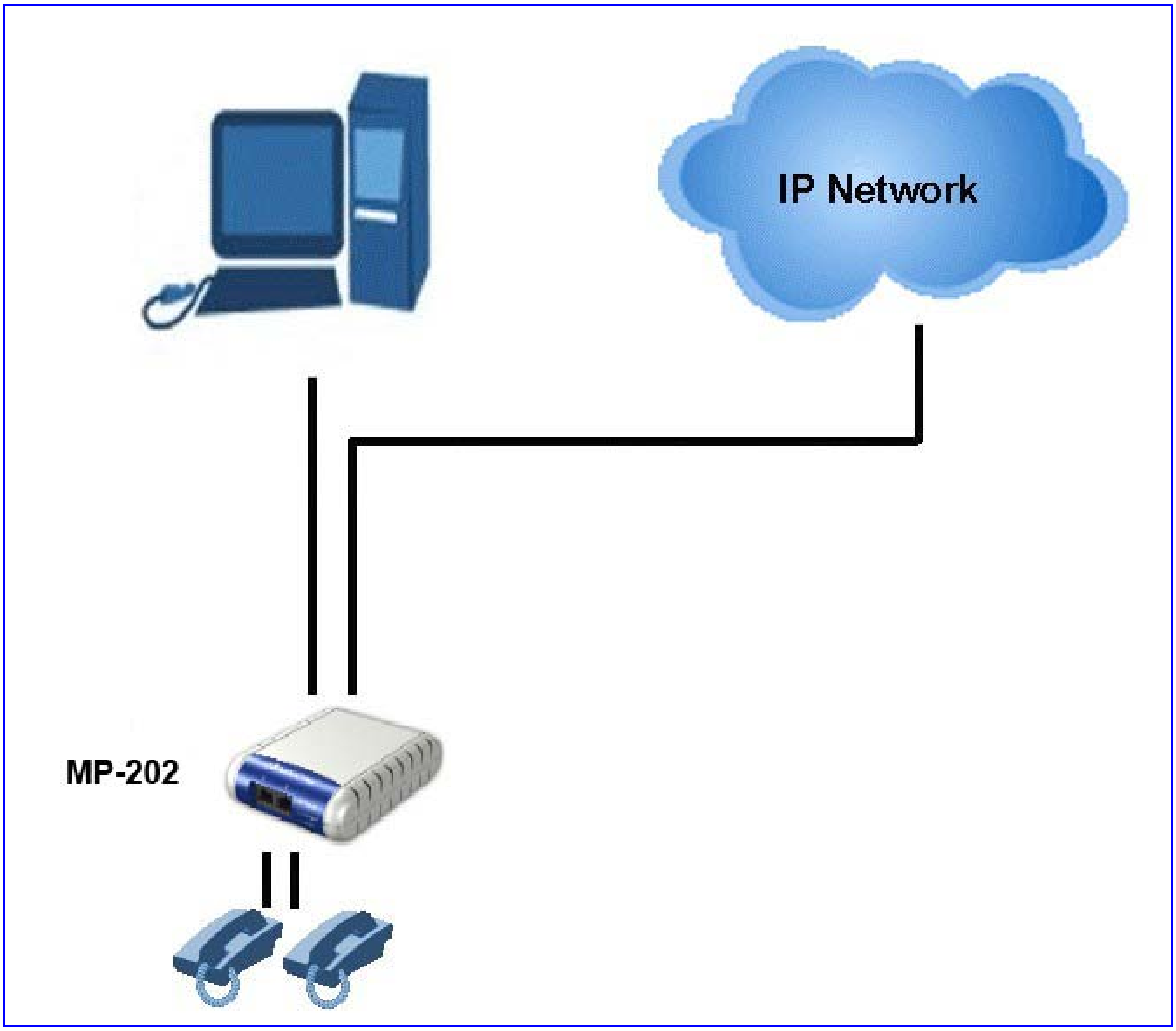
Reader's Notes

2 Cabling the MP-202 Telephone Adapter

➢ To cable the MP-202, take these steps:

1. Connect the MP-202's Ethernet 10/100 Base-T RJ-45 connector labeled 'WAN' to your cable or DSL modem (or other network connection).
2. Connect the MP-202's Ethernet 10/100 Base-T RJ-45 connector labeled 'LAN/PC' to a PC.
3. Optionally, you can connect the MP-202's connector labeled 'LAN/PC' to a switch / hub and connect multiple PCs to the latter.
4. Connect the MP-202's two RJ-11 ports labeled 'PHONE 1' and 'PHONE 2' to two analog telephones.
5. Connect the power cable to the power supply; the green LEDs illuminate; the power-up process takes approximately 40 seconds. When the power up process ends, ‘Phone 1’ and ‘Phone 2’ LEDs turn off; off-hook a phone and listen for a dial tone.

Figure 2-1: Cabling the Device



Reader's Notes

3 Setting up a Network Connection

➢ To set up a network connection:

1. Define your PC's network connection (refer to "Defining Your PC's Network Connection" on page 19)
2. Configure the MP-202's network connection (refer to "Configuring the MP-202's Network Connection" on page 21)

3.1 Defining Your PC's Network Connection

Refer to MP-202 Telephone Adapter Quick Installation Guide for instructions relating to installation on a Windows™ operating system.

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or should be instructed to automatically obtain an IP address using the Network DHCP server.

The MP-202 provides a DHCP server on its LAN and it is recommended to configure your PC to obtain its IP and DNS server IPs automatically.

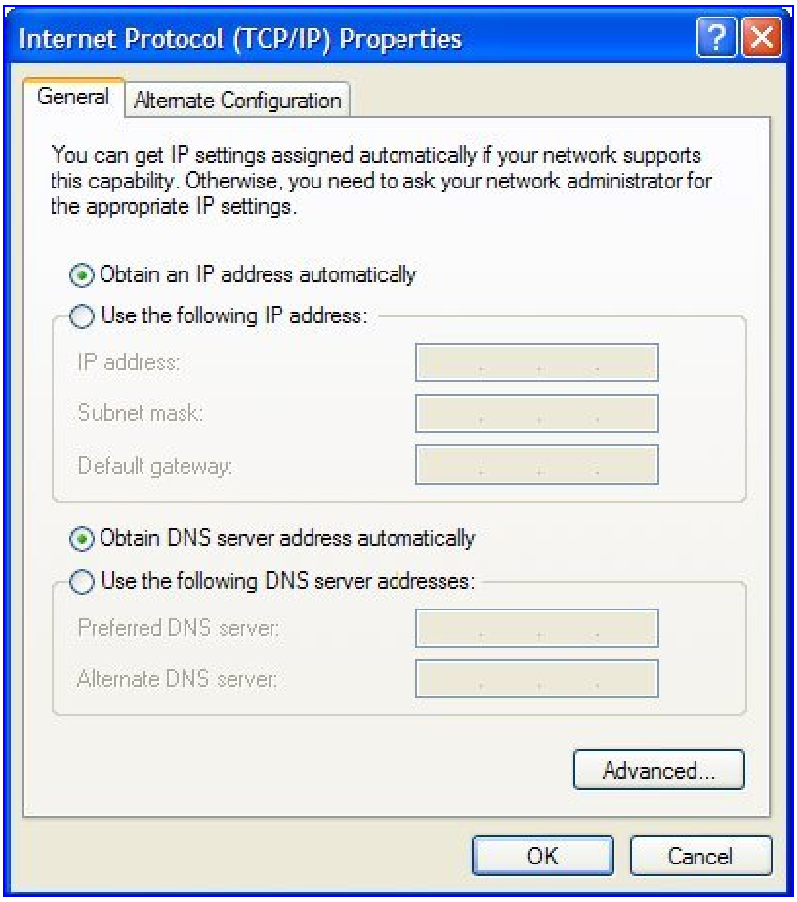
This configuration principle is identical but performed differently on each operating system.

Refer to "Windows XP" on page 20

Refer to "Linux" on page 20

Note: The setup procedure is in most cases unnecessary due to Windows' default network settings. For example, the default DHCP setting in Windows XP is 'client', requiring no further modification. It is advisable however to follow the setup procedure in order to verify that all communication parameters are valid and that the physical cable connections are correct.

Figure 3-1: IP and DNS Configuration



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

3.1.1 Windows XP

1. Access 'Network Connections' from the Control Panel.
2. Right-click on the Ethernet connection icon, and select 'Properties'.
3. Under the 'General' tab, select the 'Internet Protocol (TCP/IP)' component, and press the 'Properties' button.
4. The 'Internet Protocol (TCP/IP)' properties window will be displayed.
5. Select the 'Obtain an IP address automatically' radio button.
6. Select the 'Obtain DNS server address automatically' radio button.
7. Click 'OK' to save the settings.

3.1.2 Linux

1. Login into the system as a super-user, by entering `su' at the prompt.
2. Type 'ifconfig' to display the network devices and allocated IP's.
3. Type 'pump -i <dev>', where <dev> is the network device name.
4. Type 'ifconfig' again to view the new allocated IP address.
5. Make sure no firewall is active on device <dev>.

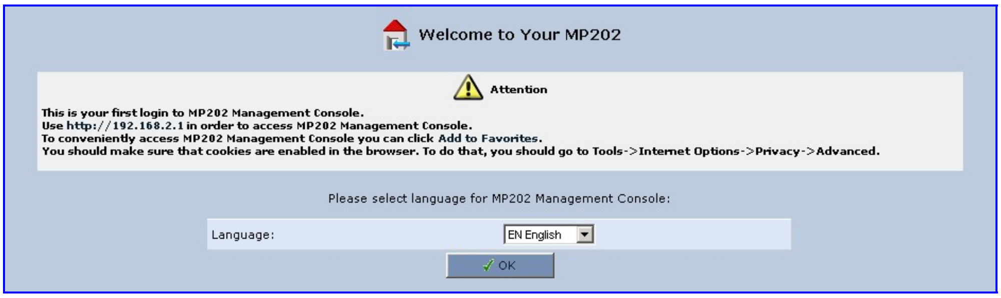
3.2 Configuring the MP-202's Network Connection

The Web-based management interface of the MP-202 allows you to control the device's system parameters. The interface is accessed through a Web browser. For detailed information on the gateway's Web-management interface, refer to "Using the MP-202's Web Interface" on page 27

➢ To access the Web-based management interface:

1. Launch a Web browser on your PC.
2. With your PC connected directly to the MP-202, use URL *http://MP202.home* to access the Web-based management interface; the 'Welcome to Your MP-202' screen appears (refer to the figure); you can click the link 'Add to Favorites' to add a shortcut to the screen in your 'Favorites' folder for future access.

Figure 3-2: 'Welcome' Screen



Welcome to Your MP202

⚠ Attention

This is your first login to MP202 Management Console.
Use http://192.168.2.1 in order to access MP202 Management Console.
To conveniently access MP202 Management Console you can click Add to Favorites.
You should make sure that cookies are enabled in the browser. To do that, you should go to Tools->Internet Options->Privacy->Advanced.

Please select language for MP202 Management Console:

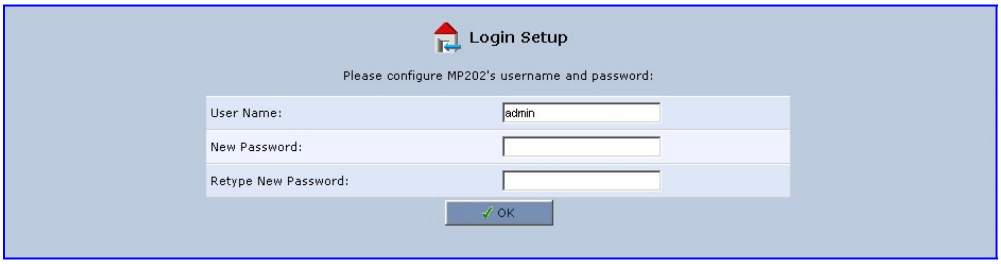
Language: EN English

3. Press 'OK' to continue; the 'Login Setup' screen appears (refer to the figure).

3.2.1 Logging In

The figure below shows the Logging In screen.

Figure 3-3: Logging In



Login Setup

Please configure MP202's username and password:

User Name: admin

New Password:

Retype New Password:

➢ To log in, take these steps:

1. The default User Name is 'admin' (note that it is case sensitive). It is recommended to define a password.
2. To verify that the Password is correct, retype it and press 'OK'; the 'Quick Setup' screen opens (refer to the figure).

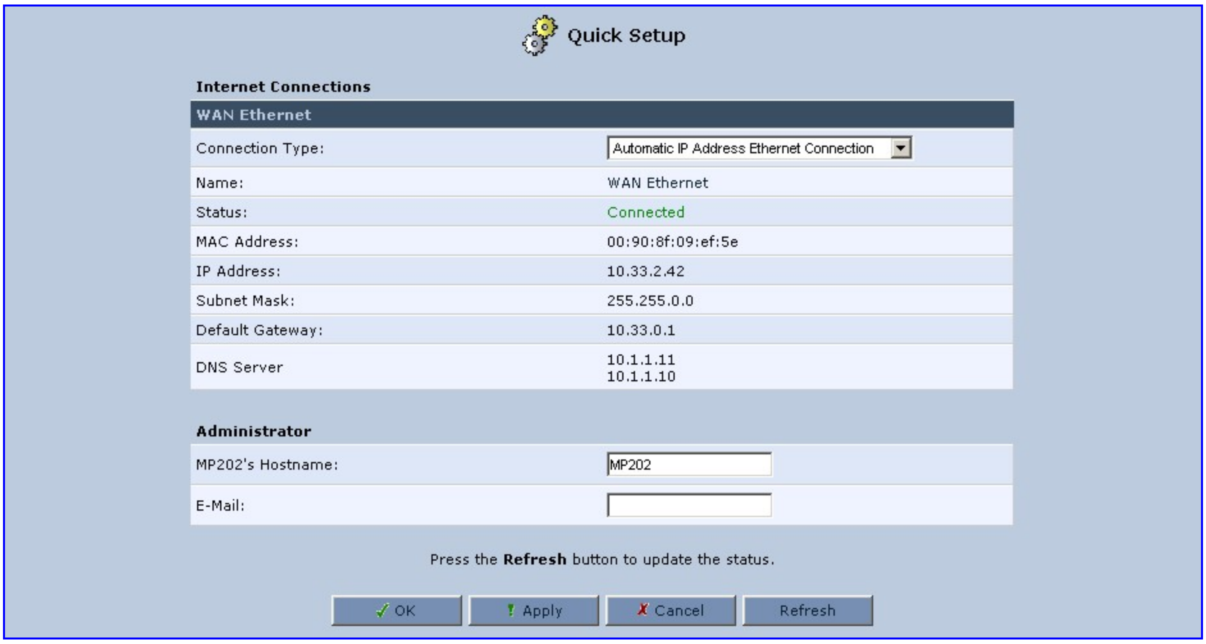
Note: Make sure you retain your User Name and Password for future reference as this is the only way you can access and manage the MP-202.

Note: If there’s inactivity after logging in, a new login becomes necessary after a lapse of 15 minutes.

3.2.2 Configuring 'Quick Setup' Screen Parameters

The 'Quick Setup' screen (refer to the figure) enables the speedy, precise, and accurate configuration of your Internet connection and other important parameters.

Figure 3-4: Quick Setup



Quick Setup

Internet Connections

WAN Ethernet	
Connection Type:	Automatic IP Address Ethernet Connection ▾
Name:	WAN Ethernet
Status:	Connected
MAC Address:	00:90:8f:09:ef:5e
IP Address:	10.33.2.42
Subnet Mask:	255.255.0.0
Default Gateway:	10.33.0.1
DNS Server	10.1.1.11 10.1.1.10

Administrator

MP202's Hostname:	MP202
E-Mail:	

Press the **Refresh** button to update the status.

Note: End users are advised not to modify the section 'Administrator' in the 'Quick Setup' screen. The screen section applies to telephony carrier technicians.

In the 'Administrator' section of the 'Quick Setup' screen:

- Specify the device's host name in the 'Hostname' field. This host name is used to access the device's Web-based management.
- Specify the administrator's e-mail in the 'E-mail' field. System alerts and notifications are sent to this address.

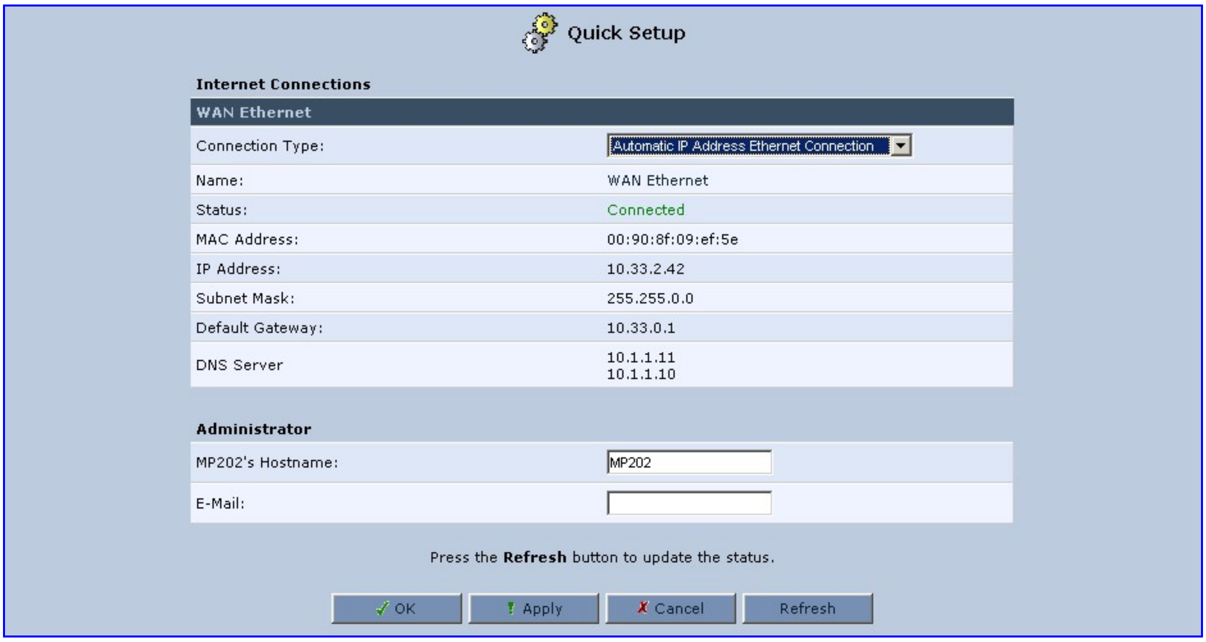
3.2.2.1 Configuring Your Internet Connection

When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Technical information regarding the properties of your Internet connection should be provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or what protocols, such as PPTP or PPPoE, you will be using to communicate over the Internet.

3.2.2.1.1 Automatic IP Address Ethernet Connection

'Automatic IP Address Ethernet Connection' is the default connection type (refer to parameter 'Connection Type' drop-down list in the figure below).

Figure 3-5: Internet Connection - Automatic IP Address Ethernet Connection



Quick Setup

Internet Connections

WAN Ethernet	
Connection Type:	Automatic IP Address Ethernet Connection
Name:	WAN Ethernet
Status:	Connected
MAC Address:	00:90:8f:09:ef:5e
IP Address:	10.33.2.42
Subnet Mask:	255.255.0.0
Default Gateway:	10.33.0.1
DNS Server	10.1.1.11 10.1.1.10

Administrator

MP202's Hostname:	MP202
E-Mail:	

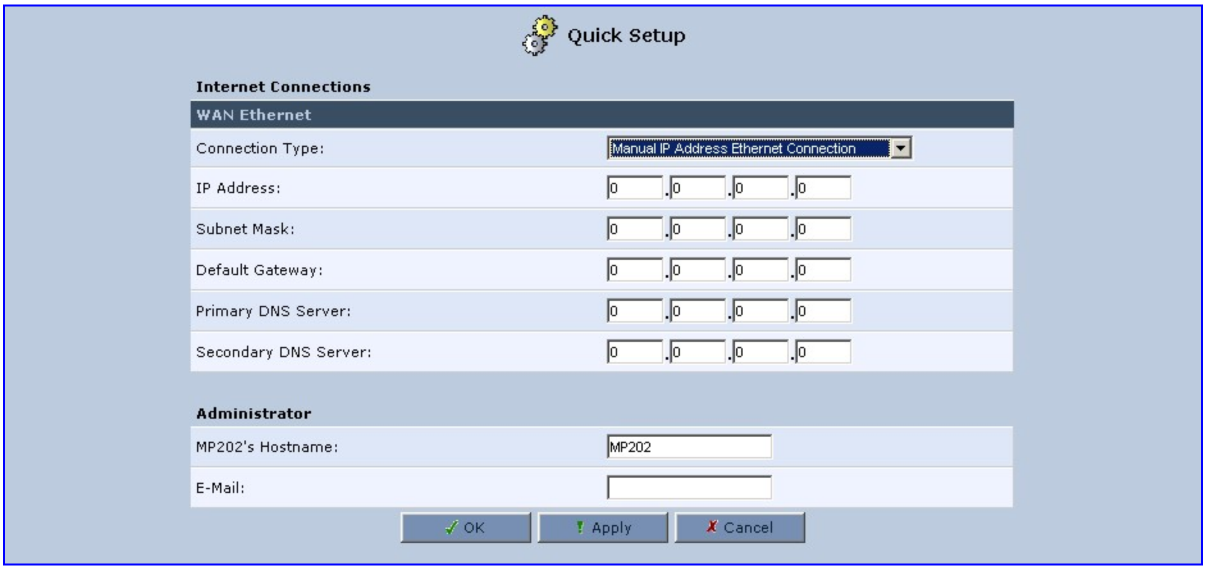
Press the **Refresh** button to update the status.

If left at the default, the MP-202 will obtain the WAN IP and DNS IP addresses from a DHCP server on the WAN.

3.2.2.1.2 Manual IP Address Ethernet Connection

- Select 'Manual IP Address Ethernet Connection' from the 'Connection Type' drop-down list (refer to the figure).

Figure 3-6: Internet Connection - Manual IP Address Ethernet Connection



Internet Connections

WAN Ethernet

Connection Type:	Manual IP Address Ethernet Connection
IP Address:	0 .0 .0 .0
Subnet Mask:	0 .0 .0 .0
Default Gateway:	0 .0 .0 .0
Primary DNS Server:	0 .0 .0 .0
Secondary DNS Server:	0 .0 .0 .0

Administrator

MP202's Hostname:	MP202
E-Mail:	

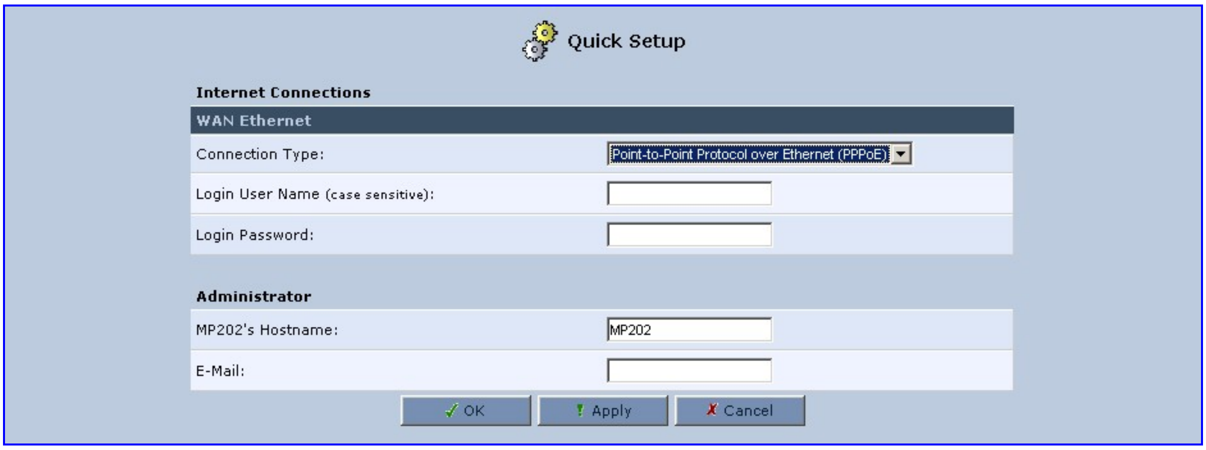
According to your ISP's instructions, specify the following parameters:

- IP address
- Subnet mask
- Default device
- Primary DNS server
- Secondary DNS server

3.2.2.1.3 Point-to-Point Protocol over Ethernet (PPPoE)

- Select 'Point-to-point protocol over Ethernet (PPPoE)' from the 'Connection Type' drop-down list (refer to the figure).

Figure 3-7: Internet Connection - PPPoE



Quick Setup

Internet Connections

WAN Ethernet

Connection Type:	Point-to-Point Protocol over Ethernet (PPPoE)
Login User Name (case sensitive):	
Login Password:	

Administrator

MP202's Hostname:	MP202
E-Mail:	

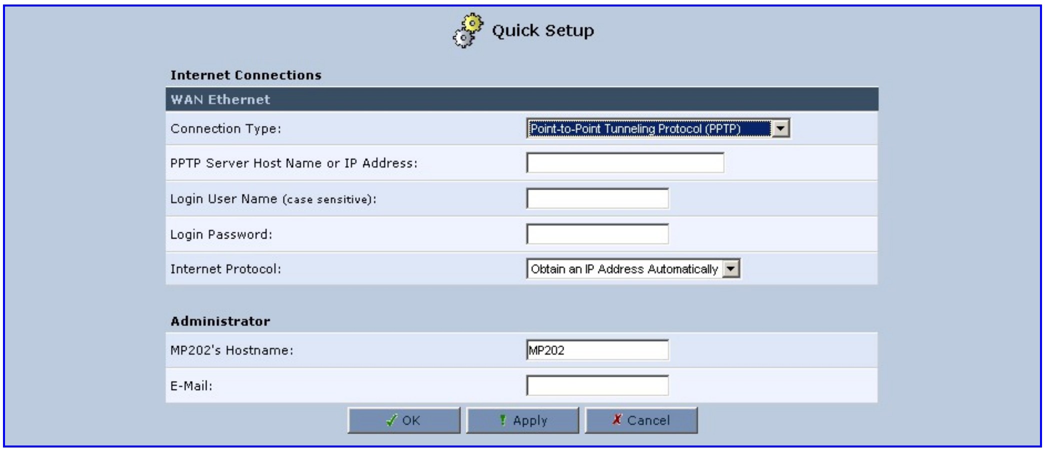
Your ISP should provide you with the following information:

- Login user name
- Login password

3.2.2.1.4 Point-to-Point Tunneling Protocol (PPTP)

- Select 'Point-to-Point Tunneling Protocol (PPTP)' from the 'Connection Type' drop-down list (refer to the figure).

Figure 3-8: Internet Connection - Point-to-Point Tunneling Protocol



Quick Setup

Internet Connections

WAN Ethernet

Connection Type:	Point-to-Point Tunneling Protocol (PPTP)
PPTP Server Host Name or IP Address:	
Login User Name (case sensitive):	
Login Password:	
Internet Protocol:	Obtain an IP Address Automatically

Administrator

MP202's Hostname:	MP202
E-Mail:	

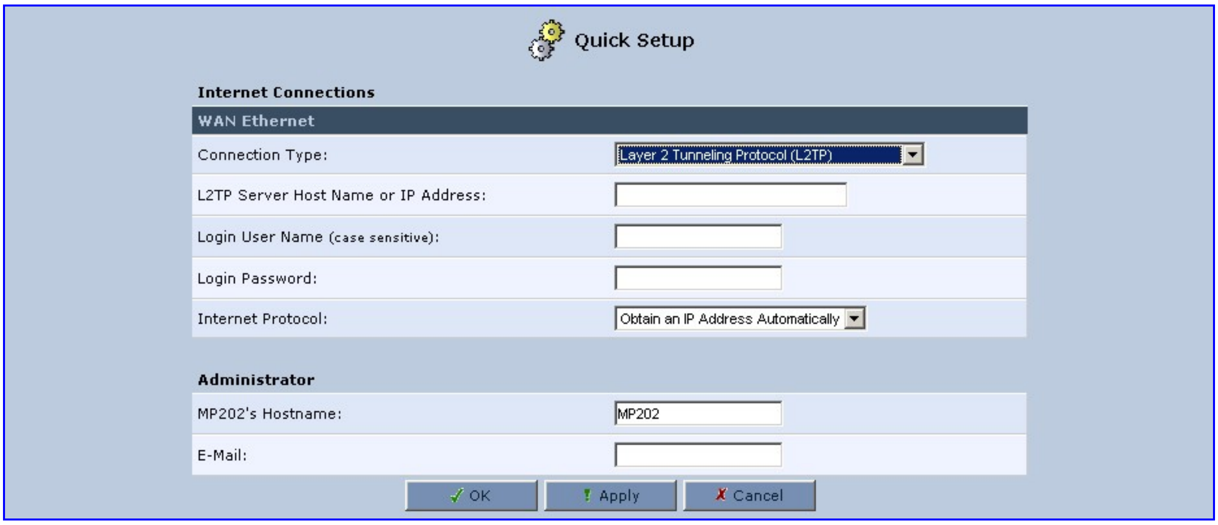
Your ISP should provide you with the following information:

- PPTP Server Host Name or IP Address
- Login user name
- Login password

3.2.2.1.5 Layer 2 Tunneling Protocol (L2TP)

- Select 'Layer 2 Tunneling Protocol (L2TP)' from the 'Connection Type' drop-down list (refer to the figure).

Figure 3-9: Layer 2 Tunneling Protocol



Quick Setup

Internet Connections

WAN Ethernet

Connection Type:	Layer 2 Tunneling Protocol (L2TP)
L2TP Server Host Name or IP Address:	
Login User Name (case sensitive):	
Login Password:	
Internet Protocol:	Obtain an IP Address Automatically

Administrator

MP202's Hostname:	MP202
E-Mail:	

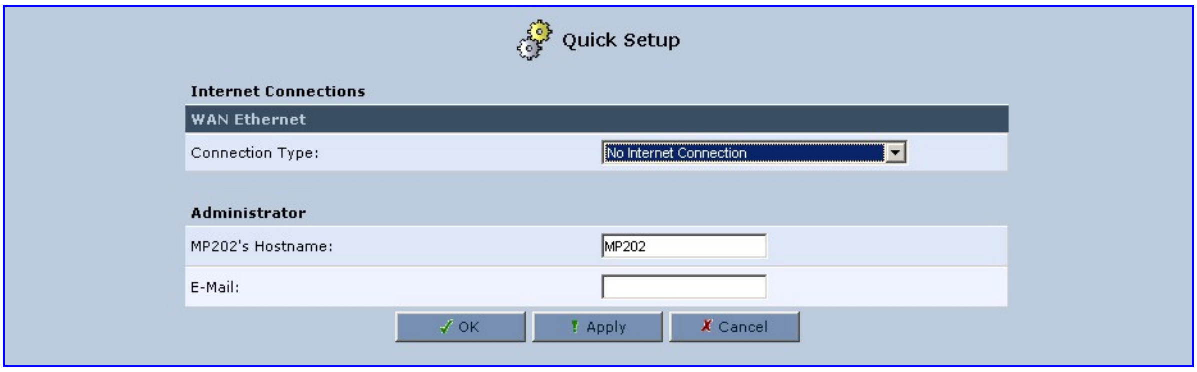
Your ISP should provide you with the following information:

- L2TP Server Host Name or IP Address
- Login user name
- Login password

3.2.2.1.6 No Internet Connection

- Select 'No Internet Connection' from the 'Connection Type' combo-box (refer to the figure). Choose this connection type if you do not have an Internet connection, or if you want to disable all existing connections.

Figure 3-10: Internet Connection - No Internet Connection



Quick Setup

Internet Connections

WAN Ethernet

Connection Type:	No Internet Connection

Administrator

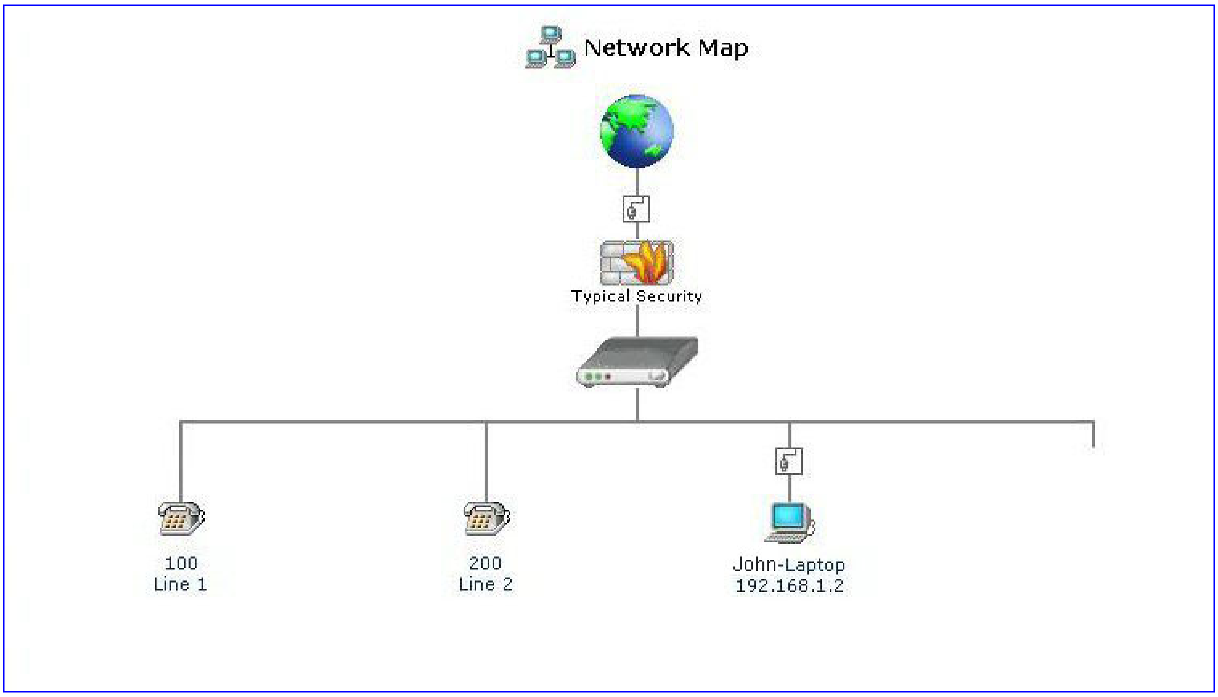
MP202's Hostname:	MP202
E-Mail:	

4 Using the MP-202's Web Interface

4.1 Your Home Network Map

When you log into the Web-based management, you'll view the Network Map.

Figure 4-1: Network Map



The network map depicts the various network elements from top going down:

1. External network interface (Internet connection)
2. Firewall
3. MP-202
4. Telephones connected to the MP-202
5. Local network computers and peripherals (the figure above shows a network element that obtained its IP address automatically via the MP-202's DHCP server).

The table below explains the meaning of different network map symbols:

Table 4-1: Network Map Symbols

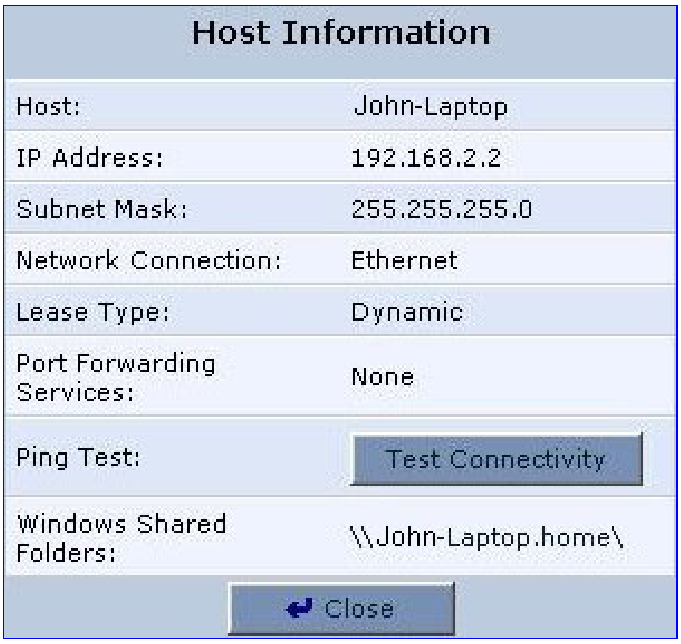
🌐	Represents the Internet
	Represents your Ethernet Wide Area Network (WAN) connection. Click this icon to configure the WAN interface.
🔥	Represents the Telephone Adapter's Firewall. The height of the wall corresponds to the security level currently selected: Minimum, Typical or Maximum. Click this icon to configure security settings.

If the MP-202 is equipped with multiple LAN devices (other than bridges) then the home network will use the following icons to indicate the interface used for connecting the PC.

Table 4-2: Icons to Indicate the Interface Used for Connecting the PC

	Represents an Ethernet Local Area Network (LAN) connection. Click this icon to configure network parameters for the Ethernet LAN device.
	Represents a bridge connected in the home network. Click this icon to view the bridge's underlying devices.
💻	Represents a computer (host) connected in the home network. Each computer connected to the network appears below the network symbol of the network through which it is connected. Click an icon to view network information for the corresponding computer.

Figure 4-2: Host Information



Host Information

Host:	John-Laptop
IP Address:	192.168.2.2
Subnet Mask:	255.255.255.0
Network Connection:	Ethernet
Lease Type:	Dynamic
Port Forwarding Services:	None
Ping Test:	Test Connectivity
Windows Shared Folders:	\\John-Laptop.home\

4.2 Web Interface Left Sidebar Icons

The Web-based management screens have been grouped into several subject areas and may be accessed by clicking on the appropriate icon in the left side-bar. The subject areas are:

Table 4-3: Icons Indicating Web-Based Management Screens' Subject Areas

Home	Display the Network Map
Quick Setup	Quickly configure your MP-202.
Network Connections	Create and configure networks connections.
Security	Configure the Firewall and regulate communications between the Internet and the home network.
VoIP	Use the MP-202's Voice over IP to place and receive calls over the Internet using a standard telephone set.
Quality of Service (QoS)	Configure QoS parameters for the gateway.
Advanced	Control system parameters (DHCP server, DNS) and perform administrative functions, including changing password, setting date & time and upgrading the system.
Monitoring	View network status, traffic statistics, the system log and the VoIP status.
Logout	Logout: Log out from the MP-202

4.3 Navigational Aids

The black navigator bar, located at the top of the Web-based management, provides an easy way to locate the current screen in the hierarchy of Web-based management screens. You may use it to quickly return to a screen that is 'above' the current screen.

The icons listed below make it easy to quickly jump to key information about your home network. They are located on the right side of the Web-based management.

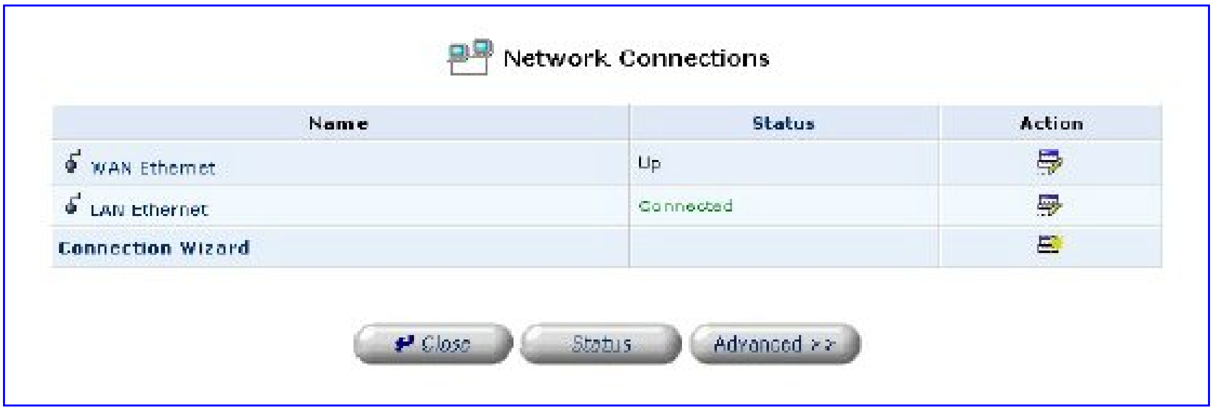
Table 4-4: Icons to Quickly Jump to Key Information About Your Home Network

⊞	Return to the 'Network Map'
☰	View a list of computers in the home network and the connection status of each. Also listed is the status of the Internet connection and each of the LAN connections. Printers or disks connected to the MP-202 are shown as well.
?	View technical information about the system that you are running, including version number and contact information.

4.4 Managing Tables

Tables are structures used throughout the Web-based Management. They handle user-defined entries relating to elements such as network connections, local servers, restrictions and configurable parameters. The principles outlined in this section apply to all tables in the Web-based Management.

Figure 4-3: Typical Table Structure



Network Connections

Name	Status	Action
WAN Ethernet	Up	✎
LAN Ethernet	Connected	✎
Connection Wizard		✱

The figure illustrates a typical table. Each row denotes an entry in the table. The following buttons located in the 'Action' column enable adding, editing and deleting table entries:

Table 4-5: Managing Tables

✱	Use the Add button to add a row to the table.
✎	Use the Edit button to edit a row from the table.
✗	Use the Delete button to remove a row from the table.

In many tables, the last row includes a button that allows adding a new row to the table.

5 Configuring VoIP Parameters

5.1 Voice over IP Screen

Open the 'Voice over IP' screen by clicking the button 'Voice over IP' on the menu bar to the left; the Voice over IP' screen opens showing the tabs that allow:

- "Configuring Signaling Protocol Parameters" on page 32
- "Configuring Dialing Parameters" on page 39
- "Configuring Media Streaming Parameters" on page 41
- "Configuring Voice and Fax Parameters" on page 44
- "Configuring Services Parameters" on page 47
- "Configuring Line Settings Screen" on page 49
- "Configuring Speed Dial Settings" on page 50
- "Configuring Telephone Interfaces" on page 53

Note: Clicking the button 'Advanced' in the Voice over IP screens enables configuration of advanced VoIP parameters.

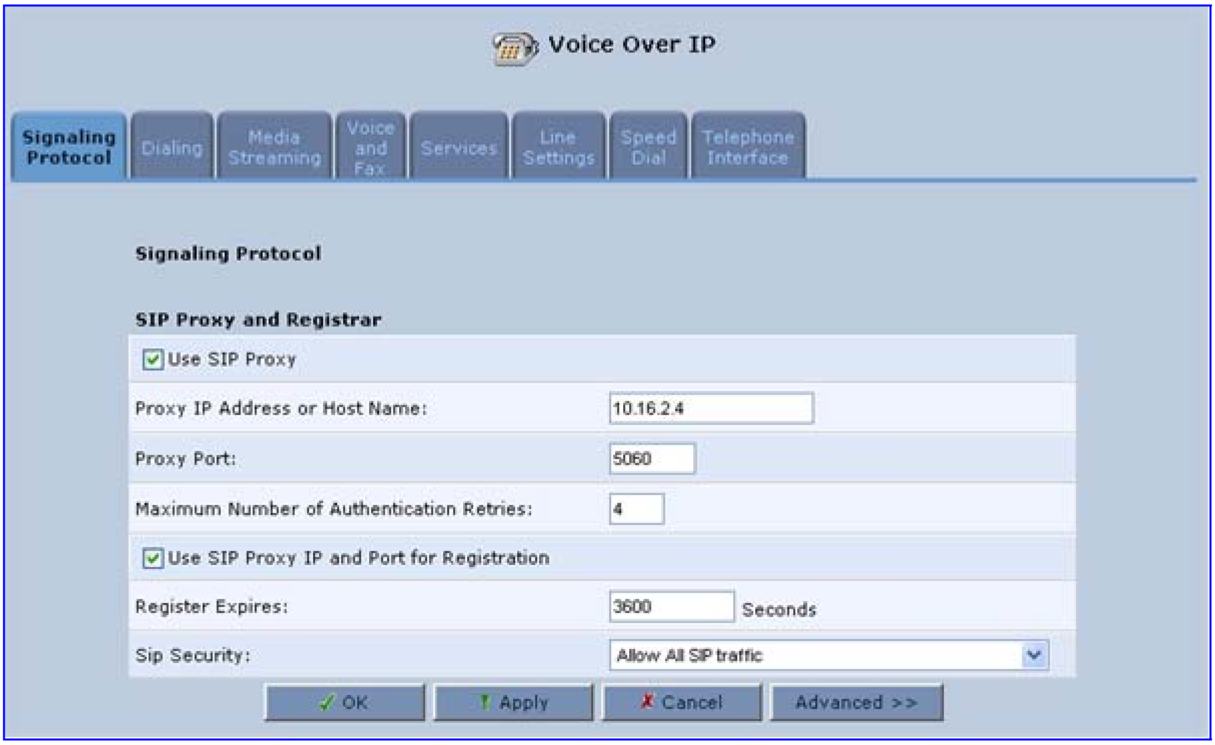
5.1.1 Configuring Signaling Protocol Parameters

Note: In the current version release, only SIP (Session Initiation Protocol) is supported.

➢ To configure signaling protocol parameters:

- After clicking the menu 'Voice over IP' in the main screen, the 'Signaling Protocol' screen opens by default (refer to the figure below).

Figure 5-1: VoIP - Signaling Protocol



Signaling Protocol

SIP Proxy and Registrar

☑ Use SIP Proxy

Proxy IP Address or Host Name: 10.16.2.4

Proxy Port: 5060

Maximum Number of Authentication Retries: 4

☑ Use SIP Proxy IP and Port for Registration

Register Expires: 3600 Seconds

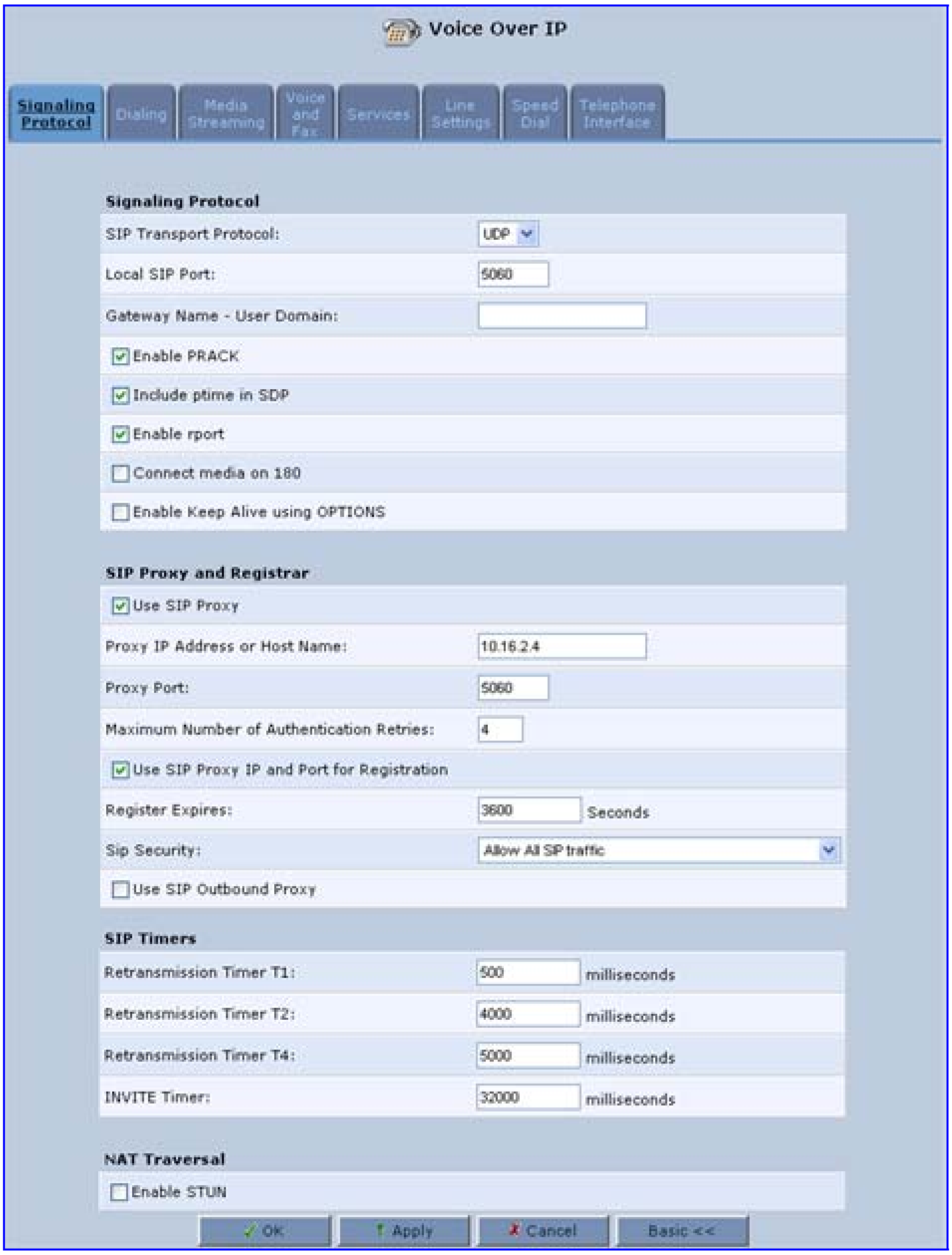
Sip Security: Allow All SIP traffic

Table 5-1: VoIP - Signaling Protocol

Parameter	Description
Use SIP Proxy	When checked, outgoing calls will be routed to the configured SIP proxy. If the parameter 'Use SIP Proxy IP and Port for Registration' is checked as well, the configured SIP proxy will also be used as the registrar, allowing incoming calls.
Use SIP Registrar	Check to use a separate SIP registrar server. Default is unchecked.

- Check the checkbox 'Use SIP Proxy'; the 'SIP Proxy' screen (showing basic parameters) opens. Click the button 'Advanced>>'; the 'SIP Proxy' screen (showing the advanced parameters, including the basic parameters) opens.

Figure 5-2: VoIP - Signaling Protocol - SIP Proxy and Registrar



Signaling Protocol

SIP Transport Protocol:	UDP
Local SIP Port:	5060
Gateway Name - User Domain:	
☑ Enable PRACK	
☑ Include ptime in SDP	
☑ Enable rport	
☐ Connect media on 180	
☐ Enable Keep Alive using OPTIONS	

SIP Proxy and Registrar

☑ Use SIP Proxy	
Proxy IP Address or Host Name:	10.16.2.4
Proxy Port:	5060
Maximum Number of Authentication Retries:	4
☑ Use SIP Proxy IP and Port for Registration	
Register Expires:	3600 Seconds
Sip Security:	Allow All SIP traffic
☐ Use SIP Outbound Proxy	

SIP Timers

Retransmission Timer T1:	500 milliseconds
Retransmission Timer T2:	4000 milliseconds
Retransmission Timer T4:	5000 milliseconds
INVITE Timer:	32000 milliseconds

NAT Traversal

☐ Enable STUN

Table 5-2: VoIP - Signaling Protocol - Signaling Protocol

Parameter	Description
SIP Transport Protocol*	Choose either UDP (default) or TCP.
Local SIP Port*	The UDP/TCP port (default = 5060) on which the Stack listens.
Gateway Name-User Domain*	This domain name will be sent in the From header of outgoing Invite messages.
Enable PRACK*	When enabled, the MP-202 replies with a PRACK message upon receipt of a reliable provisional response. The MP-202 does not initiate reliable provisional responses.
Include ptime in SDP*	When enabled, the MP-202 adds the ptime field to the SDP message body.
Enable rport*	When enabled, the MP-202 adds the rport parameter to the relevant SIP Message fields.
Connect media on 180*	When enabled, media is connected upon receipt of SIP 180, 183, or 200 messages. When the parameter is disabled, media is connected upon receipt of 183 and 200 messages only.
Enable Keep Alive using OPTIONS*	When enabled, a SIP OPTIONS message is sent periodically to the SIP registrar entity.
Keep alive period**	Sets the periodic interval.

* This parameter appears only in 'Advanced' mode.

* * This parameter appears only in 'Advanced' mode and when “Enable Keep Alive using OPTIONS” is enabled.

Table 5-3: VoIP - Signaling Protocol - SIP Proxy and Registrar

Parameter	Description
Use SIP Proxy	When checked, outgoing calls will be routed to the configured SIP proxy. If the parameter 'Use SIP Proxy IP and Port for Registration' is checked as well, the configured SIP proxy will also be used as the registrar, allowing incoming calls.
Proxy IP Address or Host Name	The IP address or host name of the SIP proxy.
Proxy Port	The UDP or TCP port of the SIP proxy.
Maximum Number of Authentication Retries	Defines how many times authenticated register messages are re-sent if 401 or 407 responses with a different “nonce” are received.
SIP Security	The MP-202's firewall can be configured to block incoming packets that have the SIP signaling port as their destination. You can configure up to two SIP entities (for example, the SIP Proxy or an SBC), which are not to be blocked by the firewall. The default value is “Allow all SIP traffic”.
Address Type**	Defines the address type of the additional SIP entity. It can be set to “IP Address” or “Host Name”.
SIP Entity Address**	The address of the additional SIP entity.

Parameter	Description
Use SIP Proxy IP and Port for Registration	Use the SIP proxy IP and port for registration. Default = checked. When checked, there is no need to configure the address of the registrar separately.
Use SIP Outbound Proxy*	Use an outbound SIP proxy (all SIP messages will be sent to this server as the first hop). Default = unchecked.

* This parameter appears only in 'Advanced' mode.

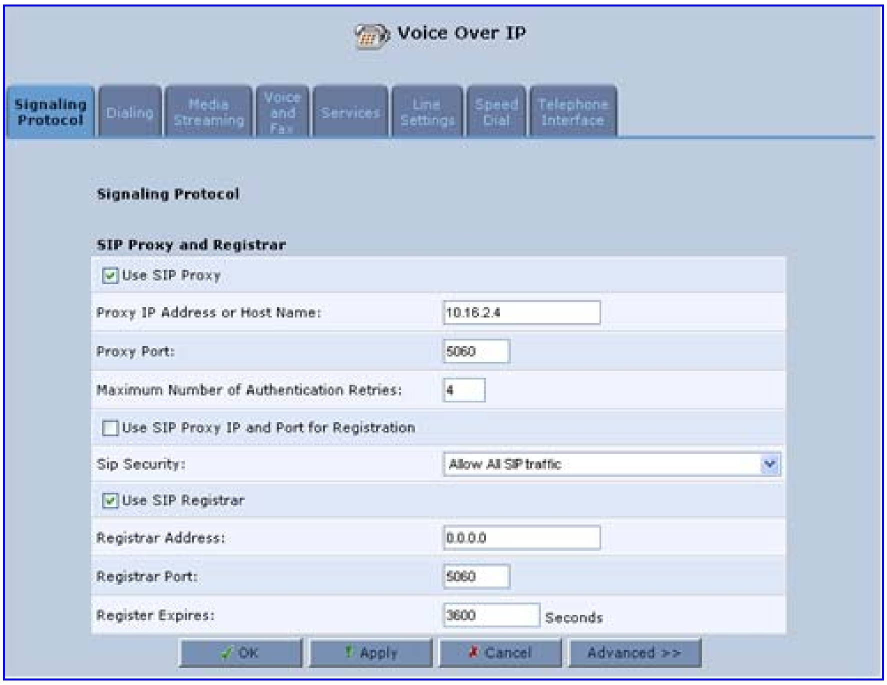
** This parameter appears only if the parameter 'SIP Security' is set to “Allow SIP traffic from Proxy and Additional SIP Entity”.

Table 5-4: VoIP - Signaling Protocol - SIP Timers

Parameter	Description
Retransmission Timer T1	The SIP T1 retransmission timer according to RFC 3261
Retransmission Timer T2	The SIP T2 retransmission timer according to RFC 3261
Retransmission Timer T4	The SIP T4 retransmission timer according to RFC 3261
INVITE Timer	The SIP INVITE timer according to RFC 3261

- Uncheck the box 'Use SIP Proxy IP and Port for Registration' and check 'Use SIP Registrar'; the parameters screen for 'SIP Registrar' opens (showing the basic parameters).

Figure 5-3: VoIP - Signaling Protocol - SIP Proxy and Registrar



Signaling Protocol

SIP Proxy and Registrar

☑ Use SIP Proxy

Proxy IP Address or Host Name: 10.16.2.4

Proxy Port: 5060

Maximum Number of Authentication Retries: 4

☐ Use SIP Proxy IP and Port for Registration

Sip Security: Allow All SIP traffic

☑ Use SIP Registrar

Registrar Address: 0.0.0.0

Registrar Port: 5060

Register Expires: 3600 Seconds

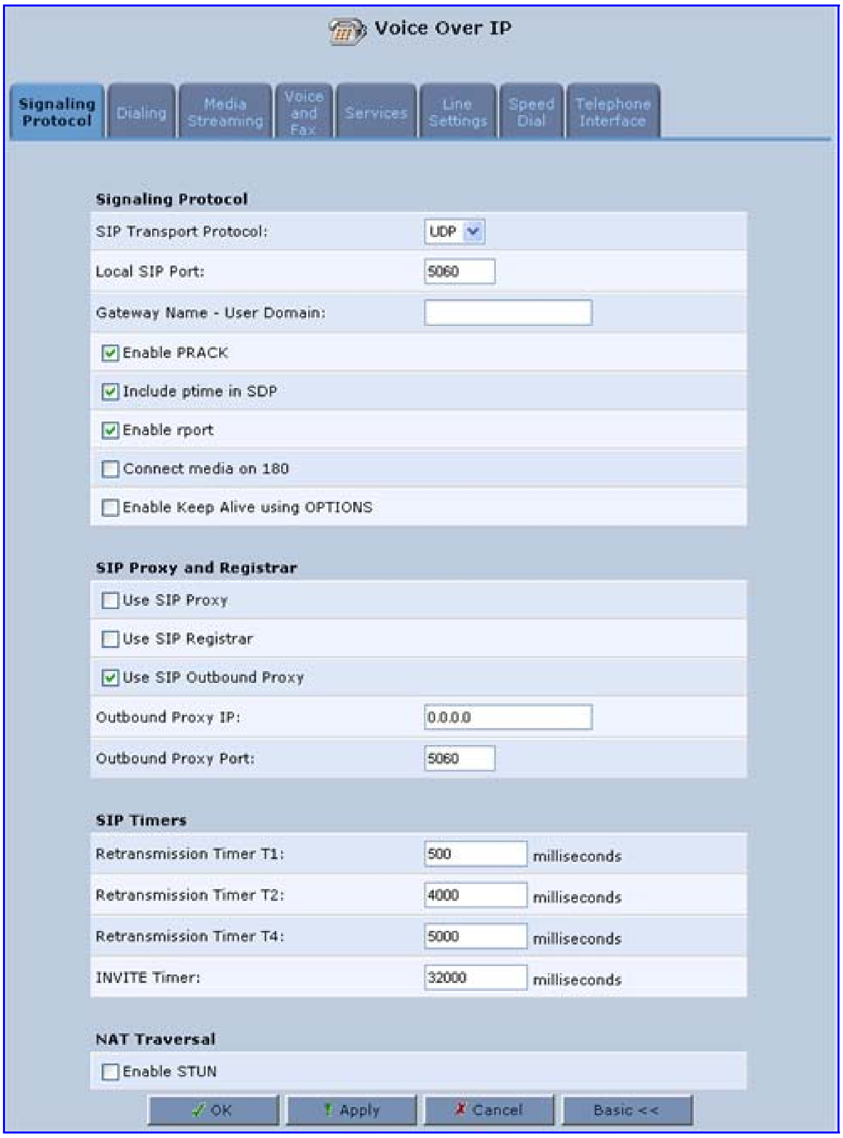
The table below shows descriptions of those SIP Registrar parameters that differ from SIP Proxy parameters. Descriptions of common parameters can be seen under the section 'SIP Proxy and Registrar', above.

Table 5-5: VoIP - Signaling Protocol - SIP Registrar SIP

Parameter	Description
Use SIP Registrar	Check the box to use a separate SIP registrar server.
Registrar Address	The IP address or host name of the registrar server.
Registrar Port	The UDP or TCP port of the registrar server.
Registrar Expires	The registration timeout, in seconds.

Click the button 'Advanced', and then check the box 'Use SIP Outbound Proxy'; the parameters screen for 'SIP Outbound Proxy' opens (showing the advanced parameters, including the basic parameters).

Figure 5-4: VoIP - Signaling Protocol - SIP Outbound Proxy



Signaling Protocol

SIP Transport Protocol: UDP

Local SIP Port: 5060

Gateway Name - User Domain:

☑ Enable PRACK

☑ Include ptime in SDP

☑ Enable rport

□ Connect media on 180

□ Enable Keep Alive using OPTIONS

SIP Proxy and Registrar

□ Use SIP Proxy

□ Use SIP Registrar

☑ Use SIP Outbound Proxy

Outbound Proxy IP: 0.0.0.0

Outbound Proxy Port: 5060

SIP Timers

Retransmission Timer T1: 500 milliseconds

Retransmission Timer T2: 4000 milliseconds

Retransmission Timer T4: 5000 milliseconds

INVITE Timer: 32000 milliseconds

NAT Traversal

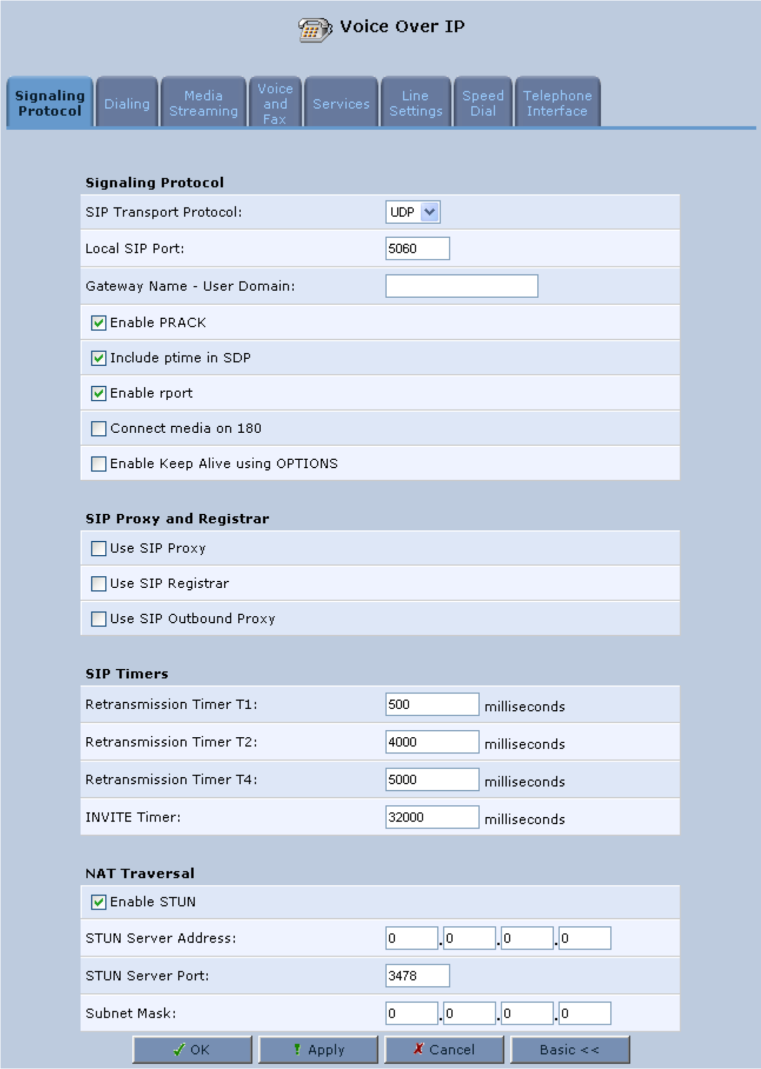
□ Enable STUN

Table 5-6: VoIP - Signaling Protocol - SIP Outbound Proxy

Parameter	**Description**
Outbound Proxy IP	The IP address of the outbound Proxy. If this parameter is set, all outgoing messages (including Registration messages) will be sent to this Proxy according to the Stack behavior.
Outbound Proxy Port	The Port on which the outbound Proxy listens.

Click the button 'Advanced', and then check the box 'Enable STUN'; the parameters screen for 'NAT Traversal' opens (showing the advanced parameters, including the basic parameters).

Figure 5-5: VoIP - Signaling Protocol - NAT Traversal



Signaling Protocol

SIP Transport Protocol: UDP

Local SIP Port: 5060

Gateway Name - User Domain:

☑ Enable PRACK

☑ Include ptime in SDP

☑ Enable rport

☐ Connect media on 180

☐ Enable Keep Alive using OPTIONS

SIP Proxy and Registrar

☐ Use SIP Proxy

☐ Use SIP Registrar

☐ Use SIP Outbound Proxy

SIP Timers

Retransmission Timer T1: 500 milliseconds

Retransmission Timer T2: 4000 milliseconds

Retransmission Timer T4: 5000 milliseconds

INVITE Timer: 32000 milliseconds

NAT Traversal

☑ Enable STUN

STUN Server Address: 0 . 0 . 0 . 0

STUN Server Port: 3478

Subnet Mask: 0 . 0 . 0 . 0

Table 5-7: VoIP - Signaling Protocol - NAT Traversal

Parameter	**Description**
Enable STUN	When checked, the SIP STUN Manager starts. SIP STUN Manager resolves private addresses that need to be resolved to public addresses.
STUN Server Address*	The IP address of the STUN server used to resolve private addresses.
STUN Server Port*	The port of the STUN server.
Subnet Mask*	The subnet mask address of the STUN server used to resolve private addresses.

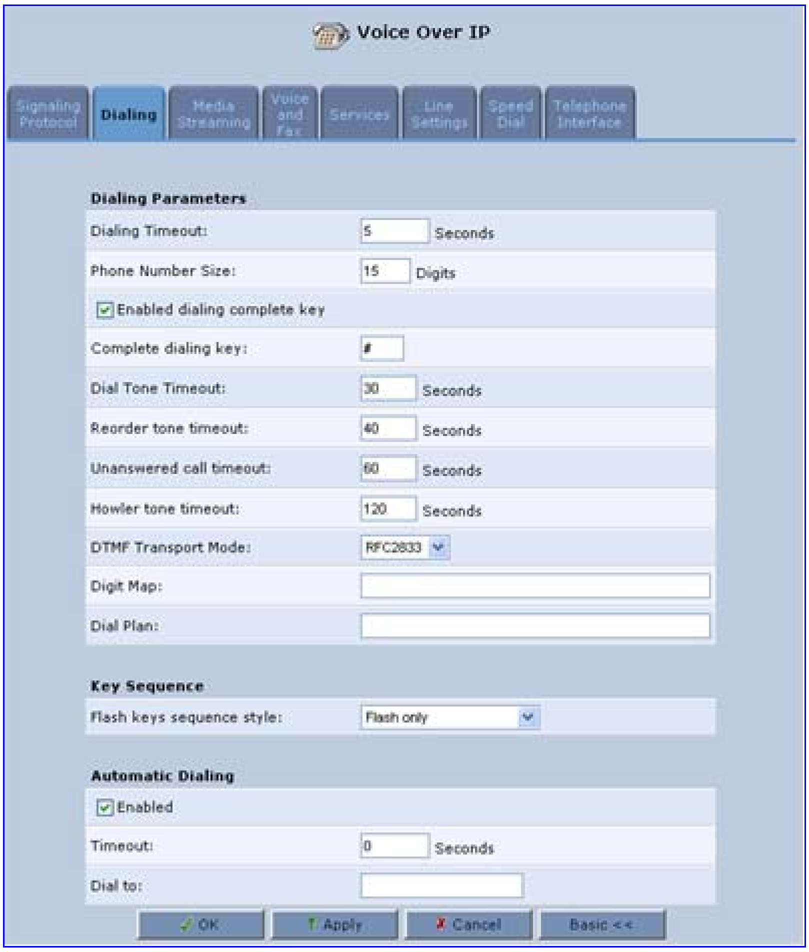
* This parameter appears only if 'Enable STUN' is checked.

5.1.2 Configuring Dialing Parameters

➢ To configure Dialing parameters:

- Click tab 'Dialing'; the 'Dialing Parameters' screen opens.
- Click the button 'Advanced>>'; the advanced Dialing Parameters screen opens.

Figure 5-6: VoIP - Dialing



Dialing Parameters

Dialing Timeout:	5 Seconds
Phone Number Size:	15 Digits
☑ Enabled dialing complete key	
Complete dialing key:	#
Dial Tone Timeout:	30 Seconds
Reorder tone timeout:	40 Seconds
Unanswered call timeout:	60 Seconds
Howler tone timeout:	120 Seconds
DTMF Transport Mode:	RFC2833
Digit Map:	
Dial Plan:	

Key Sequence

Flash keys sequence style:	Flash only

Automatic Dialing

☑ Enabled	
Timeout:	0 Seconds
Dial to:	

Table 5-8: VoIP - Dialing Parameters

Parameter	Description
Dialing Timeout	Dialing timeout specifies the duration (in seconds) of allowed inactivity between dialed digits. When you work with a proxy or gatekeeper, the number you have dialed before the dialing process has timed out is sent to the proxy/gatekeeper as the user ID to be called. This is useful for calling a remote party without creating a speed dial entry (assuming the remote party is registered with the proxy/gatekeeper).

Parameter	Description
Phone Number Size	The maximum length of shortcut numbers that you can enter and the maximum number of digits that you can dial.
Enabled dialing complete key*	When checked, a specific key can be defined for the Complete Dialing key. Pressing the Dialing complete key forces the MP-202 to make a call to the dialed digits even if there is no match in the dial plan or digit map. The default value is enabled.
Complete Dialing Key*	Defines the Complete Dialing key. The default value is the pound (#) key.
Dial Tone Timeout	The duration of the dial tone, in seconds. If the limit is exceeded, the dial tone will stop and you will hear a Reorder tone.
Reorder Tone Timeout*	The duration (in seconds) of the Reorder tone. The Reorder tone is played for example, when the MP-202 receives a 486 Response. If the limit is exceeded, the Reorder tone stops and a Howler tone is played to the user.
Unanswered Call Timeout*	Timeout before the MP-202 automatically sends a Cancel message. When the MP-202 makes a call and the other side doesn't answer, the MP-202 sends a Cancel after this timeout.
Howler Tone Timeout*	The duration (in seconds) of the Howler tone. If the limit is exceeded, the Howler tone stops. The Howler tone informs a user that the user's phone has been left in an off-hook state.
DTMF Transport Mode*	DTMFs are the tones generated by your telephone's keypad. Choose either Inband, RFC 2833, or Via SIP.
Digit Map*	Enables the ISP to predefine possible formats (or patterns) for the dialed number. A match to one of the defined patterns terminates the dialed number. An 'x' in the pattern indicates any digit. ';' separates between patterns. Example: '10x;05xxxxxxxx;4xxx'. In this example, 3 patterns are defined. A number that starts with 10 will be terminated after the 3rd digit and so on. If the user dials a number that does not match any pattern, the number will be terminated using the timeout or when the user presses the pound ('#') key.
Dial Plan*	This parameter works in conjunction with the Digit Map and enables translation of specific patterns to specific SIP destination addresses. An 'x' represents any dialed digit. Each backslash at the right side of the '=' represents one of the dialed digits. Example: '4xxx=Line_\\\@10.1.2.3' This rule will issue a call to 10.1.2.3 with the SIP ID of Line_ followed by the last 3 digits of the dialed number. Rules are separated by the character';'

Parameter	Description
Key Sequence*	Choose either 'Flash only' (default) or ‘Flash + digits sequence’. ‘Flash only’ uses only the phone's Flash button. There are 3 scenarios: (1) During an existing call, if the user presses Flash, the call is put on hold; a dial tone is heard and the user is able to initiate a second call. Once the second call is established, on-hooking transfers the first (held) call to the second call. (2) During an existing call, if the user presses Flash, the call is put on hold and a dial tone is heard. The user can initiate a second call and establish a 3-way conference by again pressing Flash after the second call is initiated. (3) During an existing call, if a call comes in (call waiting), pressing Flash puts the active call on hold and answers the waiting call; pressing Flash again toggles between these two calls. ‘Flash + digits sequence’ is where a sequence of Flash + 1 holds a call or toggles between two existing calls. Flash + 2 makes a call transfer. Flash + 3 establishes a 3-way conference.
Automatic Dialing Enabled*	Enables automatic dialing when the user picks up (i.e., off-hooks) the phone.
Timeout**	Timeout before automatic dialing occurs. When set to 0, automatic dialing is performed immediately.
Dial To**	The automatic dialing destination.

* This parameter appears only in 'Advanced' mode.

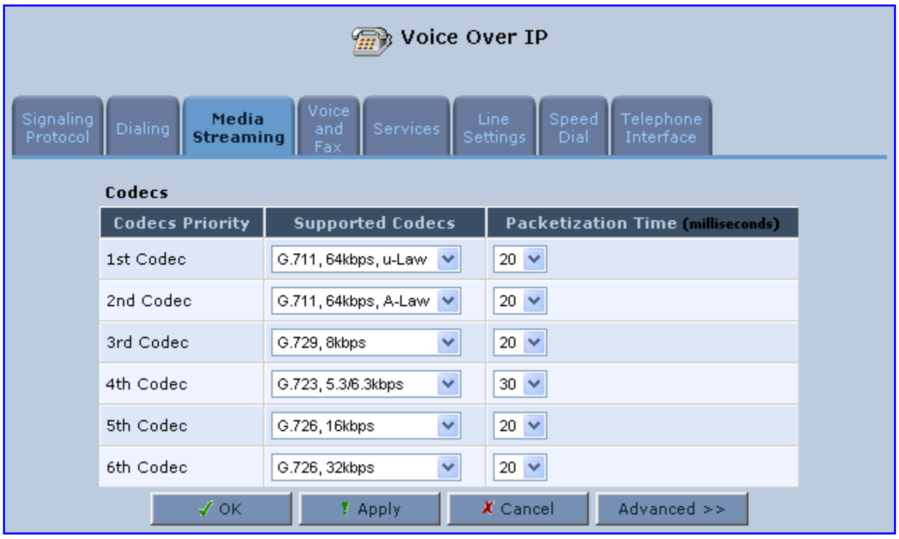
** This parameter appears only when Automatic Dialing is enabled.

5.1.3 Configuring Media Streaming Parameters

➢ **To configure Media Streaming parameters:**

- Click tab 'Media Streaming'; the 'Media Streaming' screen opens.

Figure 5-7: VoIP - Media Streaming - Basic



Codecs

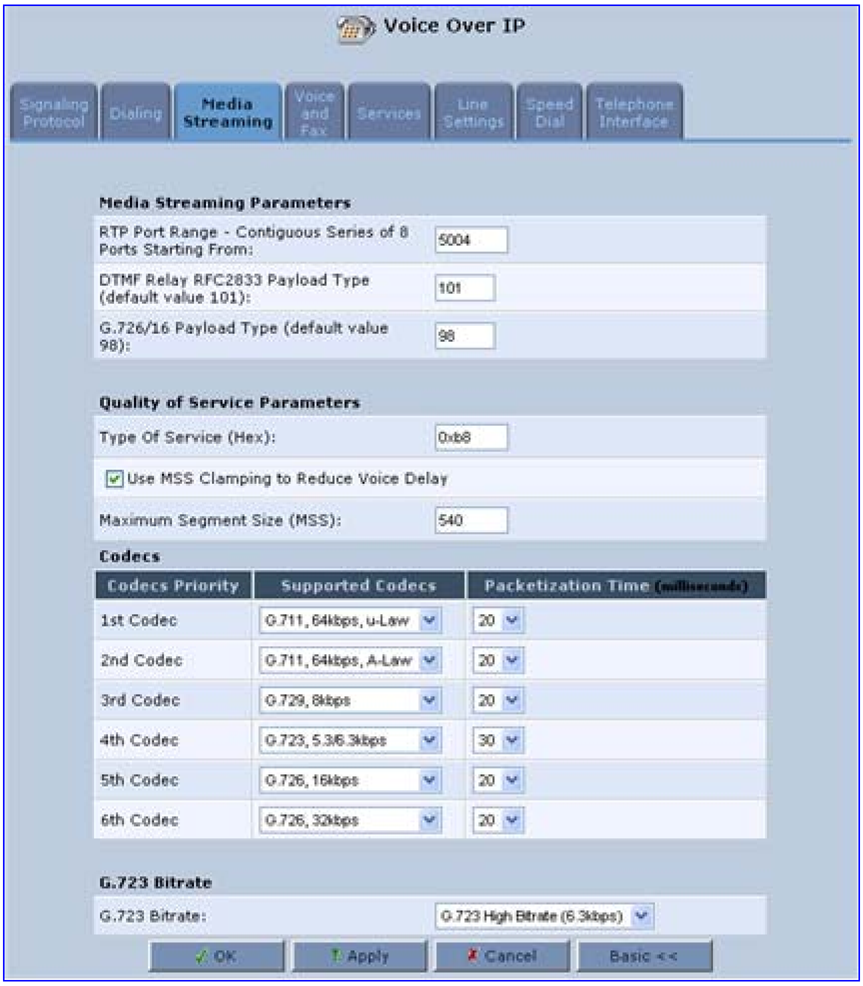
Codecs Priority	Supported Codecs	Packetization Time (milliseconds)
1st Codec	G.711, 64kbps, u-Law	20
2nd Codec	G.711, 64kbps, A-Law	20
3rd Codec	G.729, 8kbps	20
4th Codec	G.723, 5.3/6.3kbps	30
5th Codec	G.726, 16kbps	20
6th Codec	G.726, 32kbps	20

Table 5-9: VoIP - Media Streaming Parameters - Codecs

Parameter	Description
1st Codec	Refer to "Configuring Codecs" on page 43
2nd Codec	Refer to "Configuring Codecs" on page 43
3rd Codec	Refer to "Configuring Codecs" on page 43
4th Codec	Refer to "Configuring Codecs" on page 43
5th Codec	Refer to "Configuring Codecs" on page 43
6th Codec	Refer to "Configuring Codecs" on page 43

- Click the button 'Advanced'; the 'Media Streaming Parameters' and 'Quality of Service Parameters' screen sections open.

Figure 5-8: VoIP - Media Streaming - Advanced



Media Streaming Parameters

RTP Port Range - Contiguous Series of 8 Ports Starting From:	5004
DTMF Relay RFC2833 Payload Type (default value 101):	101
G.726/16 Payload Type (default value 98):	98

Quality of Service Parameters

Type Of Service (Hex):	0xb8
☑ Use MSS Clamping to Reduce Voice Delay	
Maximum Segment Size (MSS):	540

Codecs

Codecs Priority	Supported Codecs	Packetization Time (milliseconds)
1st Codec	G.711, 64kbps, u-Law	20
2nd Codec	G.711, 64kbps, A-Law	20
3rd Codec	G.729, 8kbps	20
4th Codec	G.723, 5.3/6.3kbps	30
5th Codec	G.726, 16kbps	20
6th Codec	G.726, 32kbps	20

G.723 Bitrate

G.723 Bitrate: G.723 High Bitrate (6.3kbps)

Table 5-10: VoIP - Advanced - Media Streaming Parameters

Parameter	Description
RTP Port Range - Contiguous Series of 8 Ports Starting From:	Defines the port range for Real Time Protocol (RTP) voice transport.
DTMF Relay RFC 2833 Payload Type	The RTP payload type used for RFC 2833 DTMF relay packets. Range = 0-255. Default = 101.
G.726/16 Payload Type	The RTP payload type used for 16 kbps G.726 packets. Range = 0-255. Default = 98.

Table 5-11: VoIP - Advanced - Quality of Service Parameters

Parameter	Description
Type of Service (Hex)	This is a part of the IP header that defines the type of routing service to be used to tag outgoing voice packets, originated from the MP-202. It is used to tell routers along the way that this packet should get specific QoS. Leave this value as 0xb8 (default) if you are unfamiliar with the Differentiated Services IP protocol parameter.

Table 5-12: VoIP - Advanced - G.723 Bitrate

Parameter	Description
G.723 Bitrate	Toggles between low and high bit rate for G.723.

5.1.3.1 Configuring Codecs

Codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For example, G.723 is a codec that uses compression, so it is good for use where bandwidth is limited but its voice quality is not as good compared to other codecs such as the G.711.

5.1.3.2 Supported Codecs

To make a call, at least one codec must be enabled. Moreover, all codecs may be enabled for best performance. When you start a call to a remote party, your available codecs are compared against the remote party's, to determine which codec will be used. The priority by which the codecs are compared is according to the descending order of their list, depicted in the figure above. To change the priorities, rearrange the codecs in the required order.

If there is no codec that both parties have made available, the call attempt will fail. Note that if more than one codec is common to both parties, you cannot force which of the common codecs that were found will be used by the remote party's client. If you do wish to force the use of a specific codec, leave only that codec checked.

5.1.3.3 Packetization Time

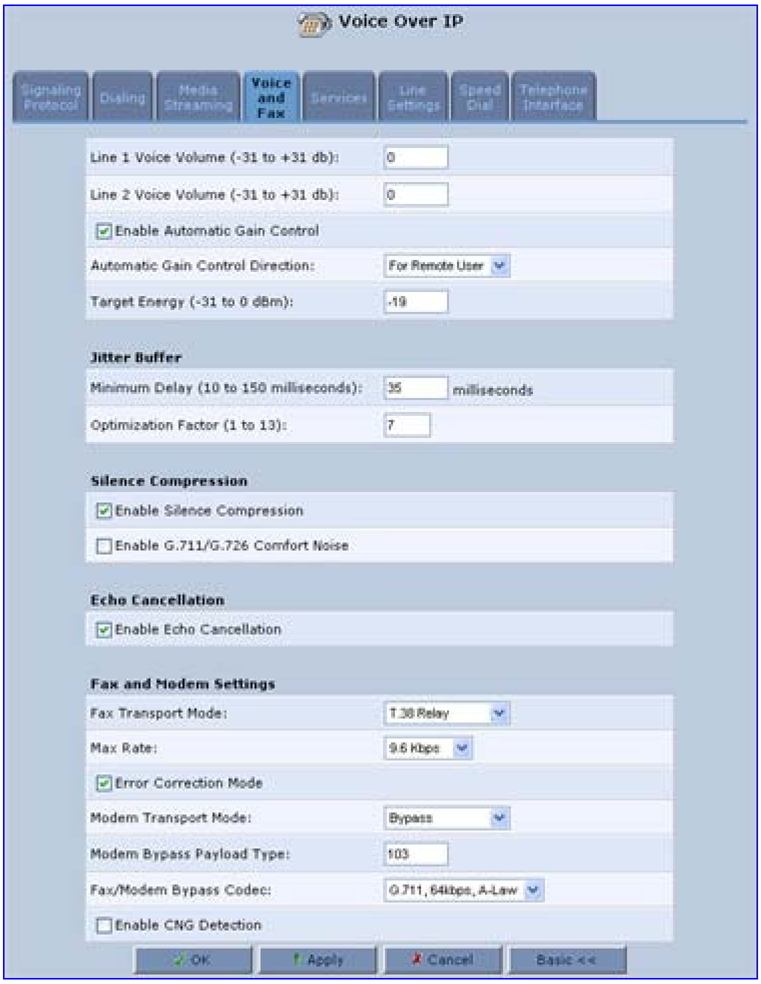
The Packetization Time is the length of the digital voice segment that each packet holds. The default is 20 millisecond packets. Selecting 10 millisecond packets reduces the delay but increases the bandwidth consumption.

5.1.4 Configuring Voice and Fax Parameters

➢ To configure Voice and Fax parameters:

- Click the tab 'Voice and Fax'; the basic 'Voice and Fax' parameters screen opens.
- Click the button 'Advanced'; the extended 'Voice and Fax' parameters screen opens.

Figure 5-9: VoIP - Voice and Fax



Line 1 Voice Volume (-31 to +31 db): 0

Line 2 Voice Volume (-31 to +31 db): 0

☑ Enable Automatic Gain Control

Automatic Gain Control Direction: For Remote User

Target Energy (-31 to 0 dBm): -19

Jitter Buffer

Minimum Delay (10 to 150 milliseconds): 35 milliseconds

Optimization Factor (1 to 13): 7

Silence Compression

☑ Enable Silence Compression

□ Enable G.711/G.726 Comfort Noise

Echo Cancellation

☑ Enable Echo Cancellation

Fax and Modem Settings

Fax Transport Mode: T.38 Relay

Max Rate: 9.6 Kbps

☑ Error Correction Mode

Modem Transport Mode: Bypass

Modem Bypass Payload Type: 103

Fax/Modem Bypass Codec: G.711, 64kbps, A-Law

□ Enable CNG Detection

Table 5-13: VoIP - Voice and Fax

Parameter	Description
Line 1 Voice Volume / Line 2 Voice Volume	The voice volume of line 1 / 2 (the gain from the network towards the local phone). Default = 0 dB.
Enable Automatic Gain Control	When enabled (when the box is checked), the device will adjust the voice volume automatically to compensate for a weak or loud signal.
Automatic Gain Control Direction	Determines whether the AGC is located before the Encoder input or after the Decoder output.
Target Energy	The required output energy of the AGC.
Minimum Delay	The initial and minimal delay of the adaptive jitter buffer mechanism, which compensates for network problems. The value should be set according to the expected average jitter in the network (in msec). Default is 35 msec.
Optimization Factor	The adaptation rate of the jitter buffer mechanism. Higher values will cause the jitter buffer to respond faster to increased network jitter. Default = 7.
Enable Silence Compression	Check to enable silence compression for reducing the network bandwidth consumption. Default = Disabled.
Enable G.711/G.726 Comfort Noise	When the Comfort Noise generation feature is enabled and silence is detected, the device transmits a series of parameters called Silence Information Descriptor (SID), which are used to reproduce the local background noise at the remote (receiving) side.
Enable Echo Cancellation	Check to enable echo cancellation (disabling echo cancellation should be done for testing purposes only). Default = Enabled.
Fax Transport Mode	Selects the way fax calls are handled: Transparent = Fax is transferred in-band (like a voice call) (can be used if the codec is G.711) T.38 Relay = Fax is relayed to the remote side according to the T.38 standard VBD = (Voice Band Data) Switch to G.711 via SIP messaging Bypass = An automatic switch to AudioCodes' proprietary payload type (102, 103).
Max Rate*	The maximum fax rate. Select from the drop-down list either: 2.4 Kbps, 4.8 Kbps, 7.2 Kbps, 9.6 Kbps, 12 Kbps or 14.4 Kbps (default).
Error Correction Mode*	Check to enable fax error correction mode (ECM). Default = Enabled.
Fax Bypass Payload Type**	Defines the payload type for fax in Bypass mode.
Modem Transport Mode	Selects the way modem calls are handled: Transparent = Data is transferred in-band (like a voice call). This can be used if the codec is G.711. VBD = (Voice Band Data) Switch to G.711 via SIP messaging. Bypass = An automatic switch to AudioCodes' proprietary payload type (102, 103). **Note:** If the modem transport mode is Bypass or VBD, it must match the Fax transport mode.

Parameter	Description
Modem Bypass Payload Type* **	Defines the payload type for modems in Bypass mode.
Fax/Modem Bypass Coder	Select the codec to be used for the VBD and Bypass modes. PCMA (default) or PCMU. G.711 64 kbps A-Law -OR-G.711 64 kbps u-Law
Enable CNG Detection	Check to enable detection of the fax CNG signal. When the local fax machine connected to the MP-202 receives a fax, the MP-202 switches to T.38 fax relay upon detection of the CED signal from the remote fax. If the local fax machine sends a fax, the MP-202 switches to T.38 only after detecting the CNG signal from the local side and the CED signal from the remote side. If the "Enable CNG Detection" checkbox is enabled, the MP-202 switches to T.38 relay immediately upon detection of the CNG signal from the local side, without waiting for the CED signal from the remote side. Default = Disabled.

* This parameter appears only if 'Fax Transport Mode' is "T.38 Relay".

** This parameter appears only if 'Fax Transport Mode' is "Bypass".

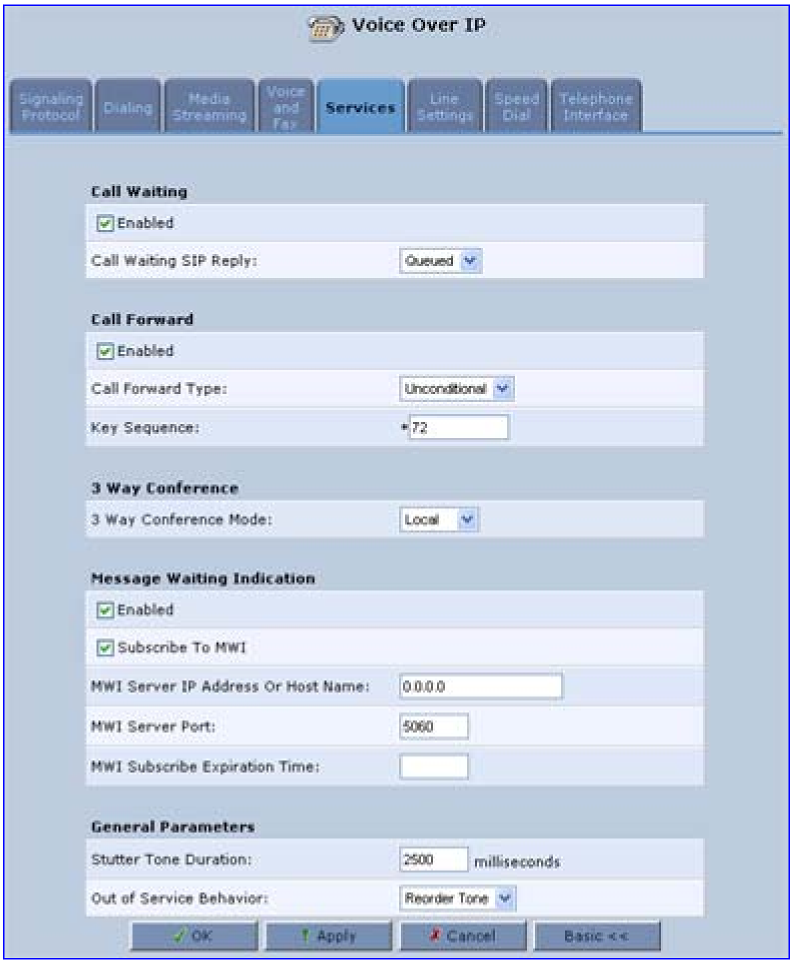
*** This parameter appears only if 'Modem Transport Mode' is "Bypass".

5.1.5 Configuring Services Parameters

➢ To configure Service parameters:

- Click the tab 'Service'; the basic 'Service' parameters screen opens.
- Click the button 'Advanced'; the extended 'Service' parameters screen opens.

Figure 5-10: VoIP - Services - Advanced



Call Waiting

☑ Enabled

Call Waiting SIP Reply: Queued

Call Forward

☑ Enabled

Call Forward Type: Unconditional

Key Sequence: *72

3 Way Conference

3 Way Conference Mode: Local

Message Waiting Indication

☑ Enabled

☑ Subscribe To MWI

MWI Server IP Address Or Host Name: 0.0.0.0

MWI Server Port: 5060

MWI Subscribe Expiration Time:

General Parameters

Stutter Tone Duration: 2500 milliseconds

Out of Service Behavior: Reorder Tone

Table 5-14: VoIP - Services

Parameter	Description
Call Waiting	Call Waiting SIP Reply - Which response message is sent when another call arrives while a call is in progress. There are two possibilities: 180 Ringing or 182 Queued (default). To disable the call waiting feature, select 180 Ringing.
Call Forward Type	The Call Forward feature permits a user to redirect incoming calls addressed to him/her to another number. The user's ability to originate calls is unaffected by Call Forward. Three types of Call Forwarding exist: ▪ Unconditional. When selected, incoming calls are forwarded independently of the status of the endpoint. ▪ Busy. When selected, incoming calls are forwarded only if the endpoint is busy, i.e., if all lines are active. ▪ No Reply. When selected, incoming calls are forwarded only if the endpoint does not answer before a pre-configured timeout (see next parameter).
Time for No Reply Forward	If you specify 5 seconds for this parameter, for example, and 'No Reply' is selected for parameter 'Call Forward Type' (see above), incoming calls are forwarded only after 5 seconds lapse.
Key Sequence	The default is *72 but users can modify to any sequence of up to 2 digits, i.e., *n or *nm.
3 Way Conference Mode	Selects how 3-way conference calls are handled - locally by the device or by a remote media server (RFC 4240).
Media Server Address*	The address of the remote media server that handles conference calls.
Message Waiting Indication	If a user has an unheard voice mail message, a stutter dial tone is heard when the user picks up the phone. In addition, the MP 202 generates an FSK signal to the phone to indicate that a message is waiting. If the telephone connected to the MP-202 supports this feature, an MWI 'envelope icon' is displayed.
Subscribe to MWI	Check this checkbox if you must register with a MWI subscriber server. If so, configure the three parameters below.
MWI Server IP Address or Host Name	The IP address or host name of the MWI server.
MWI Server Port	The port number of the MWI server.
MWI Subscribe Expiration TIme	The interval between registrations.
Stutter Tone Duration	When you enable message waiting and an unheard message exists, you'll hear a stutter tone for the duration configured in this parameter and/or when you activate the call forwarding feature (refer to "Forwarding Calls to Another Phone" on page 59)
Out of Service Behavior	Defines the tone which is played instead of a dial tone if the user configured a registrar IP and the registration failed. When the Reorder tone is selected, a Reorder tone is played instead of a dial tone. If "No Tone" is selected, then no tone is played.

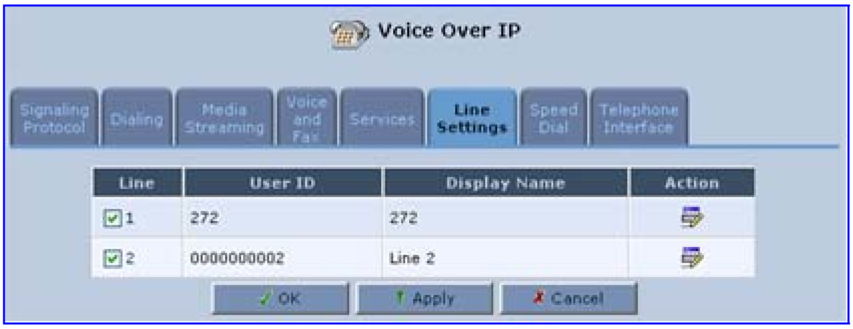
* This parameter appears only if '3 Way Conference Mode' is remote server.

5.1.6 Configuring Line Settings Screen

Before starting to make phone calls, configure each line's parameters.

1. Click the tab 'Line Settings'; the screen that opens (refer to the figure) enables you to define the phone ports of the MP-202 and to configure them.

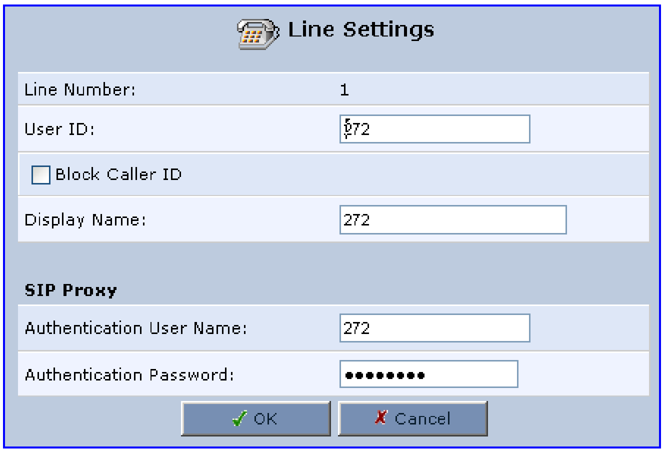
Figure 5-11: VoIP - Line Settings



Line	User ID	Display Name	Action
☑ 1	272	272	
☑ 2	0000000002	Line 2	

2. Click the 'Action' icon in each line to configure the line's different parameters (refer to the figure).

Figure 5-12: VoIP - Line Settings - Defining a New Line



Line Number: 1

User ID: 272

□ Block Caller ID

Display Name: 272

SIP Proxy

Authentication User Name: 272

Authentication Password: ••••••••

Table 5-15: VoIP - Line Settings

Parameter	Description
Line Number	A telephone port in the MP-202 to which you can connect a standard (POTS) telephone. You can manage which telephone is operational by checking the check-box adjacent to it.
User ID	This telephone's VoIP user ID, used for identification to initiate and accept calls.
Block Caller ID	Check this check box to hide your ID from the remote party.

Parameter	Description
Display Name	Used to define a name to intuitively identify the line. A free text description to be displayed to remote parties as your caller ID.
Authentication User Name	The user name received from the VoIP Service Provider. Used when sending a response to Unauthorized or Proxy Authentication Requested (401/407).
Authentication Password	The password received from the VoIP Service Provider. Used when sending a response to Unauthorized or Proxy Authentication Requested (401/407).

5.1.7 Configuring Speed Dial Settings

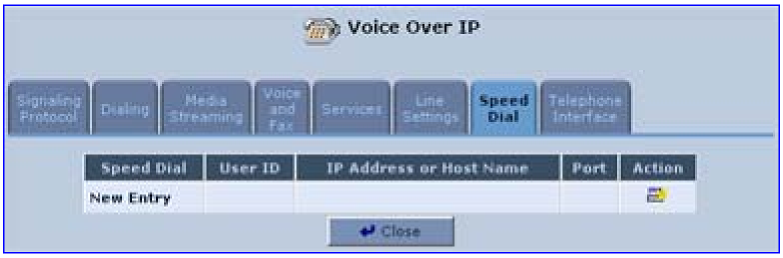
Use the 'Speed Dial Settings' screen to associate a called party's contact parameters (including the IP address of his/her ATA and Line ID) with a number that you'll dial to call him/her. The number of speed-dialing codes that can be defined is unlimited. Use the screen to define a destination type: Proxy, Local Line or Direct Call.

Note that when connecting the MP-202 to a World-Wide SIP Server (refer to" Connecting MP-202's VoIP to a VoIP Service Provider" on page 55), you don't need to configure 'Speed Dial Settings'.

➢ To configure 'Speed Dial' settings:

1. Click tab 'Speed Dial'; the 'Speed Dial' screen opens.

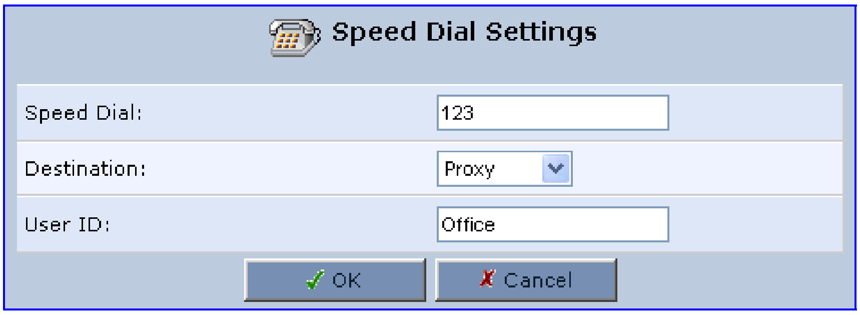
Figure 5-13: VoIP - Speed Dial



Speed Dial	User ID	IP Address or Host Name	Port	Action
New Entry				

Click 'New Entry' to add a new speed dial entry; the 'Speed Dial Settings' screen appears. The figure below shows how a proxy speed dial is configured. The proxy IP address is 'Office' and number to speed-dial is 123.

Figure 5-14: VoIP - Speed Dial Settings



Speed Dial: 123

Destination: Proxy

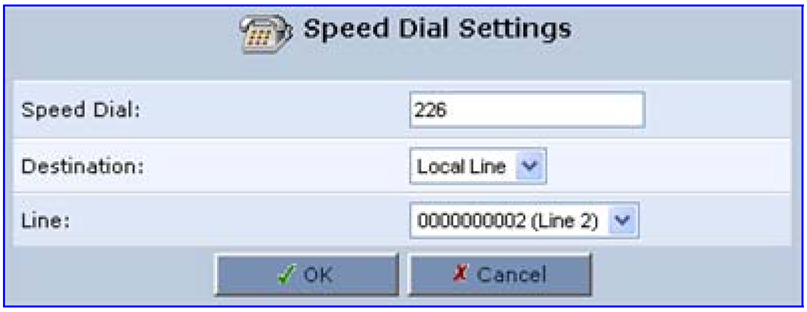
User ID: Office

Table 5-16: 'Speed Dial Settings' - via Proxy

Parameter	Description
Speed Dial	Defines the number to dial.
Destination	Defines the entry's destination, in this case a proxy server.
User ID	Defines the user ID to call.

The figure below shows how a local line speed dial is configured from port ‘Line 2’ on the MP-202 to port ‘Line 1’ on the MP-202. The speed dial number 225 is now associated with Line 1 on the MP-202.

Figure 5-15: VoIP - Speed Dial - Local Line

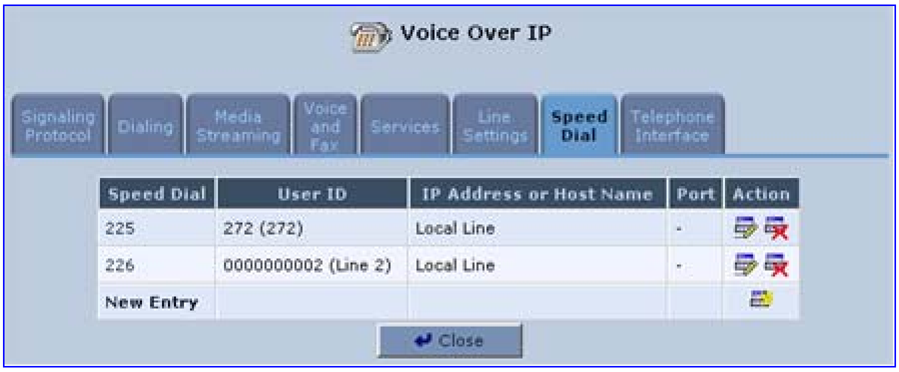


Speed Dial Settings

Speed Dial:	226
Destination:	Local Line
Line:	0000000002 (Line 2)

- Click 'OK'; you're returned to the Voice Over IP' screen displaying the configured speed dial (refer to the figure below, displaying how two local lines are configured for speed dial).

Figure 5-16: VoIP - Speed Dial Settings - Local Line

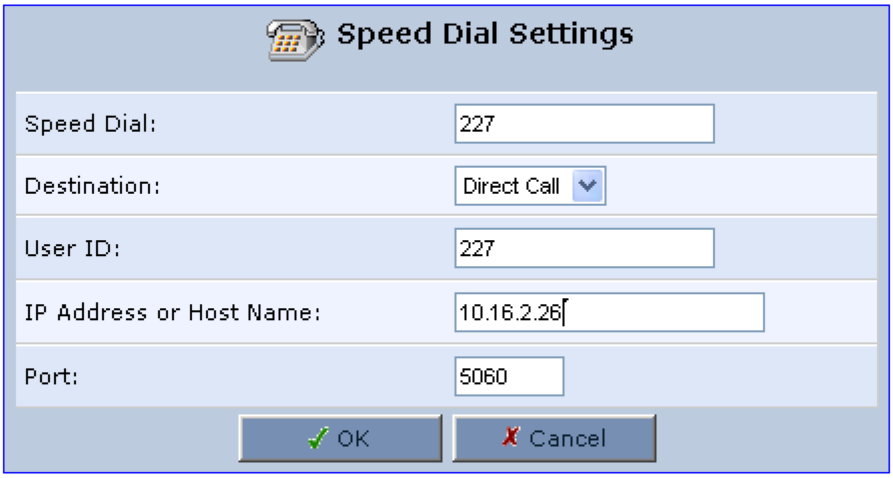


Voice Over IP

Speed Dial	User ID	IP Address or Host Name	Port	Action
225	272 (272)	Local Line	-	
226	0000000002 (Line 2)	Local Line	-	
New Entry				

The figure below shows how a speed dial direct call is configured. The call is configured to one of the pre-configured lines of a remote device (10.16.2.26).

Figure 5-17: VoIP - Speed Dial - Direct Call



Speed Dial Settings

Speed Dial:	227
Destination:	Direct Call
User ID:	227
IP Address or Host Name:	10.16.2.26
Port:	5060

Table 5-17: 'Speed Dial Settings' - Direct Call

Parameter	Description
Speed Dial	A shortcut number which you will dial to call this party.
Destination	The entry's destination, in this case a direct call.
User ID	Specify the remote party's user ID.
IP Address or Host Name	Specify the remote party's IP Address or host name.
Port	The SIP UDP or TCP port of the remote party.

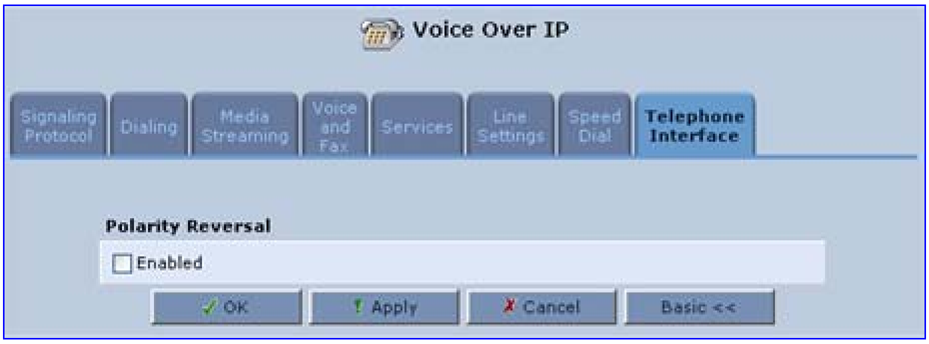
5.1.8 Configuring Telephone Interfaces

Use the 'Telephone Interface' screen to enable and disable FXS (telephone interface) parameters.

➢ To configure "Telephone Interface' settings:

1. Click the tab 'Telephone Interface'; the 'Telephone Interface' screen opens.

Figure 5-18: VoIP - Telephone Interface

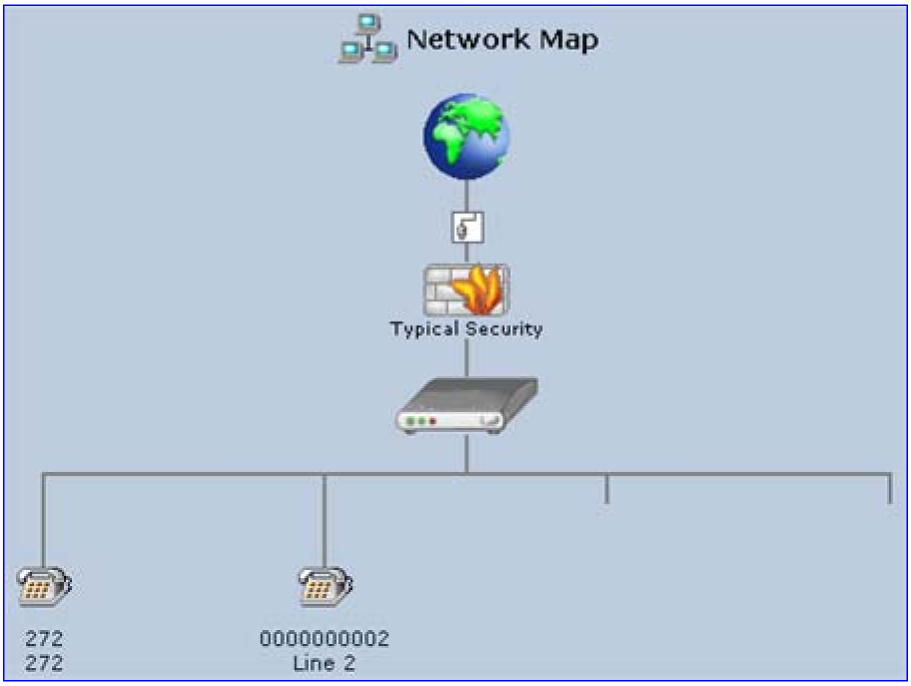


Polarity Reversal

□ Enabled

2. Check the checkbox 'Enabled' to enable the Polarity Reversal feature. When this feature is enabled, the FXS polarity is reversed to indicate the start of a VoIP session, and is reversed back when the VoIP session ends.

Figure 5-19: VoIP - Telephone Interface - NW Map



Reader's Notes

6 Connecting the MP-202 to a VoIP Service Provider

Using the MP-202's VoIP capabilities, it is possible to connect to a remote SIP server in order to conduct worldwide phone calls.

The following section describes how to place a worldwide phone call utilizing the MP-202's VoIP capabilities over a SIP server. Verify that your Telephone Adapter and telephone are correctly connected and that your WAN connection is up.

6.1 Opening a SIP Account

Before you can connect to a SIP server, it is necessary that you obtain a SIP account. The following section describes how to open a free worldwide dialing SIP account. You can also obtain a paid SIP account.

➢ To open a free worldwide dialing SIP account on the Pulver.com Free World Dialup service:

- Browse to "http://www.pulver.com/fwd" http://www.pulver.com/fwd and open a new account.

6.2 Configuring VoIP Parameters

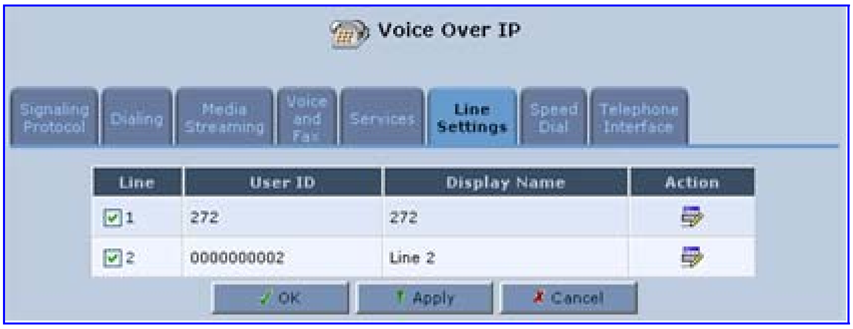
Note: This section describes the minimal set of changes required to connect to a VoIP Service Provider. Other configuration changes might be required to connect to some Service Providers.

➢ To configure VoIP parameters:

1. Click the icon ‘Voice Over IP’ on the toolbar on the left side of the page; the ‘Voice Over IP’ configuration screen opens.

2. Click tab ‘Line Settings’. If you only have a single number, disable line 2 by unchecking the ‘2’ checkbox and click ‘Apply’.

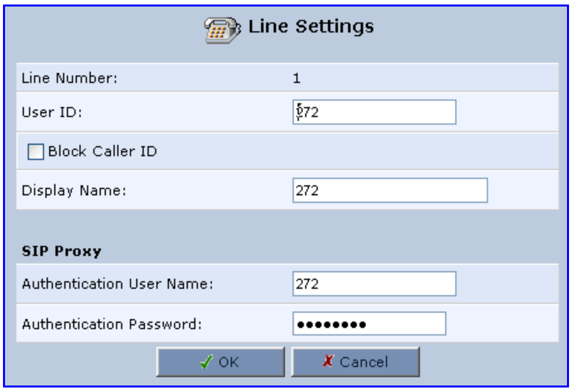
Figure 6-1: VoIP - Line Settings



Line	User ID	Display Name	Action
☑ 1	272	272	
☑ 2	0000000002	Line 2	

3. Click the ‘Action’ icon on the right of line 1; the ‘Line Settings’ screen opens (refer to the figure). Use the configuration values provided by your ISP to configure the parameters in this screen.

Figure 6-2: VoIP - Line Settings - Defining a New Line



Line Settings

Line Number:	1
User ID:	272
□ Block Caller ID	
Display Name:	272

SIP Proxy

Authentication User Name:	272
Authentication Password:	•••••••••

4. Click tab ‘Signaling Protocol’ and check the box ‘Use SIP Proxy’ (refer to "Configuring Signaling Protocol Parameters" on page 32

5. Define the field ‘Proxy IP Address or Host Name’ of the ISP’s SIP proxy, provided by the ISP (refer to "Configuring Signaling Protocol Parameters" on page 32

6. Press ‘OK’ or ‘Apply’ to complete the VoIP configuration.

Note: Check that the gateway was successfully registered by clicking ‘System Monitoring’ > tab ‘Voice over IP’; entry ‘SIP Registration’ should indicate ‘Registered’ for the line(s) you configured. Phone 1 and Phone 2 LEDs should be flashing slowly.

- Pick up the phone receiver and listen for the dial tone; you’re now ready to place an outgoing call.
- All your settings are saved in the gateway's non-volatile memory. From now on, you won’t need the PC to make VoIP calls.

7 Making VoIP Calls

Users connected to the MP-202 can place calls, put calls on hold, transfer calls and manage 3-way conferences. The following describes how to perform these operations.

7.1 Placing a Call

➢ To place a call, take these steps:

1. Pick up the phone.
2. Make sure that you can hear a dial tone
3. Dial the remote party's number or pre-configured speed dial number.

7.2 Answering a Waiting Call

➢ To answer a waiting call when 'Flash only' is configured (refer to "Configuring Dialing Parameters" on page 39):

1. When you hear a call waiting tone (during a call), press 'Flash' on the phone; this puts the active call on hold and switches to the waiting call.
2. To return to the original call, press Flash again. You can toggle from one party to another as much as you like by pressing Flash.

➢ To answer a waiting call when 'Flash + digits sequence' is configured (refer to "Configuring Dialing Parameters" on page 39):

1. When you hear the call waiting tone (during a call), press the 'Flash' key on the phone and then the '1' key; this puts the original call on hold and switches to the waiting call.
2. To return to the original call, press Flash+1 again. You can toggle from one party to another as much as you like by pressing Flash+1.

7.3 Putting a Call on Hold

➢ To place the remote party on hold when 'Flash only' is configured (refer to "Configuring Dialing Parameters" on page 39):

1. During a call, press 'Flash' on the phone; the phone plays a dial tone. At this point you can initiate a second call by dialing another party's number.

Note: If you press 'Flash' again before the other party answers, you'll revert to the original call. If, however, the other party answers and you press 'Flash', a 3-way conference is established.

- ➢ **To place the remote party on hold when 'Flash + digits sequence' is configured (refer to "Configuring Dialing Parameters" on page 39):**

1. Press the 'Flash' key and then the '1' key on the phone; the phone plays a dial tone. At this point you can initiate a second call by dialing another party's number.
2. To cancel the hold state and resume the previous phone call, press 'Flash' and then '1'.

7.4 Performing a Call Transfer

- ➢ **To transfer an existing call with (B) to a third party (C) when 'Flash only' is configured (refer to "Configuring Dialing Parameters" on page 39):**

1. During a call with party B, press 'Flash'; Party B is placed on hold and you'll hear a dial tone.
2. Dial party C's number.
3. You can wait for C to answer or not.
4. On hook; you've transferred B to C.

- ➢ **To transfer an existing call with (B) to a third party (C) when 'Flash + digits sequence' is configured (refer to "Configuring Dialing Parameters" on page 39):**

1. During a call with party B, press 'Flash' and then the '1' key on the phone; Party B is placed on hold and you'll hear a dial tone.
2. Dial party C's number.
3. You can wait for C to answer or not.
4. Press the 'Flash' key and then the '2'; you've transferred B to C; a warning tone is heard.

7.5 Establishing a 3-Way Conference

- ➢ **To extend an existing call with party B into a 3-way conference by bringing in party C when 'Flash only' is configured (refer to "Configuring Dialing Parameters" on page 39):**

1. During a call with party B, press 'Flash'; Party B is placed on hold and you'll hear a dial tone.
2. Dial party C's number and wait until the call is established.
3. Press 'Flash' again to put B and C in a 3-way conference.
4. To end the 3-way conference call, on-hook. Alternatively, press 'Flash' again.

➢ To extend an existing call with party B into a 3-way conference by bringing in party C when 'Flash + digits sequence' is configured (refer to "Configuring Dialing Parameters" on page 39):

1. During a call with party B, press 'Flash' and then the '1' key on the phone; Party B is now placed on hold and you'll hear a dial tone.
2. Dial party C's number and wait until the call is established.
3. Press 'Flash' and then the '3' key to put B and C in a 3-way conference.
4. To end the 3-way conference call, on-hook. Alternatively, press 'Flash' and then the '3' key.

7.6 Forwarding Calls to Another Phone

➢ To forward calls to another phone:

1. First configure call forwarding (refer to "Configuring Services Parameters" on page 47)
2. Pick up the phone.
3. Make sure that you can hear a dial tone
4. Dial the call forward key sequence, for example, *32; you'll hear a dial tone.
5. Dial the number of the phone to which you want calls forwarded; you'll hear a stutter tone (refer to "Configuring Services Parameters" on page 47).
6. Replace the receiver; from now on, all incoming calls will be forwarded. Every time you pick up this receiver you'll hear the stutter tone for the length of time you configured for parameter 'Stutter Tone Duration'.

➢ To deactivate calls fowarding:

1. Pick up the phone; you'll hear a stutter tone.
2. Dial the call forward key sequence.
3. Replace the receiver.
4. To make sure you've de-activated, pick up the phone again; you should hear a regular dial tone and not the stutter tone.

Reader's Notes

8 Quality of Service (QoS)

8.1 Traffic Shaping

Traffic Shaping is the solution for managing and avoiding congestion where a high speed LAN meets limited broadband bandwidth. A user may have, for example, a 100 Mbps Ethernet LAN with a 100 Mbps WAN interface router. The router may communicate with the ISP using a modem with a bandwidth of 2Mbps. This typical configuration makes the modem, having no QoS module, the bottleneck. The router sends traffic as fast as it is received, while its well-designed QoS algorithms are left unused. Traffic shaping limits the bandwidth of the router, artificially forcing the router to be the bottleneck.

A traffic shaper is essentially a regulated queue that accepts uneven and/or bursty flows of packets and transmits them in a steady, predictable stream so that the network is not overwhelmed with traffic.

While Traffic Priority allows basic prioritization of packets, Traffic Shaping provides more sophisticated definitions, such as:

- Bandwidth limit for each device
- Bandwidth limit for classes of rules
- Prioritization policy
- TCP serialization on a device

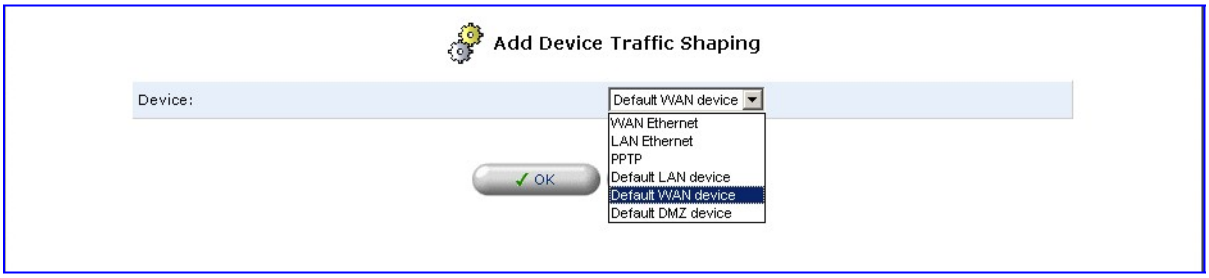
Additionally, you can define QoS traffic shaping rules for a default device. These rules will be used on a device that has no definitions of its own. This enables the definition of QoS rules on Default WAN, for example, and their maintenance even if the PPP or bridge device over the WAN is removed.

8.1.1 Device Traffic Shaping

This section describes the different Traffic Shaping screens and terms, and presents the feature's configuration logic.

1. On the sidebar click the QoS link and then click the tab 'Traffic Shaping'.
2. Click the link 'New Entry'; the screen 'Add Device Traffic Shaping' opens (refer to the figure).

Figure 8-1: QoS - Add Device Traffic Shaping

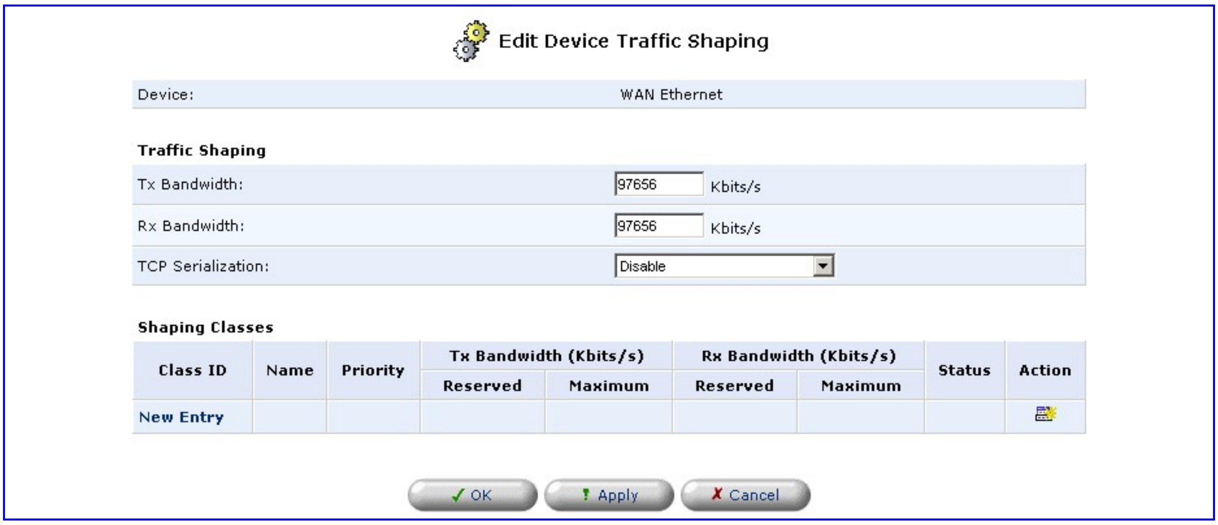


Add Device Traffic Shaping

Device: Default WAN device

3. From the drop-down list select the device for which to shape traffic. The drop-down list includes all your interfaces as well as category options (e.g., All LAN Devices, All WAN Devices) and VPNs such as PPoE, PPTP and L2TP (if defined). Select, for example, the option 'WAN Ethernet' and click ‘OK’; the ’Edit Device Traffic Shaping’ screen opens (refer to the figure).

Figure 8-2: QoS - Edit Device Traffic Shaping



Edit Device Traffic Shaping

Device: WAN Ethernet

Traffic Shaping

Tx Bandwidth: 97656 Kbits/s

Rx Bandwidth: 97656 Kbits/s

TCP Serialization: Disable

Shaping Classes

Class ID	Name	Priority	Tx Bandwidth (Kbits/s)		Rx Bandwidth (Kbits/s)		Status	Action
			Reserved	Maximum	Reserved	Maximum		
New Entry								

4. Configure the following fields:

Table 8-1: Edit Device Traffic Shaping - Parameter Descriptions

Parameter	Description
Tx Bandwidth	This parameter limits the gateway’s bandwidth transmission rate. The purpose is to limit the bandwidth of the WAN device to that of the weakest outbound link, for instance, the DSL speed provided by the ISP. This forces the gateway to be the network bottleneck, where sophisticated QoS prioritization can be performed. If the device’s bandwidth is not limited correctly, the bottleneck will be in an unknown router or modem on the network path, rendering the gateway QoS useless.
Rx Bandwidth	In the same manner, this parameter limits the gateway’s bandwidth reception rate to that of the DSL modem.
TCP Serialization	You can enable TCP Serialization in its combo box, either for active voice calls only or for all traffic. The screen will refresh, adding a ’Maximum Delay’ field (refer to the figure). This function allows you to define the maximal allowed transmission time frame (in milliseconds) of a single packet. Any packet that requires a longer time to be transmitted, will be fragmented to smaller sections. This avoids transmission of large, bursty packets that may cause delay or jitter for real-time traffic such as VoIP.

8.1.2 Shaping Classes

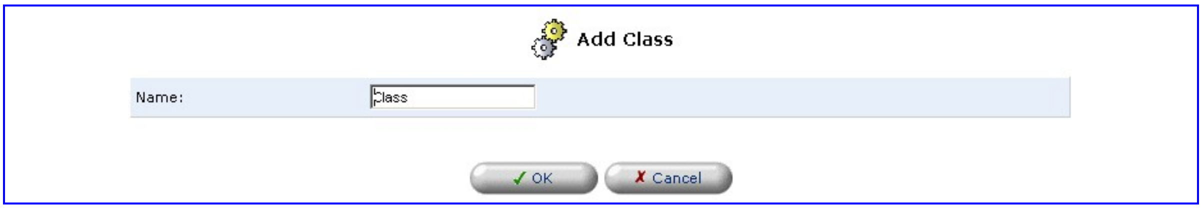
The bandwidth of a device can be divided in order to reserve constant portions of bandwidth to predefined traffic types. Such a portion is known as a Shaping Class. When not used by its predefined traffic type, or owner (for example VoIP), the class will be available to all other traffic. However when needed, the entire class is reserved solely for its owner. Moreover, you can limit the maximum bandwidth that a class can use even if the entire bandwidth is available.

When a shaping class is defined for a specific traffic type, two shaping classes are created. The second class is the 'Default Class', responsible for all the packets that do not match the defined shaping class, or any other classes that may be defined on the device. This can be viewed in the Class Statistics screen.

➢ To add a shaping class:

1. In the screen 'Edit Device Traffic Shaping', section 'Shaping Classes' (refer to the figure), click the link 'New Entry'; the screen 'Add Class' opens (refer to the figure).

Figure 8-3: QoS - Edit Device Traffic Shaping - Add Class



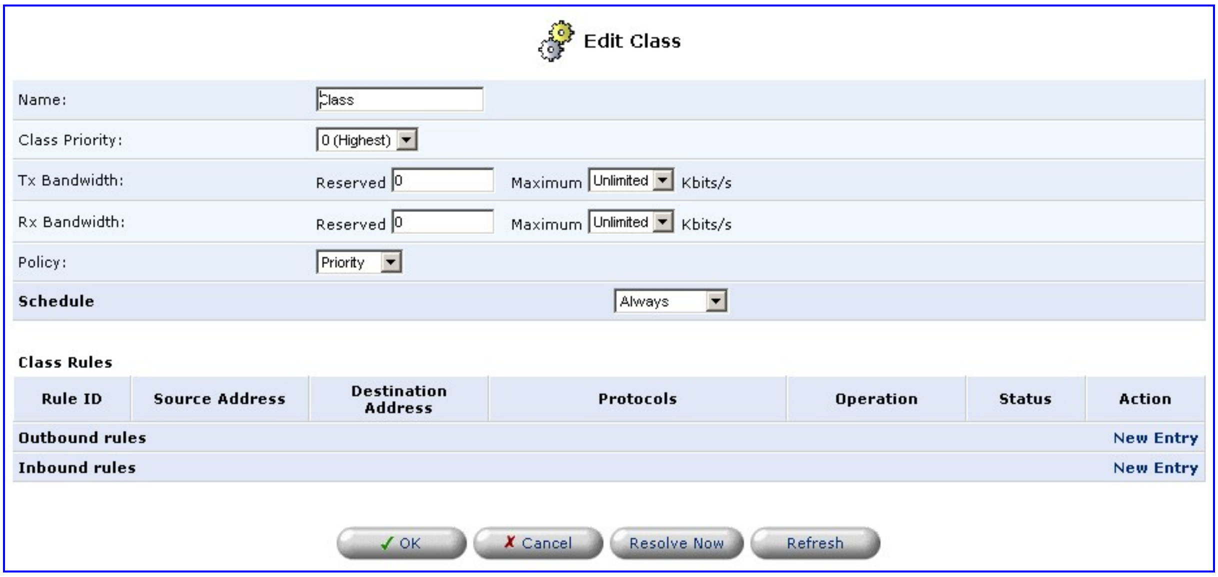
Add Class

Name: Class

2. Name the new class and click 'OK' to save the settings; the screen 'Edit Device Traffic Shaping' opens.

3. Click the class name to edit the shaping class. Alternatively, click its icon 'Edit' under the column 'Action'; the 'Edit Class' screen opens (refer to the figure).

Figure 8-4: QoS - Edit Device Traffic Shaping - Edit Class



Edit Class

Name:	Class		
Class Priority:	0 (Highest)		
Tx Bandwidth:	Reserved 0	Maximum Unlimited	Kbits/s
Rx Bandwidth:	Reserved 0	Maximum Unlimited	Kbits/s
Policy:	Priority		
Schedule	Always		

Class Rules

Rule ID	Source Address	Destination Address	Protocols	Operation	Status	Action
Outbound rules						New Entry
Inbound rules						New Entry

Configure the following fields:

Table 8-2: Edit Class - Parameter Descriptions

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>Name</td><td colspan="2">The name of the class.</td></tr>
<tr><td>Class Priority</td><td colspan="2">The class can be granted one of eight priority levels, zero being the highest and seven the lowest.</td></tr>
<tr><td>Tx Bandwidth</td><td colspan="2">The reserved transmission bandwidth (Committed Information Rate, or CIR) , in kbps, for each class.</td></tr>
<tr><td>Rx Bandwidth</td><td colspan="2">The reserved reception bandwidth (Committed Information Rate, or CIR) , in kbps, for each class.</td></tr>
<tr><td rowspan="5">Policy</td><td colspan="2">The class policy determines the policy of routing packets inside the class. Select either:
1. Priority
2. FIFO
3. Fairness
4. RED
Refer to the following four descriptions.</td></tr>
<tr><td>Priority</td><td>Priority queuing utilizes multiple queues so that traffic is distributed among queues based on priority. This priority is defined according to packet priority, which can be defined explicitly, by a DSCP value, or by a 802.1p value.</td></tr>
<tr><td>FIFO</td><td>First In First Out. This priority queue ignores any previously-marked priority that packets may have.</td></tr>
<tr><td>Fairness</td><td>The fairness algorithm ensures no starvation by granting all packets a certain level of priority.</td></tr>
<tr><td>RED</td><td>Random Early Detection. Utilizes statistical methods to drop packets in a ‘probabilistic’ way before queues overflow. Dropping packets in this way slows a source down enough to keep the queue steady and reduces the number of packets that would be lost when a queue overflows and a host is transmitting at a high rate.</td></tr>
<tr><td>Schedule</td><td colspan="2">By default, the class will always be active. However, you can configure scheduler rules in order to define time segments during which the class may be active.</td></tr>
</table>

8.1.2.1 Class Rules

Class rules define which packets belong to the class. They must be defined in order to associate packets that meet them with the shaping class. Without class rules, the shaping class will have no effect whatsoever. Each class can have outbound and/or inbound rules, for outgoing and incoming traffic respectively. For example, you can define that all outgoing packets from computer A in your LAN belong to your VoIP class. These packets will be limited to the class settings (bandwidth, schedule, etc.). In addition, you can define the traffic protocol and priority for each rule (this is not mandatory as in Traffic Priority rules).

8.1.2.1.1 Inbound and Outbound Data

The gateway can control outgoing data easily. It can queue packets, delay them, give precedence to other packets, or drop them. This helps in resolving upload (Tx) traffic bottlenecks and in most cases is sufficient. However, in the case of download (Rx) traffic bottlenecks, the ability to control the flow is much more limited. The gateway cannot queue packets, since in most cases the LAN is much faster then the WAN, and when the gateway receives a packet from the WAN, it passes it immediately to the LAN.

QoS for ingress data has the following limitations, which do not exist for outgoing data:

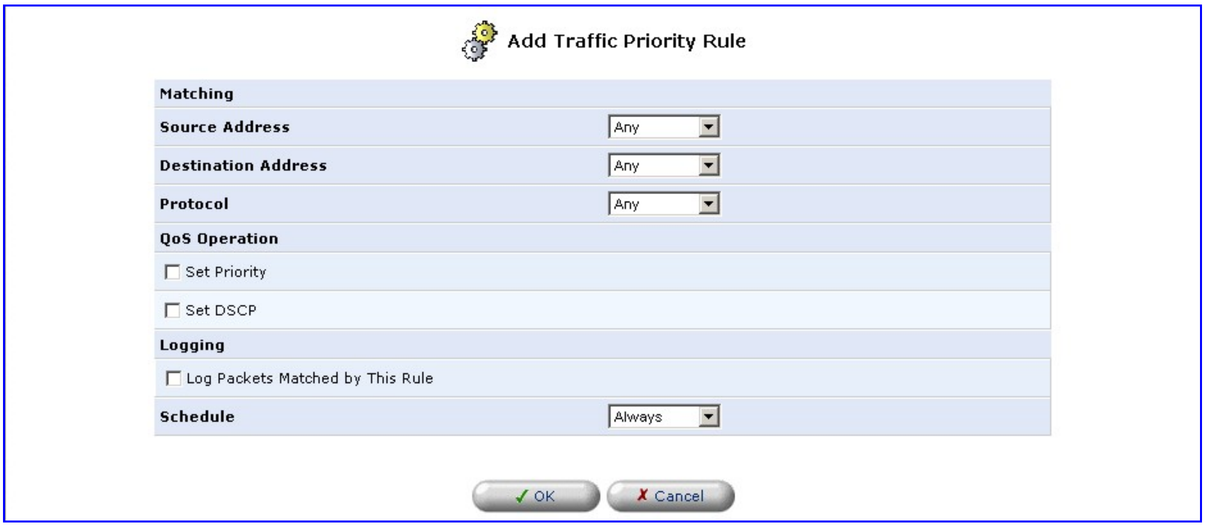
- QoS can only be applied to TCP streams (UDP streams cannot be delayed).
- No borrowing mechanism.
- When reserving Rx bandwidth, it is strictly taken from the bandwidth of all other classes.

Furthermore, the gateway cannot control the behavior of its WAN gateway (usually the ISP), which may not have proper QoS handling. Unfortunately, this is a common situation. Let’s look at a scenario of downloading a large file and surfing the Internet at the same time. Downloading the file is distinguished by small requests, followed by very large responses. This may result in blocking HTML traffic at the ISP. A solution for such a situation is limiting the bandwidth of low-priority TCP connections (such as the file download).

➢ To add a new outbound/inbound class rule:

1. In the screen 'Edit Class' under the screen section 'Class Rules', click link 'New Entry'; the screen 'Add Traffic Priority Rule’ opens (refer to the figure).

Figure 8-5: QoS - Edit Device Traffic Shaping - Edit Class - Add Traffic Priority Rule



Add Traffic Priority Rule

Matching	
Source Address	Any
Destination Address	Any
Protocol	Any
QoS Operation	
□ Set Priority	
□ Set DSCP	
Logging	
□ Log Packets Matched by This Rule	
Schedule	Always

Table 8-3: Add Traffic Priority Rule - Parameter Descriptions

Parameter	Description
Matching	Use the parameters in this screen section to apply a rule. To apply the rule, matching must be performed between IP addresses and/or a traffic protocol must be defined. From the drop-down list choose 'Any', 'User Defined' or the host.
Source Address	The source address of the packets. From the drop-down list choose 'Any', 'User Defined' or the host.
Destination Address	The destination address of the packets. From the drop-down list choose 'Any', 'User Defined' or the host.
Protocol	From the drop-down list, choose a specific protocol, or add a new one by choosing 'User Defined'; the screen 'Edit Service' opens. Click the icon 'new' under the column 'Action'; this commences a sequence that adds a new protocol.
QoS Operation	In this screen section, set a Quality of Service working method. Check parameter 'Set Priority' or 'Set DSCP' (refer to the descriptions below).
Set Priority	Check this check box to add a priority to the rule. Select priority level 0-7 where 0 = lowest and 7 = highest (each priority level is mapped to low/medium/high priority). This sets the priority of a packet on the connection matching the rule, while routing the packet.
Set DSCP	Check this check box to mark a DSCP value on packets matching this rule. Enter a value between 0-63 in the field that appears.
Log Packets Matched by This Rule	Under the screen section 'Logging', this check box must be checked in order to log the first packet from a connection that was matched by this rule.
Schedule	'Always' or 'User Defined'. By default, the rule will always be active. However, you can configure scheduler rules in order to define time segments during which the rule may be active.

Note: The hierarchy of the class rules is determined by the order of their addition to the class. For example, if your first rule is 'match packets with any source address, any destination address, and any protocol to this class; then all packets traveling through the gateway will be associated with the specific class. Any rules defined later will not have any effect.

8.2 Traffic Priority

Traffic Priority allows you to manage and avoid traffic congestion by defining inbound and outbound priority rules for each device on your gateway. These rules determine the priority that packets, traveling through the device, will receive. QoS parameters (DSCP marking and packet priority) are set per packet, on an application basis.

You can set QoS parameters using flexible rules, according to the following parameters:

- Source/destination IP address, MAC address or host name
- Device
- Source/destination ports

Limit the rule for specific days and hours; the gateway supports two priority marking methods for packet prioritization:

- DSCP
- 802.1p Priority

The matching of packets by rules is connection-based, known as Stateful Packet Inspection (SPI), using the same connection-tracking mechanism used by firewall. Once a packet matches a rule, all subsequent packets with the same attributes receive the same QoS parameters, both inbound and outbound.

A packet can match more than one rule. Therefore:

- The first class rule has precedence over all other class rules (scanning is stopped once the first rule is reached).
- The first traffic-priority (classless) rule has precedence over all other traffic-priority rules.
- There is no prevention of a traffic-priority rule conflicting with a class rule. In this case, the priority and DSCP setting of the class rule (if given) will take precedence.

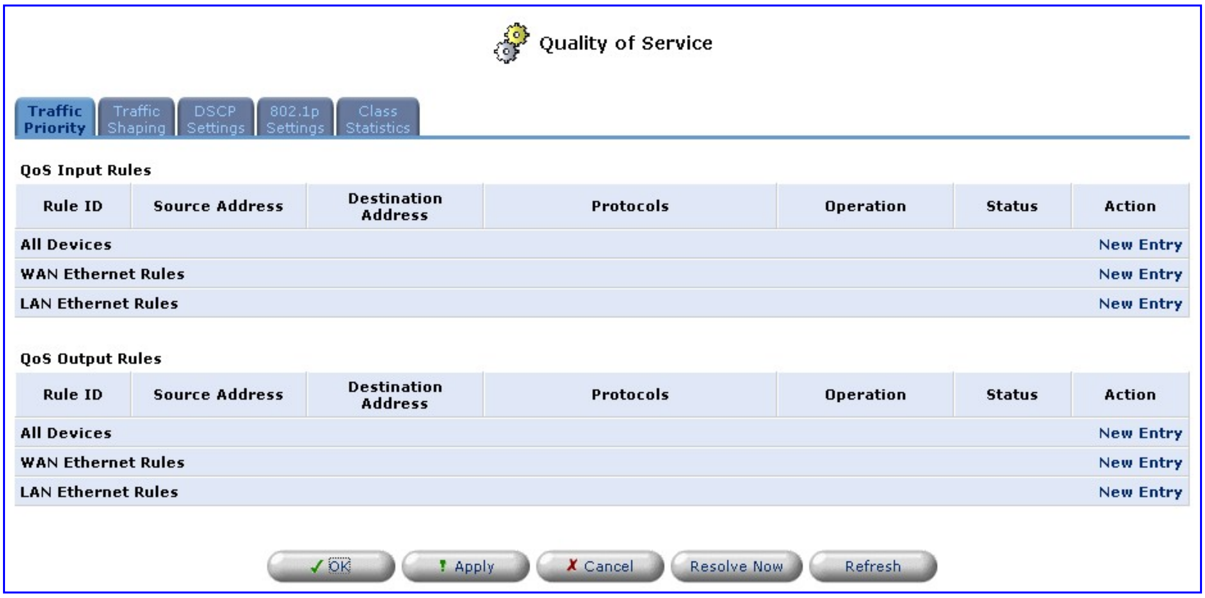
Connection-based QoS also allows inheriting QoS parameters by some of the applications that open subsequent connections. For instance, you can define QoS rules on SIP, and the rules will apply to both control and data ports (even if the data ports are unknown). This feature applies to all applications that have ALG at firewall:

- Any
- User Defined (FTP, HTTP, HTTPS, TFTP, IMAP, PING, POP3, SNMP, SMTP, Telnet, L2TP, Traceroute or any other protocol)

➢ To set traffic priority rules:

1. Press the QoS button on the sidebar; the Traffic Priority screen (the first tab) appears. This screen is divided into two identical sections, one for 'QoS Input Rules' and the other for 'QoS Output Rules', which are for prioritizing inbound and outbound traffic respectively. Each section lists all the devices on which rules can be set. You can set rules on all devices at once by clicking the link 'New Entry' adjacent to 'All Devices'.

Figure 8-6: QoS - Traffic Shaping



QoS Input Rules

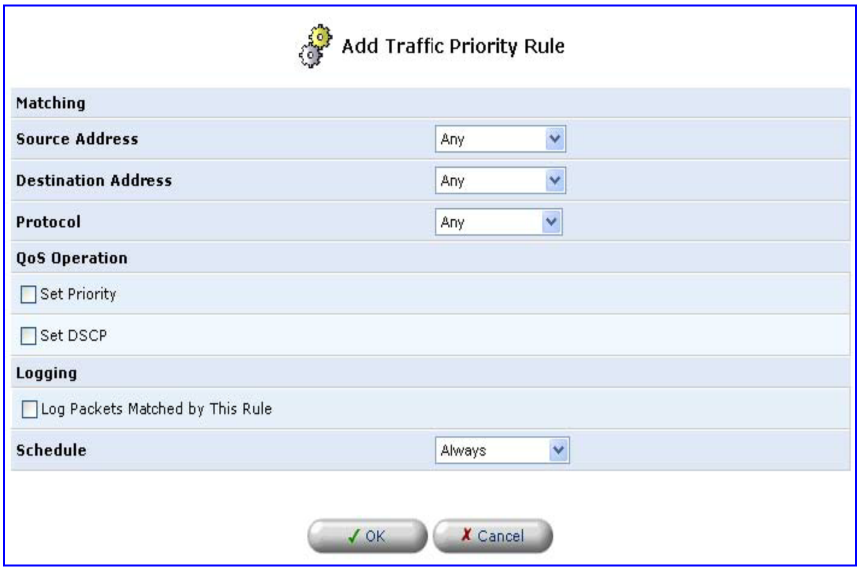
Rule ID	Source Address	Destination Address	Protocols	Operation	Status	Action
All Devices						New Entry
WAN Ethernet Rules						New Entry
LAN Ethernet Rules						New Entry

QoS Output Rules

Rule ID	Source Address	Destination Address	Protocols	Operation	Status	Action
All Devices						New Entry
WAN Ethernet Rules						New Entry
LAN Ethernet Rules						New Entry

2. After clicking the appropriate 'New Entry' link, the screen 'Add Traffic Priority Rule' opens (refer to the figure).

Figure 8-7: QoS - Add Traffic Priority Rule



Matching	
Source Address	Any
Destination Address	Any
Protocol	Any
QoS Operation	
□ Set Priority	
□ Set DSCP	
Logging	
□ Log Packets Matched by This Rule	
Schedule	Always

Table 8-4: Add Traffic Priority Rule - Parameter Descriptions

Parameter	Description
Source Address	The source address of the packets sent to or received from the network object. From the drop-down list choose 'Any', 'User Defined' or the host.
Destination Address	The destination address of the packets sent to or received from the network object. This address can be configured in the same manner as the source address. From the drop-down list choose 'Any', 'User Defined' or the host.
Protocol	From the drop-down list, choose a specific traffic protocol, or add a new one by choosing 'User Defined'; the screen 'Edit Service' opens. Click the icon 'new' under the column 'Action'; this commences a sequence that adds a new protocol.
QoS Operation	In this screen section, set a Quality of Service working method. Check parameter 'Set Priority' or 'Set DSCP' (refer to the descriptions below).
Set Priority	Check this check box to add a priority to the rule; the screen 'Edit Service' opens, allowing you to select between one of eight priority levels, 0 = lowest and 7 = highest (each priority level is mapped to low/medium/high priority). This sets the priority of a packet on the connection matching the rule, while routing the packet.
Set DSCP	Check this check box to mark a DSCP value on packets matching this rule; the screen 'Edit Service' opens, allowing you to enter the hexadecimal value of the DSCP.
Log Packets Matched by This Rule	Under the screen section 'Logging', this check box must be checked in order to log the first packet from a connection that was matched by this rule.
Schedule	'Always' or 'User Defined'. By default, the rule will always be active. However, you can configure scheduler rules in order to define time segments during which the rule may be active.

3. Click ’OK’ to save the settings

8.3 DSCP Mapping

In order to understand what is Differentiated Services Code Point (DSCP), one must first be familiarized with the Differentiated Services model.

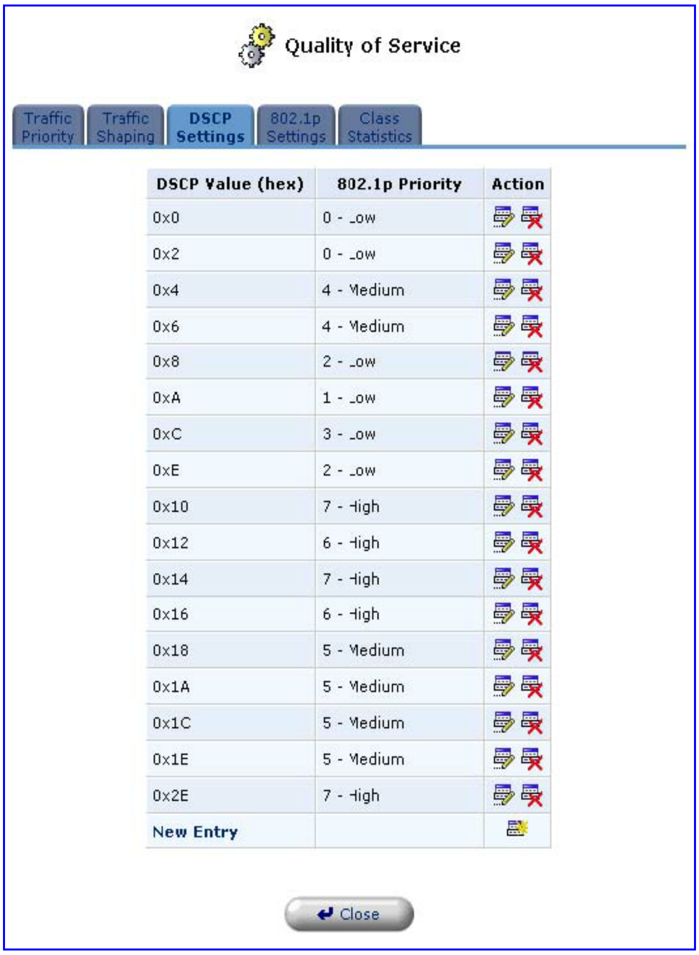
Differentiated Services (Diffserv) is a Class of Service (CoS) model that enhances best-effort Internet services by differentiating traffic by users, service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service, as appropriate for voice calls, video playback or other delay-sensitive applications, via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

Diffserv defines a field in IP packet headers referred to as DSCP. Hosts or routers passing traffic to a Diffserv-enabled network will typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular queue handling or scheduling behavior.

The gateway provides a table of predefined DSCP values, which are mapped to 802.1p priority marking method. You can edit or delete any of the existing DSCP setting, as well as add new entries.

1. Press the QoS button on the sidebar and then click the DSCP Settings tab. The following screen will appear (refer to the figure).

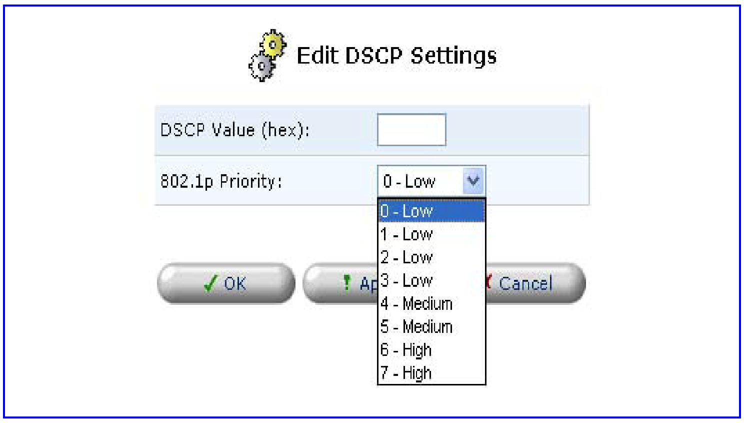
Figure 8-8: QoS - DSCP Settings



DSCP Value (hex)	802.1p Priority	Action
0x0	0 - Low	✎ ✖
0x2	0 - Low	✎ ✖
0x4	4 - Medium	✎ ✖
0x6	4 - Medium	✎ ✖
0x8	2 - Low	✎ ✖
0xA	1 - Low	✎ ✖
0xC	3 - Low	✎ ✖
0xE	2 - Low	✎ ✖
0x10	7 - High	✎ ✖
0x12	6 - High	✎ ✖
0x14	7 - High	✎ ✖
0x16	6 - High	✎ ✖
0x18	5 - Medium	✎ ✖
0x1A	5 - Medium	✎ ✖
0x1C	5 - Medium	✎ ✖
0x1E	5 - Medium	✎ ✖
0x2E	7 - High	✎ ✖
New Entry		✚

2. To edit an existing entry, click its Edit action icon. To add a new entry, click the New Entry link. In both cases, the 'Edit DSCP Settings' screen will appear (refer to the figure).

Figure 8-9: QoS - Edit DSCP Settings



Edit DSCP Settings

DSCP Value (hex):

802.1p Priority: 0 - Low

3. Configure the following fields:

Table 8-5: Edit DSCP Settings- Parameter Descriptions

Parameter	Description
DSCP Value (hex)	Enter a hexadecimal number that will serve as the DSCP value.
802.1p Priority	Select a 802.1p priority level from the combo box (each priority level is mapped to low/medium/high priority).

- Click 'OK' to save the settings.

Note that the DSCP value overriding the priority of incoming packets with an unassigned value (priority 0, assumed to be a no-priority-set) is '0x0' (refer to the figure). By default, this value is mapped to 802.1p priority level '0 -Low', which means that such packets will receive the lowest priority.

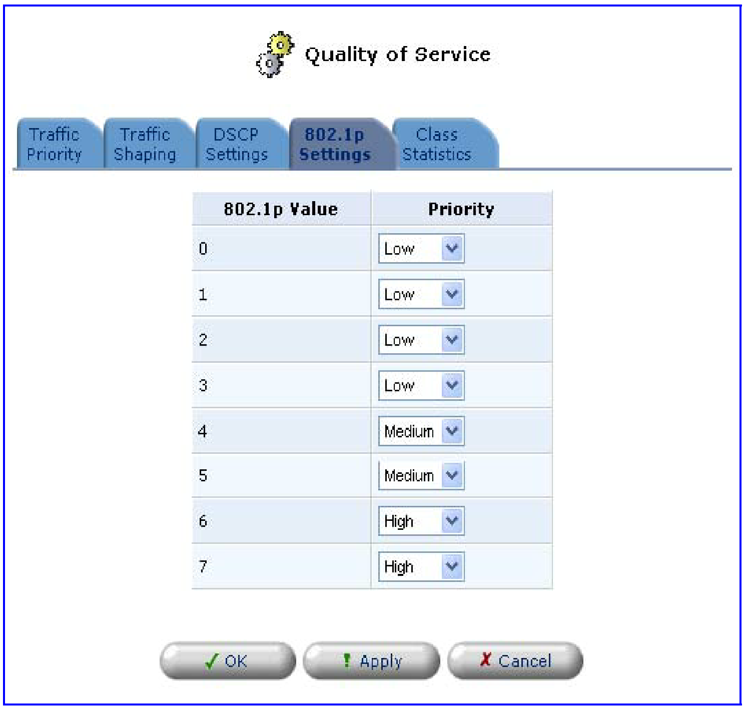
8.4 802.1p Mapping

The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer. 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority. The gateway maps these eight levels to three main priorities: high, medium and low. By default, values six and seven are mapped to high priority, which may be assigned to network-critical traffic. Values four and five are mapped to medium priority, which may be applied to delay-sensitive applications, such as interactive video and voice. Values three to zero are mapped to low priority, which may range from controlled-load applications down to 'loss eligible' traffic. The zero value is normally used for best-effort traffic. It is the default value for traffic with unassigned priority.

- Click the QoS link on the sidebar and then click the tab '802.1p Settings'; the following screen opens:

Figure 8-10: QoS - 802.1p Settings



802.1p Value	Priority
0	Low
1	Low
2	Low
3	Low
4	Medium
5	Medium
6	High
7	High

- The eight 802.1p values are pre-configured with the three priority levels: high, medium and low. You can change these levels for each of the eight values in their respective combo box.
- Click 'OK' to save the settings.

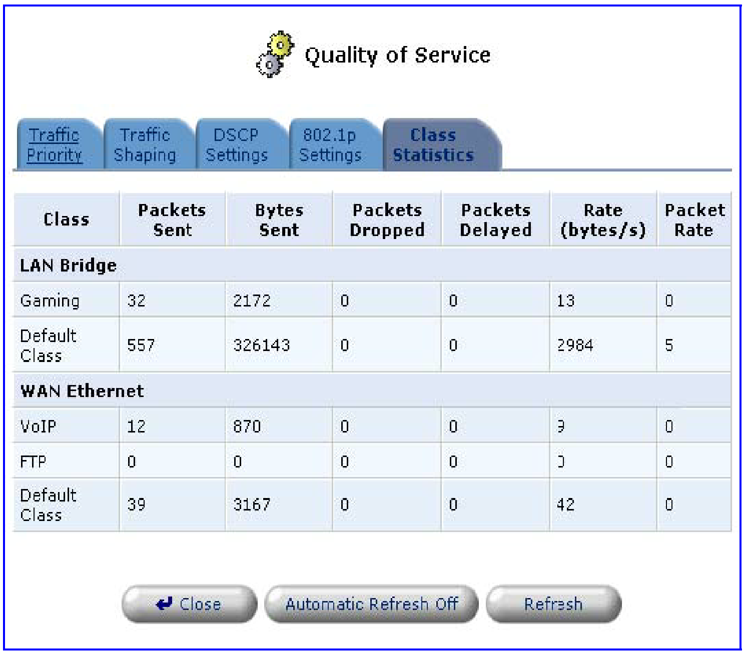
8.5 Class Statistics

The gateway provides you with accurate, real-time information on the traffic moving through your defined device classes. For example, the amount of packets sent, dropped or delayed, are just a few of the parameters that you can monitor per each shaping class.

To view your class statistics, press the QoS button on the sidebar and then click the Class Statistics tab. The following screen will appear (refer to the figure).

Note: Class statistics will only be available after defining at least one class (otherwise the screen will not present any information).

Figure 8-11: QoS - Class Statistics



Class	Packets Sent	Bytes Sent	Packets Dropped	Packets Delayed	Rate (bytes/s)	Packet Rate
LAN Bridge						
Gaming	32	2172	0	0	13	0
Default Class	557	326143	0	0	2984	5
WAN Ethernet						
VoIP	12	870	0	0	3	0
FTP	0	0	0	0	0	0
Default Class	39	3167	0	0	42	0

8.6 Configuring Basic VoIP QoS

The 'Traffic Shaping' feature only ensures priority to calls that are originated *inside* the MP-202. When giving VoIP priority over data, the bottleneck is effectively moved from the Cable / ADSL modem into the MP-202. To give priority to calls from the LAN, you must define a traffic priority rule (for SIP and RTP from the device on the LAN).

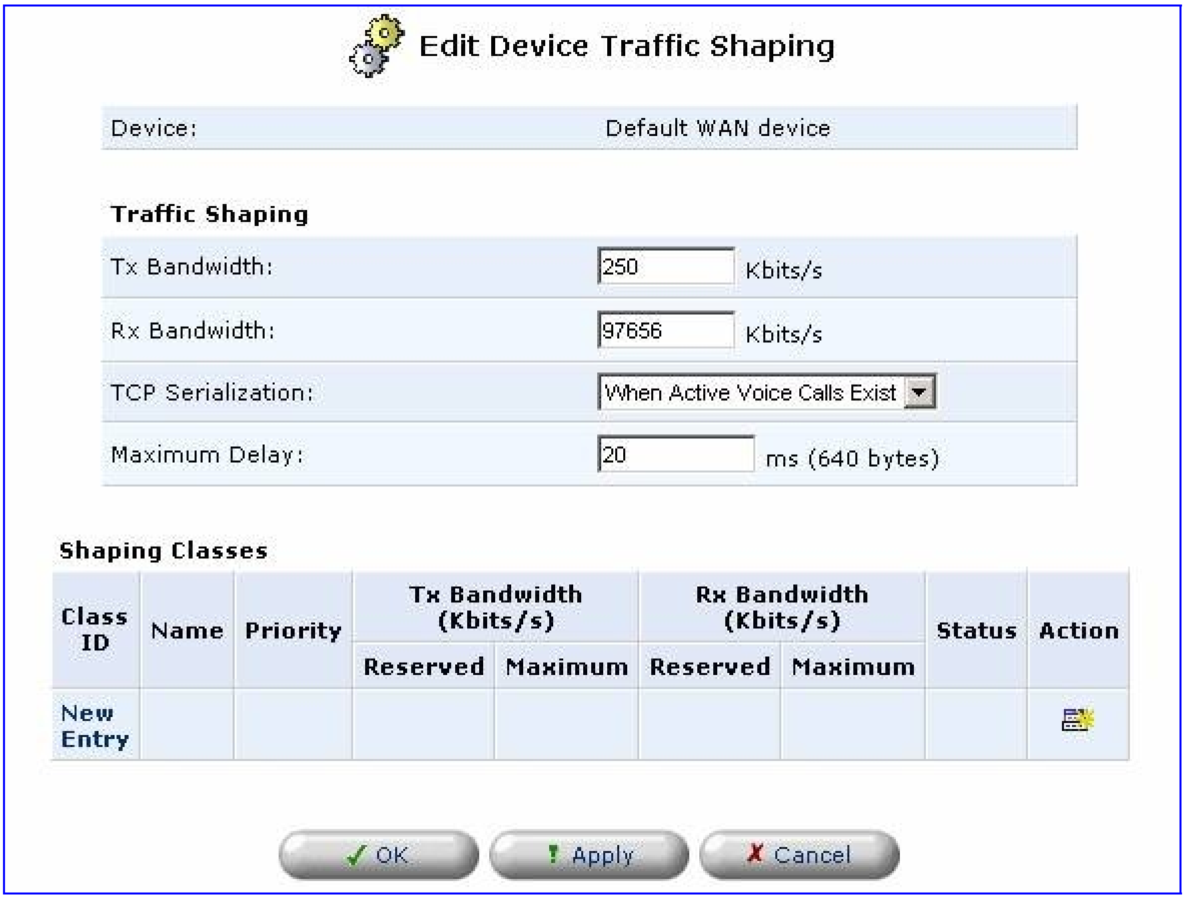
This section recommends a minimal QoS configuration that ensures sufficient QoS for VoIP calls when the gateway is connected behind a broadband (cable or DSL) modem with limited uplink bandwidth and the user runs bandwidth-consuming applications on their PC.

Since most modems do not have any priority mechanisms, the Tx bandwidth of the gateway should be limited according to the modem's uplink bandwidth. Since the gateway will automatically give higher priority to VoIP packets (in its internal queues), it is not necessary to define traffic shaping classes.

➢ To perform a minimal QoS configuration for VoIP:

1. Click on menu 'QoS' on the left sidebar and then click tab 'Traffic Shaping'; the Quality of Service - Traffic Shaping screen opens.
2. Click 'New Entry' (or the icon under column 'Action'); the screen 'Add Device Traffic Shaping' opens.
3. From the drop-down list adjacent to parameter 'Device', select 'Default WAN Device' (or your PPTP/L2TP connection you have created) and click OK; the screen 'Edit Device Traffic Shaping' opens.
4. Limit the Tx bandwidth (parameter 'Tx Bandwidth') according to your modem’s uplink bandwidth.
5. To prevent jitter in outgoing RTP packets, select 'When Active Voice Calls Exist' from the drop-down list adjacent to parameter 'TCP Serialization' and use parameter 'Maximum Delay' to define the maximum allowed delay (e.g. 20 milliseconds). This will cause long TCP packets to be fragmented when there is an active voice call.

Figure 8-12: QoS - Edit Device Traffic Shaping



Edit Device Traffic Shaping

Device:	Default WAN device

Traffic Shaping

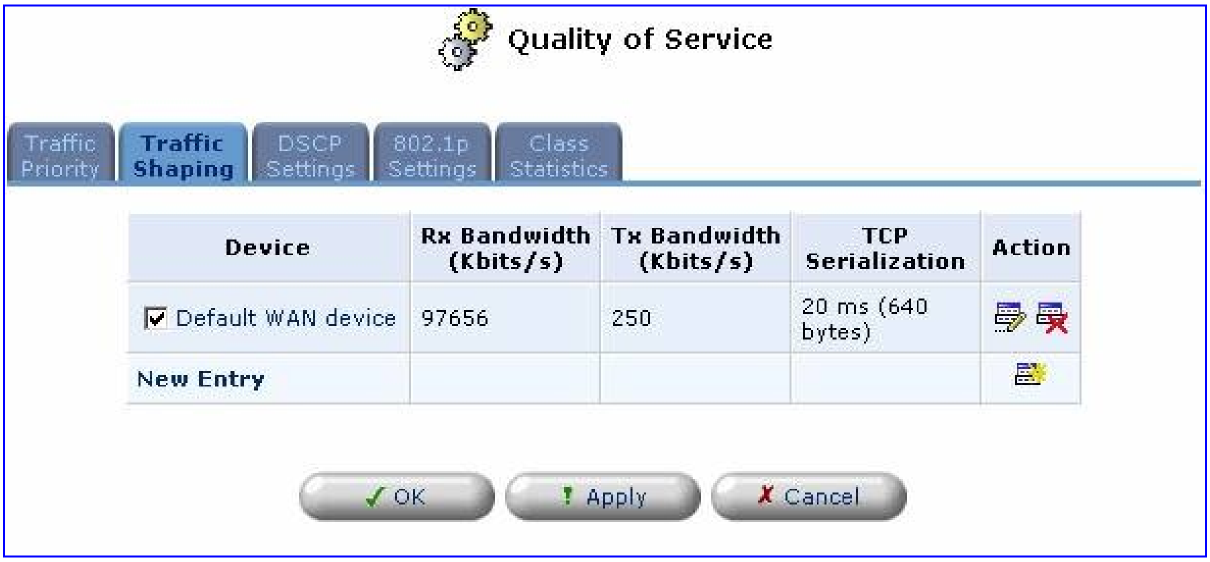
Tx Bandwidth:	250 Kbits/s
Rx Bandwidth:	97656 Kbits/s
TCP Serialization:	When Active Voice Calls Exist
Maximum Delay:	20 ms (640 bytes)

Shaping Classes

Class ID	Name	Priority	Tx Bandwidth (Kbits/s)		Rx Bandwidth (Kbits/s)		Status	Action
			Reserved	Maximum	Reserved	Maximum		
New Entry								

6. Click OK to submit the new definition.

Figure 8-13: QoS - Edit Device Traffic Shaping - Submitting the Configuration



Device	Rx Bandwidth (Kbits/s)	Tx Bandwidth (Kbits/s)	TCP Serialization	Action
☑ Default WAN device	97656	250	20 ms (640 bytes)	
New Entry				

7. Click OK again to exit the QoS page and return to the main page.

Reader's Notes

9 WAN Settings

To change the WAN mode from its default connection type (Ethernet) to PPP, choose from the 'Connection Type' drop-down list in the Quick Setup screen. Alternatively, click link 'New Connection' in the 'Network Connections' screen, check the 'Advanced Connection' radio button and then choose the connection type.

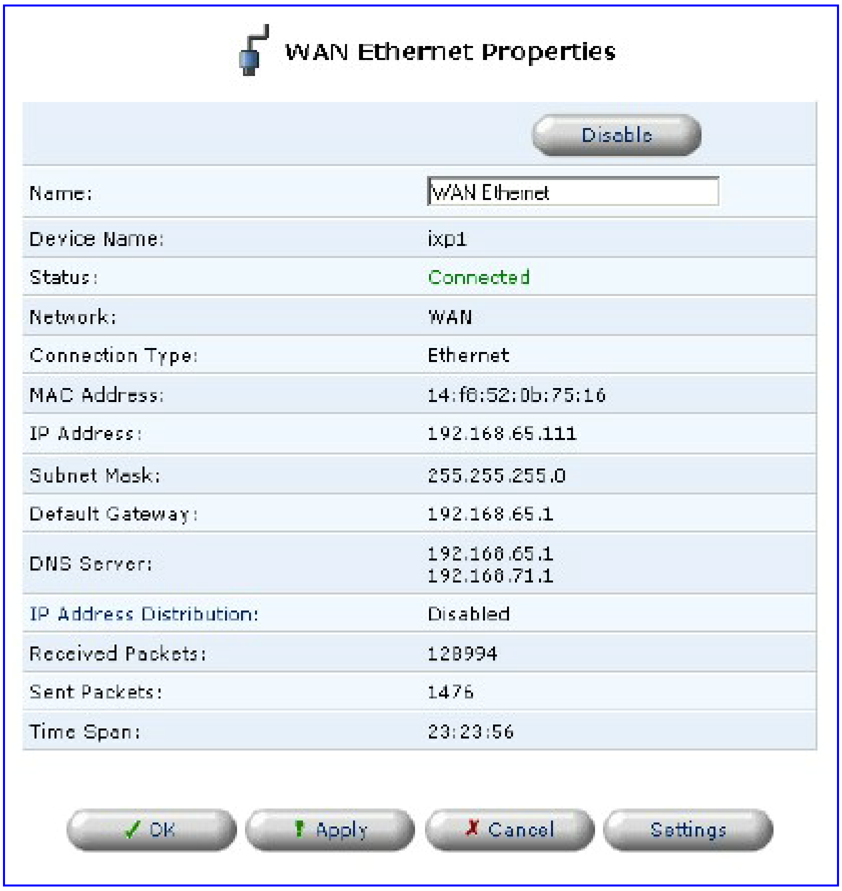
9.1 WAN Ethernet

WAN Ethernet is the default mode. WAN Ethernet is used to connect the MP-202 to the network either directly or via an external modem.

➢ To access its properties:

- Click on the link 'Network Connections' and in the screen 'Network Connections', click link 'WAN Ethernet'; the screen 'WAN Ethernet Properties' opens (refer to the figure).

Figure 9-1: WAN Ethernet Properties

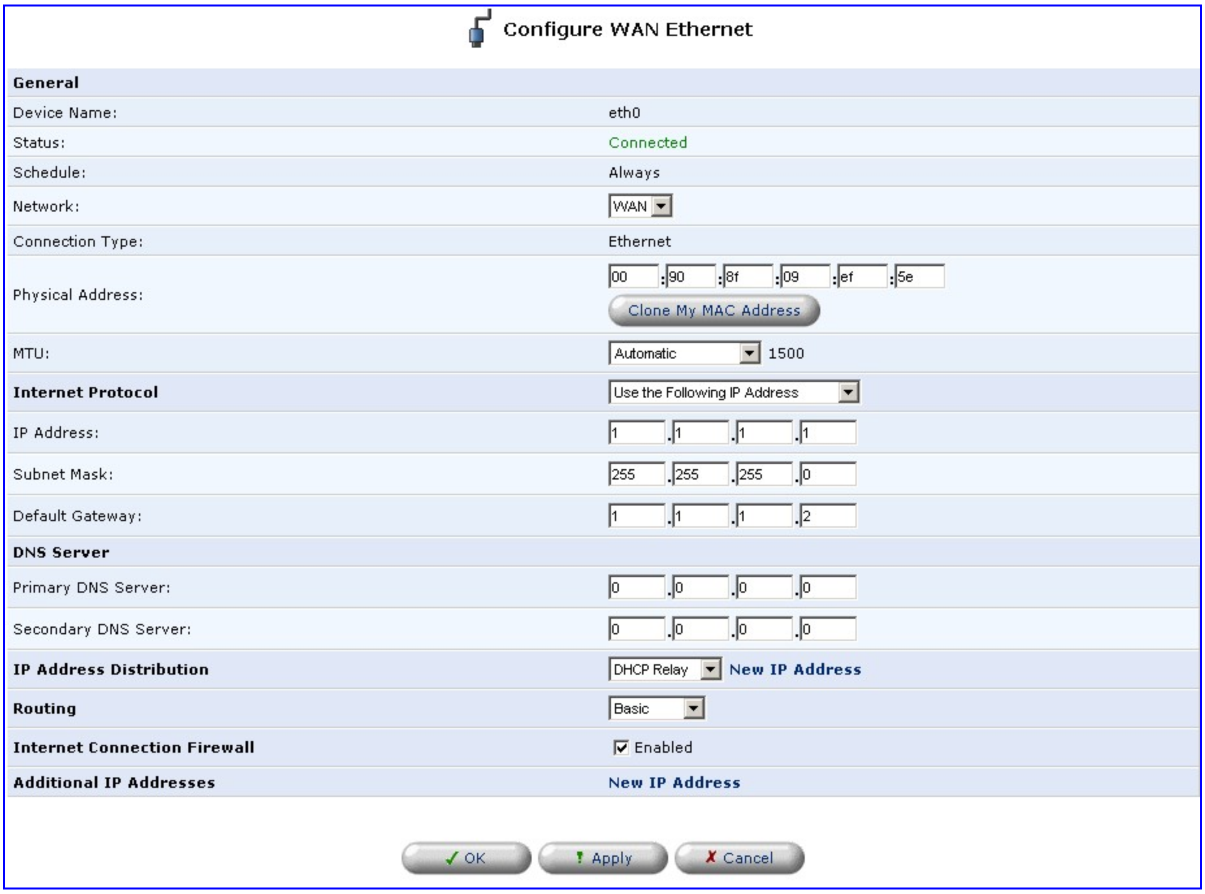


Name:	WAN Ethernet
Device Name:	ixp1
Status:	Connected
Network:	WAN
Connection Type:	Ethernet
MAC Address:	14:f6:52:0b:75:16
IP Address:	192.168.65.111
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.65.1
DNS Server:	192.168.65.1 192.168.71.1
IP Address Distribution:	Disabled
Received Packets:	128994
Sent Packets:	1476
Time Span:	23:23:56

➢ To configure the WAN Ethernet connection:

- Click on the 'Settings' button at the bottom-right of the connection's Properties screen; the screen 'Configure WAN Ethernet' opens:

Figure 9-2: WAN Ethernet Configuration



Configure WAN Ethernet

General	
Device Name:	eth0
Status:	Connected
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00 : 90 : 8f : 09 : ef : 5e Clone My MAC Address
MTU:	Automatic 1500
Internet Protocol	Use the Following IP Address
IP Address:	1 . 1 . 1 . 1
Subnet Mask:	255 . 255 . 255 . 0
Default Gateway:	1 . 1 . 1 . 2
DNS Server	
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0
IP Address Distribution	DHCP Relay **New IP Address**
Routing	Basic
Internet Connection Firewall	☑ Enabled
Additional IP Addresses	**New IP Address**

9.1.1 General

The top part of the screen 'Configure WAN Ethernet' displays general communication parameters. It is recommended not to change the default values in this screen unless you are familiar with the networking concepts they represent. Since your Telephone Adapter is configured to operate with the default values, no parameter modification is necessary. You can configure the following general connection settings:

Table 9-1: General Connection Settings

Parameter	Description
Schedule	You can configure scheduler rules in order to define time segments during which the connection is active (via Advanced>Scheduler Rules).
Network	Select whether the parameters you are configuring relate to a LAN/WAN connection, by selecting LAN/WAN from the drop down list.
Physical Address	The physical address of the network card used for your network. Some cards allow you to change this address.
Clone MAC	Allows you to copy the current MAC address of your PC to the MAC address of this device.
MTU	MTU is the Maximum Transmission Unit. It species the largest packet size permitted for Internet transmission. In the default setting, Automatic, the Telephone Adapter selects the best MTU for your Internet connection. In case you change to manual, you can enter the largest packet size, you should leave this value in the 1200 to 1500 range.

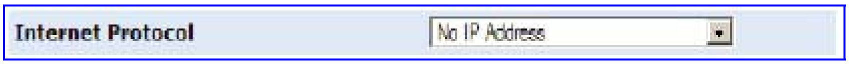
9.1.2 Internet Protocol Settings

Select one of the following Internet Protocol options from the 'Internet Protocol' drop down menu:

- **No IP Address**
- **Obtain an IP Address Automatically** (Your WAN connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports DHCP, or if you are connecting using a dynamic IP address)
- **Use the Following IP Address**

Note that according to the selection you make in the 'Internet Protocol' drop down menu, the screen will refresh and display relevant configuration settings.

Figure 9-3: Internet Protocol Settings - No IP Address



Internet Protocol: No IP Address

The server that assigns the Telephone Adapter with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead.

You can press the 'Release' button to release the current leased IP address.

Once the address has been released, the button text changes to 'Renew'.

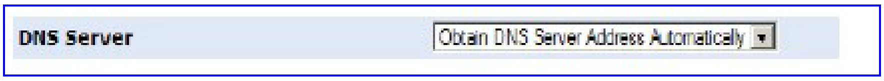
Use the 'Renew' button to renew the leased IP address. Use the Following IP Address Your WAN connection can be configured using a permanent (static) IP address. Your service provider should provide you with this IP address, subnet mask and the default Telephone Adapter IP address.

9.1.3 DNS Server

Domain Name System (DNS) is the method by which website or domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP.

To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 9-4: Obtain DNS Server Address Automatically

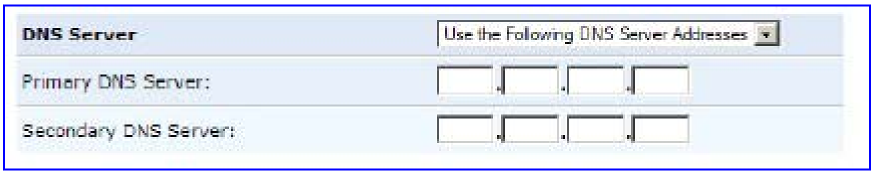


DNS Server: Obtain DNS Server Address Automatically

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (refer to the figure below).

Specify up to two different DNS server address, one primary, another secondary.

Figure 9-5: DNS Server Settings



DNS Server: Use the Following DNS Server Addresses

Primary DNS Server: . . .

Secondary DNS Server: . . .

9.1.4 Routing

You can choose to setup your Telephone Adapter to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

Table 9-2: Static or Dynamic Routing Parameters

Parameter	Description	
Routing	Select 'Advanced' or 'Basic' routing.	
Routing Mode	Select one of the following Routing modes:	
	Route	Use route mode if you want your Telephone Adapter to function as a router between two networks.
	NAPT	Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Parameter	Description
Device Metric	The device metric is a value used by the Telephone Adapter to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.
Default Route	Select this check box to define this device as a the default route.
Routing Information Protocol (RIP)	Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, select the following: Listen to RIP messages - select 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'. Send RIP messages select 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.
Multicast - IGMP Proxy Internal	IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. IGMP proxy enables the routing of multicast packets according to the IGMP requests of LAN devices asking to join multicast groups. Select the 'Multicast IGMP Proxy Internal' check-box to enable this feature.
Routing Table	Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.

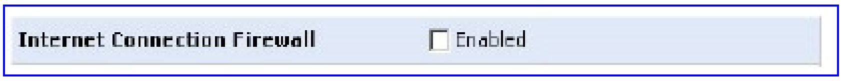
9.1.5 Advanced Routing Properties

Refer to "Routing" on page 86.

9.1.6 Internet Connection Firewall

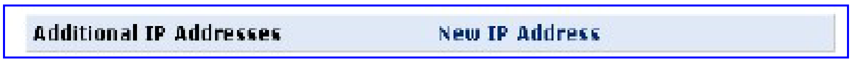
Your Telephone Adapter's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. For detailed information on your Telephone Adapter's security features, refer to "Security" on page 135.

Figure 9-6: Internet Connection Firewall



Internet Connection Firewall ☐ Enabled

Figure 9-7: Additional IP Addresses



Additional IP Addresses New IP Address

You can add alias names (additional IP addresses) to the Telephone Adapter by clicking the link 'New IP Address'. This enables you to access the Telephone Adapter using these aliases in addition to 192.168.1.1 and *http://MP202.home*.

9.2 WAN PPPoE

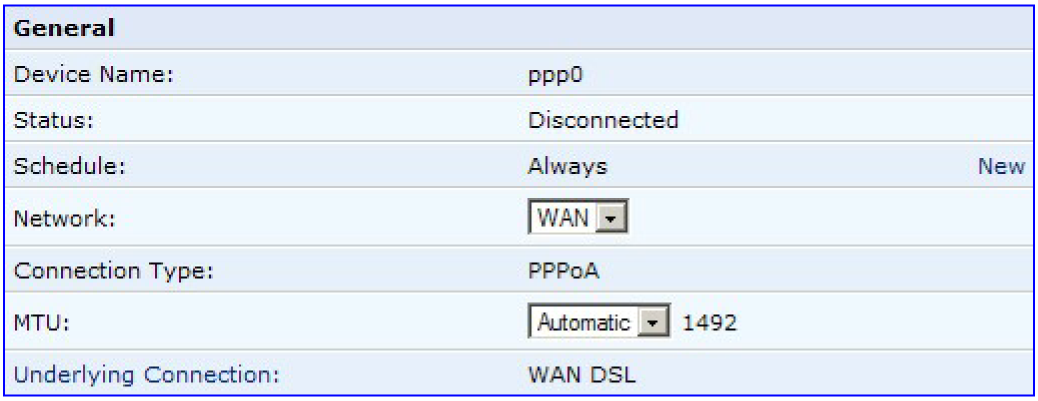
Point-to-Point Protocol over Ethernet (PPPoE) relies on two widely accepted standards, PPP and Ethernet. PPPoE enables your home network PCs that communicate on an Ethernet network to exchange information with PCs on the Internet. PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the normally multipoint architecture of Ethernet. A discovery process in PPPoE determines the Ethernet MAC address of the remote device in order to establish a session.

9.2.1 General

Table 9-3: PPPoE Parameter Descriptions

Parameter	Description
Schedule	You can configure scheduler rules in order to define time segments during which the connection is active (via Advanced>Scheduler Rules).
Network	Select whether the parameters you are configuring relate to a LAN/WAN connection, by selecting LAN/WAN from the drop down list.
MTU	MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The default setting, Manual, allows you to enter the largest packet size that will be transmitted. The recommended size, is 1492. You should leave this value in the 1200 to 1500 range. To have the Telephone Adapter select the best MTU for your Internet connection, select Automatic.
Underlying Connection	Specify the underlying connection above which the protocol will be initiated.

Figure 9-8: General PPPoE Settings



General

Device Name:	ppp0
Status:	Disconnected
Schedule:	Always New
Network:	WAN
Connection Type:	PPPoA
MTU:	Automatic 1492
Underlying Connection:	WAN DSL

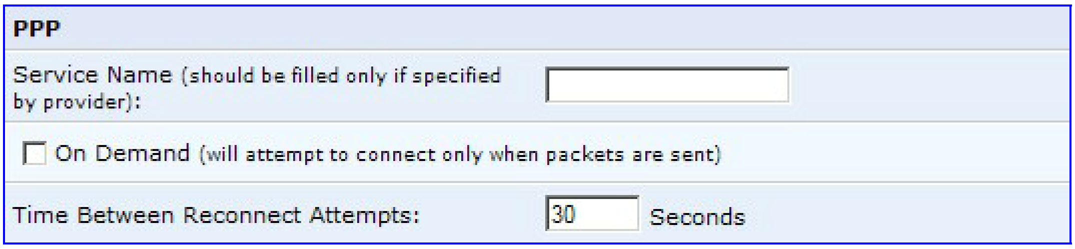
9.2.2 PPP Configuration

Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the Internet service provider. PPP supports authentication protocols such as PAP and CHAP, as well as other compression and encryption protocols.

Table 9-4: PPP Configuration Parameter Descriptions

Parameter	Description
Service Name	Specify the networking peer's service name, if provided by your ISP.
PPP-on-Demand	Use PPP on demand to initiate the point-to-point protocol session only when packets are actually sent over the Internet.
Time Between Reconnect Attempts	Specify the duration between PPP reconnected attempts, as provided by your ISP.

Figure 9-9: PPP Configuration



PPP

Service Name (should be filled only if specified by provider):

□ On Demand (will attempt to connect only when packets are sent)

Time Between Reconnect Attempts: 30 Seconds

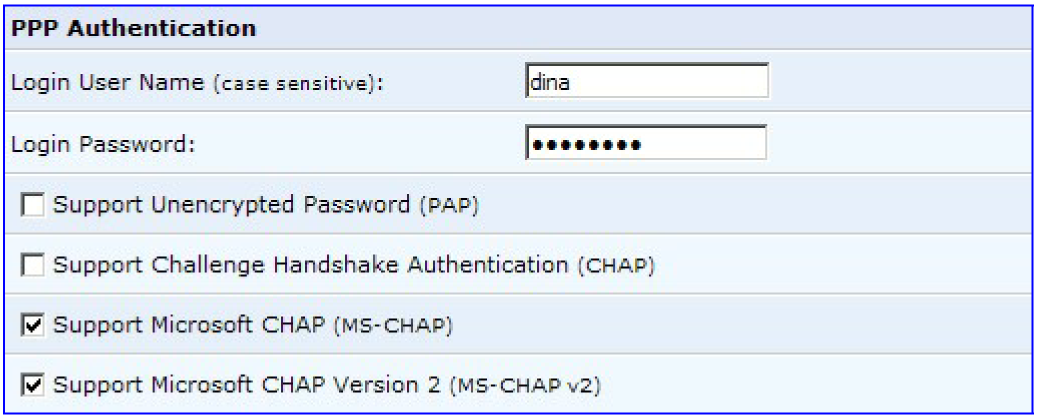
9.2.3 PPP Authentication

Point-to-Point Protocol (PPP) currently supports four authentication protocols:

1. Password Authentication Protocol (PAP)
2. Challenge Handshake Authentication Protocol (CHAP)
3. Microsoft CHAP version 1
4. Microsoft CHAP version 2

This section allows you to select the authentication protocols your gateway may use when negotiating with a PPTP server. Select all the protocols if no information is available about the server's authentication protocols. Note that encryption is performed only if 'Microsoft CHAP', 'Microsoft CHAP version 2', or both are selected.

Figure 9-10: PPP Authentication Settings



PPP Authentication

Login User Name (case sensitive): dina

Login Password: ••••••••

□ Support Unencrypted Password (PAP)

□ Support Challenge Handshake Authentication (CHAP)

☑ Support Microsoft CHAP (MS-CHAP)

☑ Support Microsoft CHAP Version 2 (MS-CHAP v2)

Table 9-5: PPP Authentication Parameter Descriptions

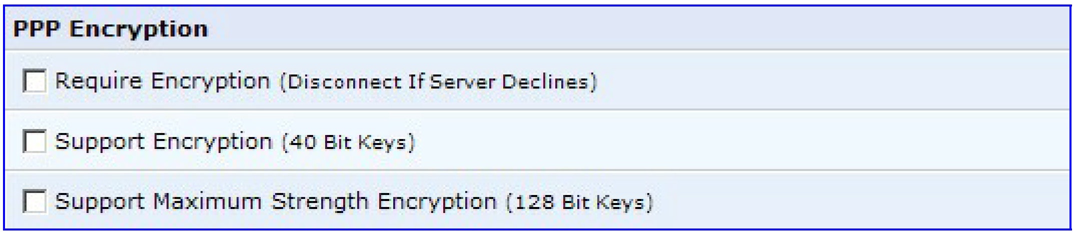
Parameter	Description
Login User Name	As agreed with ISP.
Login Password	As agreed with ISP.
Support Unencrypted Password (PAP)	Password Authentication Protocol (PAP) is a simple, plaintext authentication scheme. The user name and password are requested by your networking peer in plaintext. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.
Support Challenge Handshake Authentication (CHAP)	The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.
Support Microsoft CHAP	Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.
Support Microsoft CHAP Version 2	Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

9.2.4 PPP Encryption

PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically only one method is used in each direction of the link.

Note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication algorithms.

Figure 9-11: PPP Encryption



PPP Encryption

□ Require Encryption (Disconnect If Server Declines)

□ Support Encryption (40 Bit Keys)

□ Support Maximum Strength Encryption (128 Bit Keys)

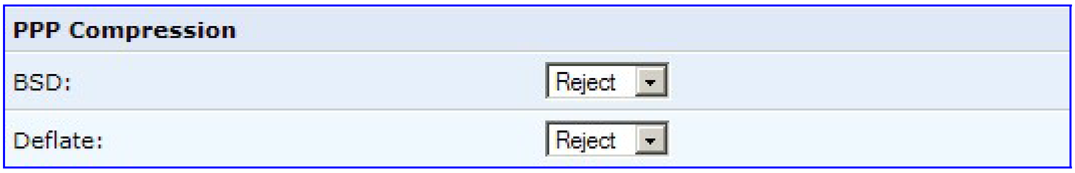
Table 9-6: PPP Encryption Parameter Descriptions

Parameter	Description
Require Encryption	Select this check box to ensure that the PPP connection is encrypted.
Support Encryption (40 Bit Keys)	Select this check box if your peer supports 40 bit encryption keys.
Support Maximum Strength Encryption (128 Bit Keys)	Select this check box if your peer supports 128 bit encryption keys.

9.2.5 PPP Compression

The PPP Compression Control Protocol (CCP) is responsible for configuring, enabling, and disabling data compression algorithms on both ends of the point-to-point link. It is also used to signal a failure of the compression/ decompression mechanism in a reliable manner.

Figure 9-12: PPP Compression



PPP Compression

BSD: Reject

Deflate: Reject

For each compression algorithm, select one of the following from the drop down menu:

Table 9-7: PPP Compression Parameter Descriptions

Parameter	Description
Reject	Reject PPP connections with peers that use the compression algorithm.
Allow	Allow PPP connections with peers that use the compression algorithm.
Require	Ensure a connection with a peer is using the compression algorithm.

9.2.6 Internet Protocol

Refer to "Internet Protocol Settings" on page 79

9.2.7 DNS Server

Refer to "DNS Server" on page 80.

9.2.8 Routing

Refer to "Routing" on page 80

9.2.9 Internet Connection Firewall

Refer to "Internet Connection Firewall" on page 81

9.3 WAN PPTP

Point-to-Point Tunneling Protocol (PPTP) is a protocol developed by Microsoft targeted at creating VPN connections over the Internet. This enables remote users to access the gateway via any ISP that supports PPTP on its servers. PPTP encapsulates network traffic, encrypts content using Microsoft's Point-to-Point Encryption (MPPE) protocol that is based on RC4, and routes using the generic routing encapsulation (GRE) protocol.

With your gateway, PPTP is targeted at serving two purposes:

1. Connecting the gateway to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established using user name and password authentication.
2. Connecting the gateway to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, using user name and password authentication.

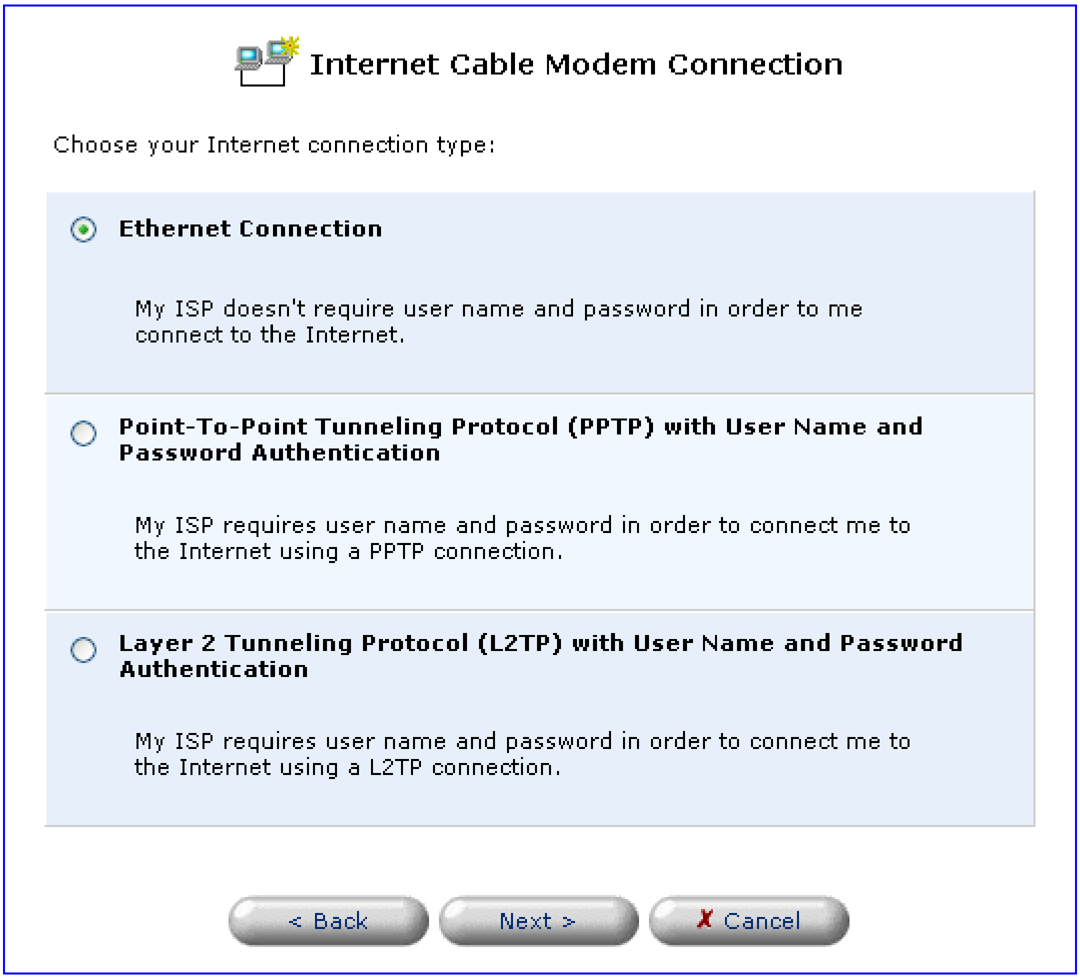
9.3.1 Creating a PPTP Connection with the Connection Wizard

➢ To create a new PPTP connection, take these steps:

1. Open the screen 'Network Connections' and click the link 'New Connection'; the 'Connection Wizard' screen opens.
2. Select the radio button 'Internet Connection' and click 'Next'; the screen 'Internet Connection' opens.

3. Select the radio button External Cable Modem (this option is for both internal and external cable modems) and click 'Next'; the screen 'Internet Cable Modem Connection' opens (refer to the figure).

Figure 9-13: Internet Cable Modem Connection



Internet Cable Modem Connection

Choose your Internet connection type:

● **Ethernet Connection**

My ISP doesn't require user name and password in order to me connect to the Internet.

○ **Point-To-Point Tunneling Protocol (PPTP) with User Name and Password Authentication**

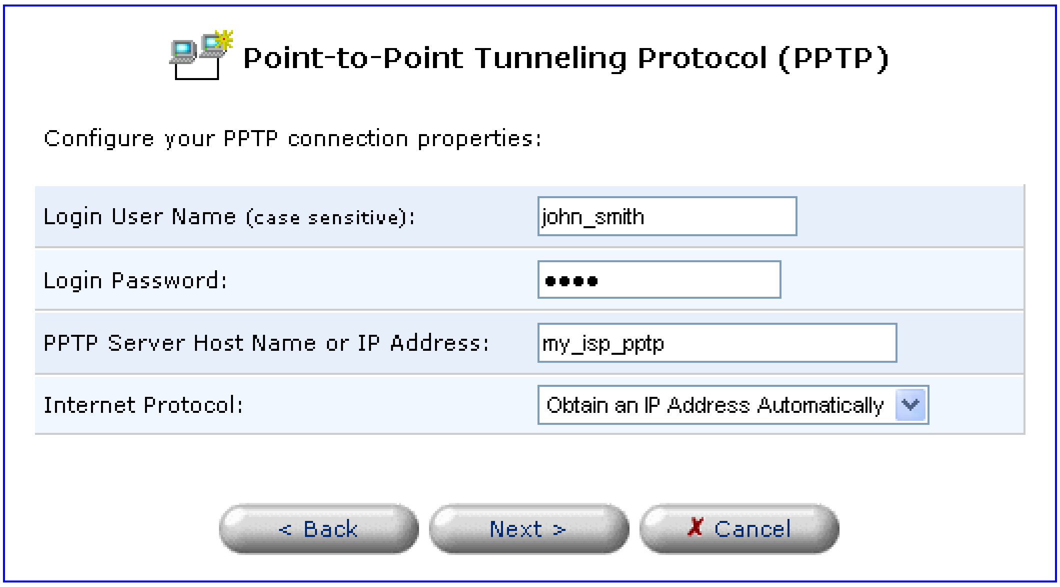
My ISP requires user name and password in order to connect me to the Internet using a PPTP connection.

○ **Layer 2 Tunneling Protocol (L2TP) with User Name and Password Authentication**

My ISP requires user name and password in order to connect me to the Internet using a L2TP connection.

4. Select the radio button 'Point-To-Point Tunneling Protocol (PPTP) with User Name and Password Authentication' and click Next; the screen 'Point-to-Point Tunneling Protocol (PPTP)' opens (refer to the figure).

Figure 9-14: Point-to-Point Tunneling Protocol



Point-to-Point Tunneling Protocol (PPTP)

Configure your PPTP connection properties:

Login User Name (case sensitive):	john_smith
Login Password:	●●●●
PPTP Server Host Name or IP Address:	my_isp_pptp
Internet Protocol:	Obtain an IP Address Automatically

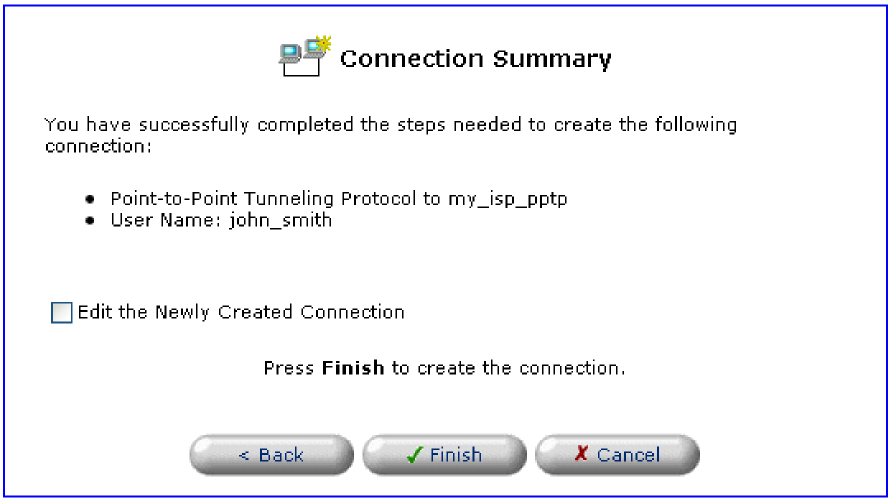
5. Enter the username and password provided by your Internet Service Provider (ISP).

6. Enter the PPTP server host name or IP address provided by your ISP.

7. Select whether to obtain an IP address automatically or specify one.

8. Click Next; the screen 'Connection Summary' opens (refer to the figure).

Figure 9-15: Connection Summary



Connection Summary

You have successfully completed the steps needed to create the following connection:

- Point-to-Point Tunneling Protocol to my_isp_pptp
- User Name: john_smith

□ Edit the Newly Created Connection

Press **Finish** to create the connection.

9. Check the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking Finish.

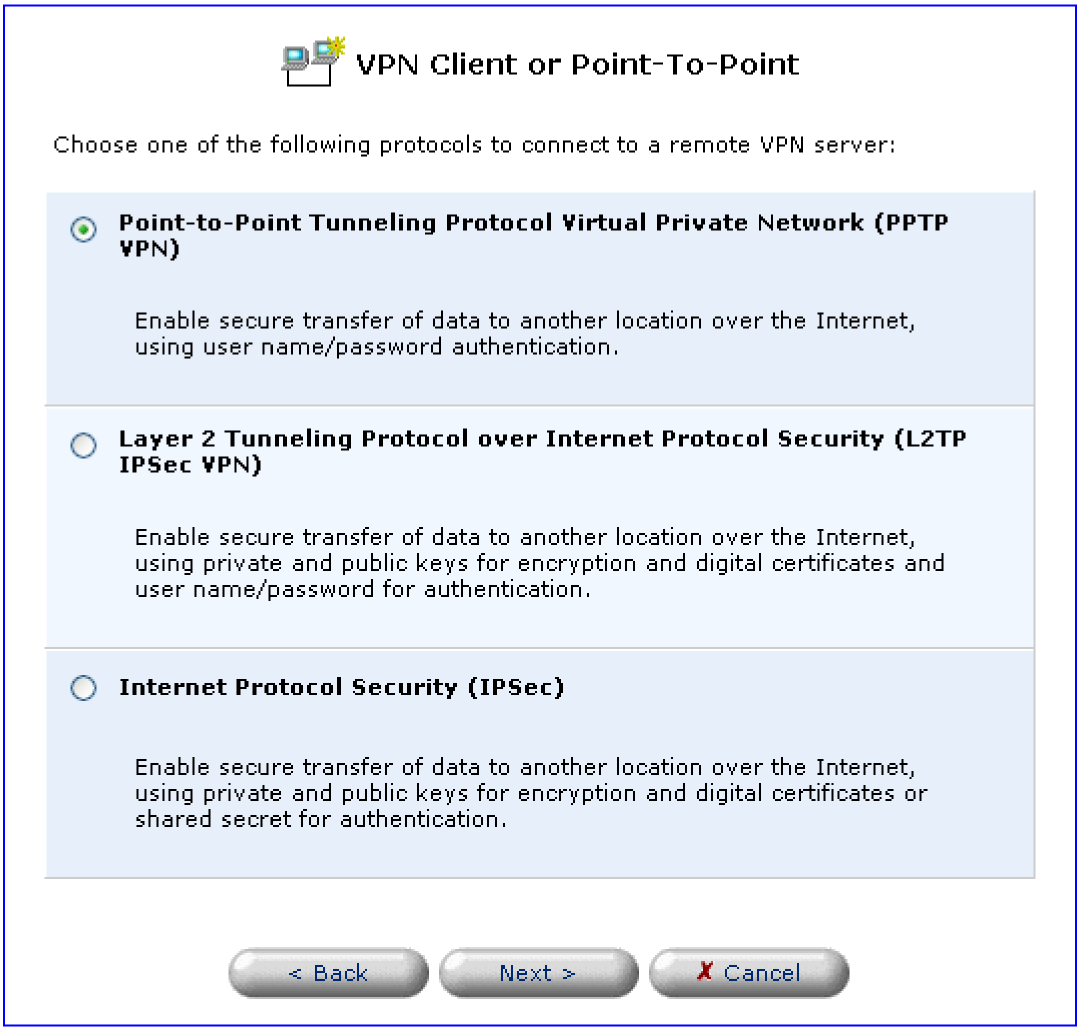
10. Click Finish to save the settings; the new PPTP connection is added to the network connections list and is configurable like any other connection.

9.3.2 Creating a PPTP VPN Connection with the Connection Wizard

➢ To create a new PPTP VPN connection, take these steps:

1. Open the screen 'Network Connections' and click link 'New Connection'; the screen 'Connection Wizard' opens.
2. Select the radio button 'Connect to a Virtual Private Network over the Internet' and click 'Next'; the screen 'Connect to a Virtual Private Network over the Internet' opens.
3. Select the radio button 'VPN Client or Point-To-Point' and click 'Next'; the screen 'VPN Client or Point-To-Point' opens (refer to the figure).

Figure 9-16: VPN Client or Point-To-Point



VPN Client or Point-To-Point

Choose one of the following protocols to connect to a remote VPN server:

● **Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)**

Enable secure transfer of data to another location over the Internet, using user name/password authentication.

○ **Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)**

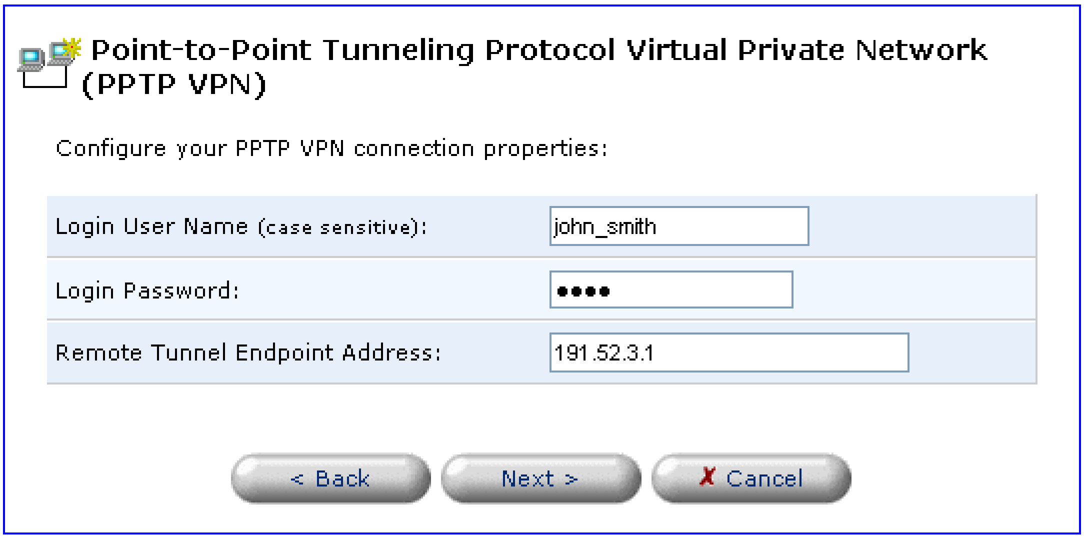
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates and user name/password for authentication.

○ **Internet Protocol Security (IPSec)**

Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates or shared secret for authentication.

4. Select the 'Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)' radio button and click Next. The 'Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)' screen will appear (see figure 8.205).

Figure 9-17: Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)



Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)

Configure your PPTP VPN connection properties:

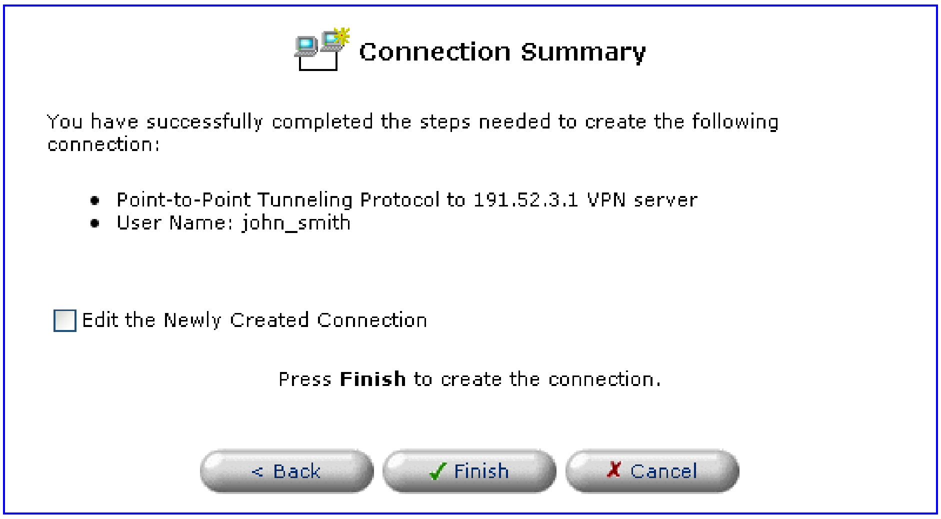
Login User Name (case sensitive):	john_smith
Login Password:	●●●●
Remote Tunnel Endpoint Address:	191.52.3.1

5. Enter the username and password provided by the administrator of the network you are trying to access.

6. Enter the remote tunnel endpoint address. This would be the IP address or domain name of the remote network computer, which serves as the tunnel's endpoint.

7. Click 'Next'; the screen 'Connection Summary' opens (refer to the figure).

Figure 9-18: Connection Summary



Connection Summary

You have successfully completed the steps needed to create the following connection:

- Point-to-Point Tunneling Protocol to 191.52.3.1 VPN server
- User Name: john_smith

□ Edit the Newly Created Connection

Press **Finish** to create the connection.

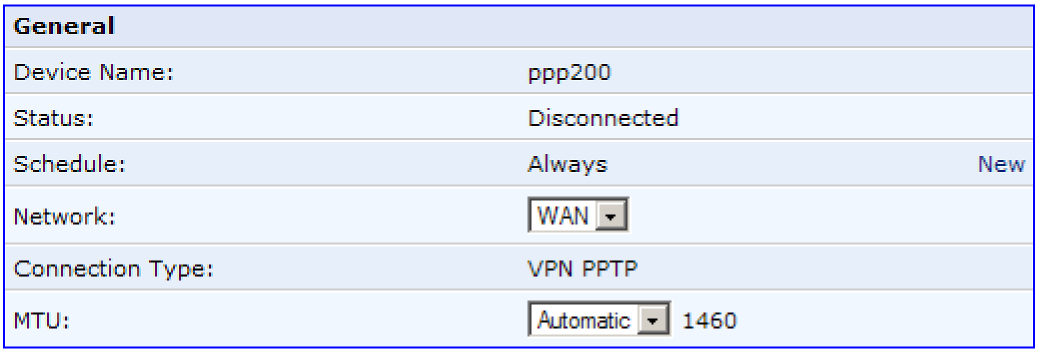
8. Check the check box 'Edit the Newly Created Connection' if you wish to be routed to the new connection's configuration screen after clicking Finish.

9. Click Finish to save the settings; the new PPTP VPN connection is added to the network connections list and is configurable like any other connection.

9.3.3 General

This section displays the connection's general parameters.

Figure 9-19: General PPTP Settings



General		
Device Name:	ppp200	
Status:	Disconnected	
Schedule:	Always	New
Network:	WAN	
Connection Type:	VPN PPTP	
MTU:	Automatic 1460	

Table 9-8: General PPTP Settings

Parameter	Description
Schedule	By default, the connection is always active. However, you can configure scheduler rules (via Advanced>Scheduler Rules) in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, this field changes to a drop-down list, allowing you to choose between the available rules.
Network	Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down list.
MTU	MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to its default (Automatic), the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' for the DHCP to determine the MTU. If you select 'Manual', it is recommended to enter a value in the range of 1200 to 1500.

9.3.4 PPP Configuration

Refer to "PPP Configuration" on page 82

9.3.5 PPP Authentication

Refer to "PPP Authentication" on page 83

9.3.6 PPP Encryption

Refer to "PPP Encryption" on page 84

9.3.7 Internet Protocol

Refer to "Internet Protocol Settings" on page 79

9.3.8 DNS Server

Refer to "DNS Server" on page 80

9.3.9 Routing

Refer to "Routing" on page 80

9.3.10 Internet Connection Firewall

Refer to "Internet Connection Firewall" on page 81

9.4 WAN L2TP

Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol, enabling your gateway to create VPN connections. Derived from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP Remote Access Concentrator (LAC). The LAC transmits the L2TP packets over the network to the L2TP Network Server (LNS) at the corporate side.

With your gateway, L2TP is targeted at serving two purposes:

1. Connecting the gateway to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established using user name and password authentication.

2. Connecting the gateway to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates, and user name and password for authentication.

9.4.1 Creating an L2TP IPSec VPN Connection with the Connection Wizard

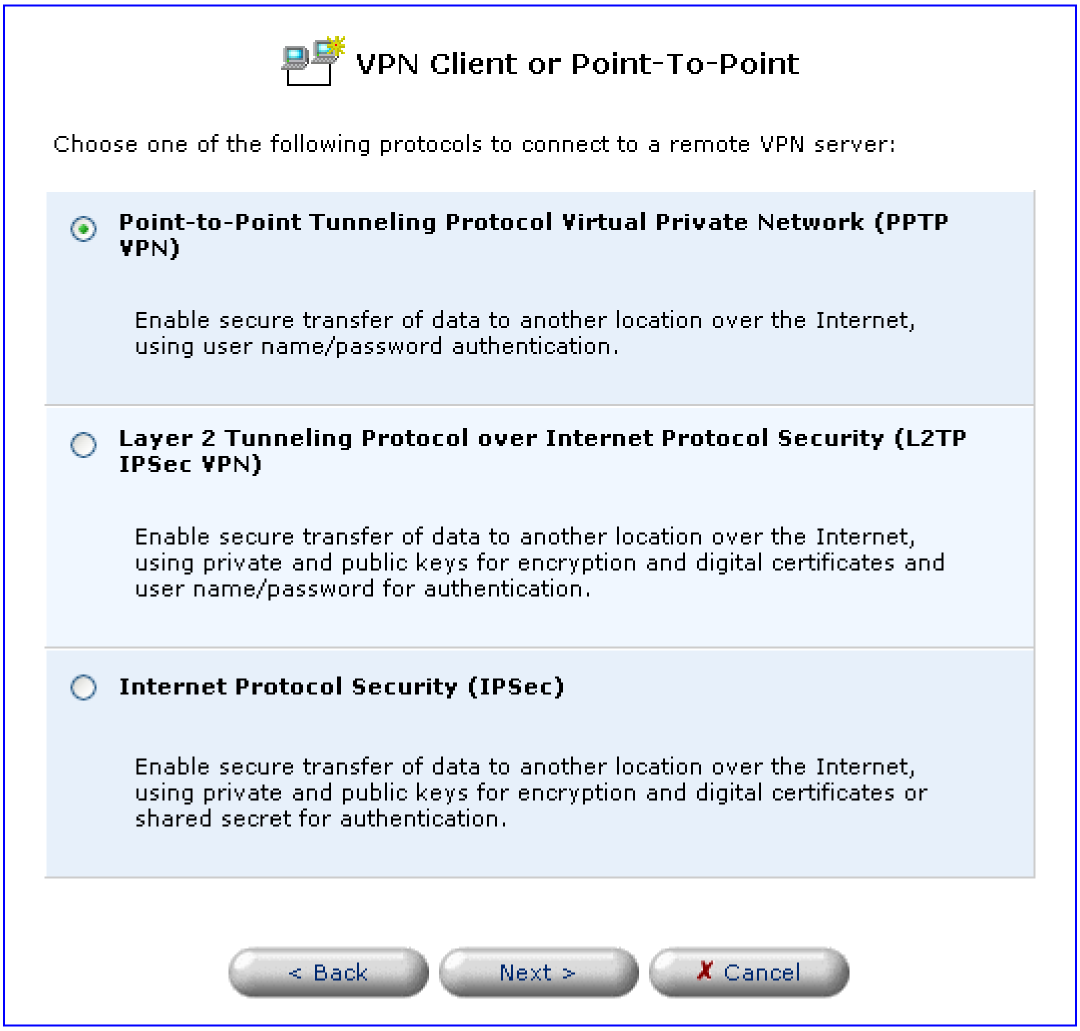
➢ To create a new L2TP IPSec VPN connection, take these steps:

1. Click the link 'New Connection' in the screen 'Network Connections'; the screen 'Connection Wizard' opens.

2. Select the radio button 'Connect to a Virtual Private Network over the Internet' and click 'Next'; the screen 'Connect to a Virtual Private Network over the Internet' opens.

3. Select the radio button 'VPN Client or Point-To-Point' and click 'Next'; the screen 'VPN Client or Point-To-Point' opens(refer to the figure).

Figure 9-20: VPN Client or Point-To-Point



VPN Client or Point-To-Point

Choose one of the following protocols to connect to a remote VPN server:

● **Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)**

Enable secure transfer of data to another location over the Internet, using user name/password authentication.

○ **Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)**

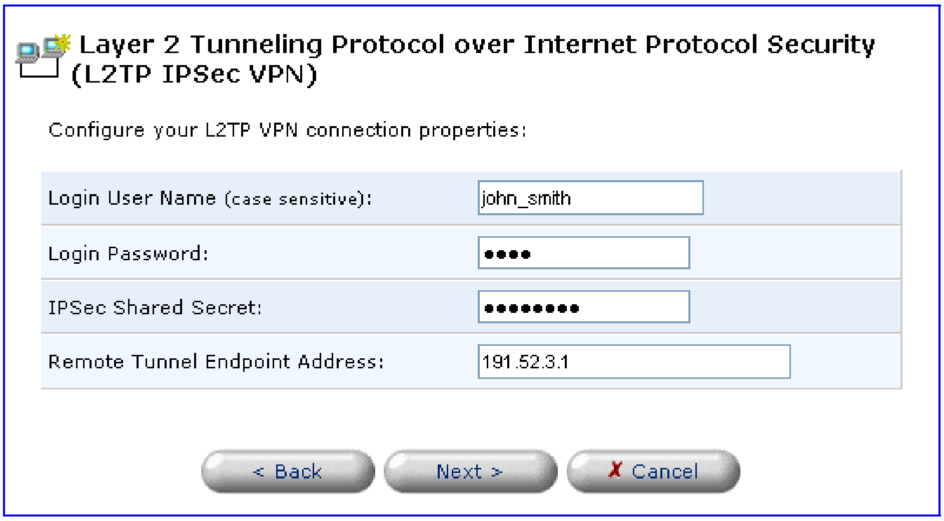
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates and user name/password for authentication.

○ **Internet Protocol Security (IPSec)**

Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates or shared secret for authentication.

4. Check the radio button 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)' and click 'Next'; the screen 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)' opens (refer to the figure).

Figure 9-21: Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)



Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)

Configure your L2TP VPN connection properties:

Login User Name (case sensitive):	john_smith
Login Password:	●●●●
IPSec Shared Secret:	●●●●●●●●
Remote Tunnel Endpoint Address:	191.52.3.1

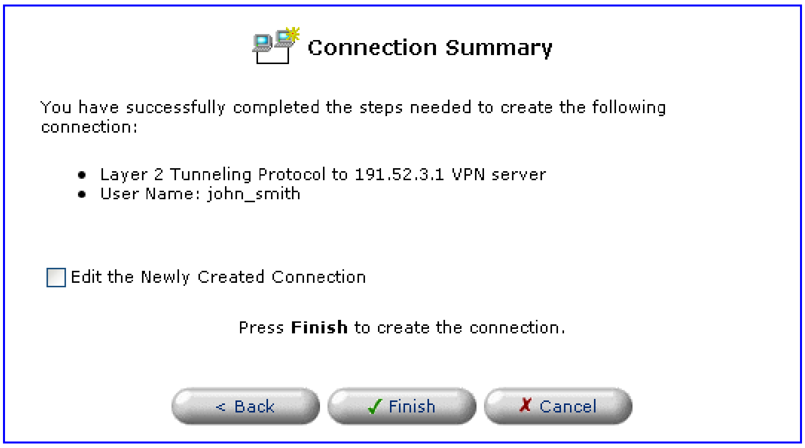
5. Enter the username and password provided by the administrator of the network you are trying to access.

6. Enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.

7. Enter the remote tunnel endpoint address. This would be the IP address or domain name of the remote network computer, which serves as the tunnel's endpoint.

8. Click 'Next'; the screen 'Connection Summary' opens (refer to the figure).

Figure 9-22: Connection Summary



Connection Summary

You have successfully completed the steps needed to create the following connection:

- Layer 2 Tunneling Protocol to 191.52.3.1 VPN server
- User Name: john_smith

□ Edit the Newly Created Connection

Press **Finish** to create the connection.

9. Check the check box 'Edit the Newly Created Connection' to be routed to the new connection's configuration screen after clicking 'Finish'.

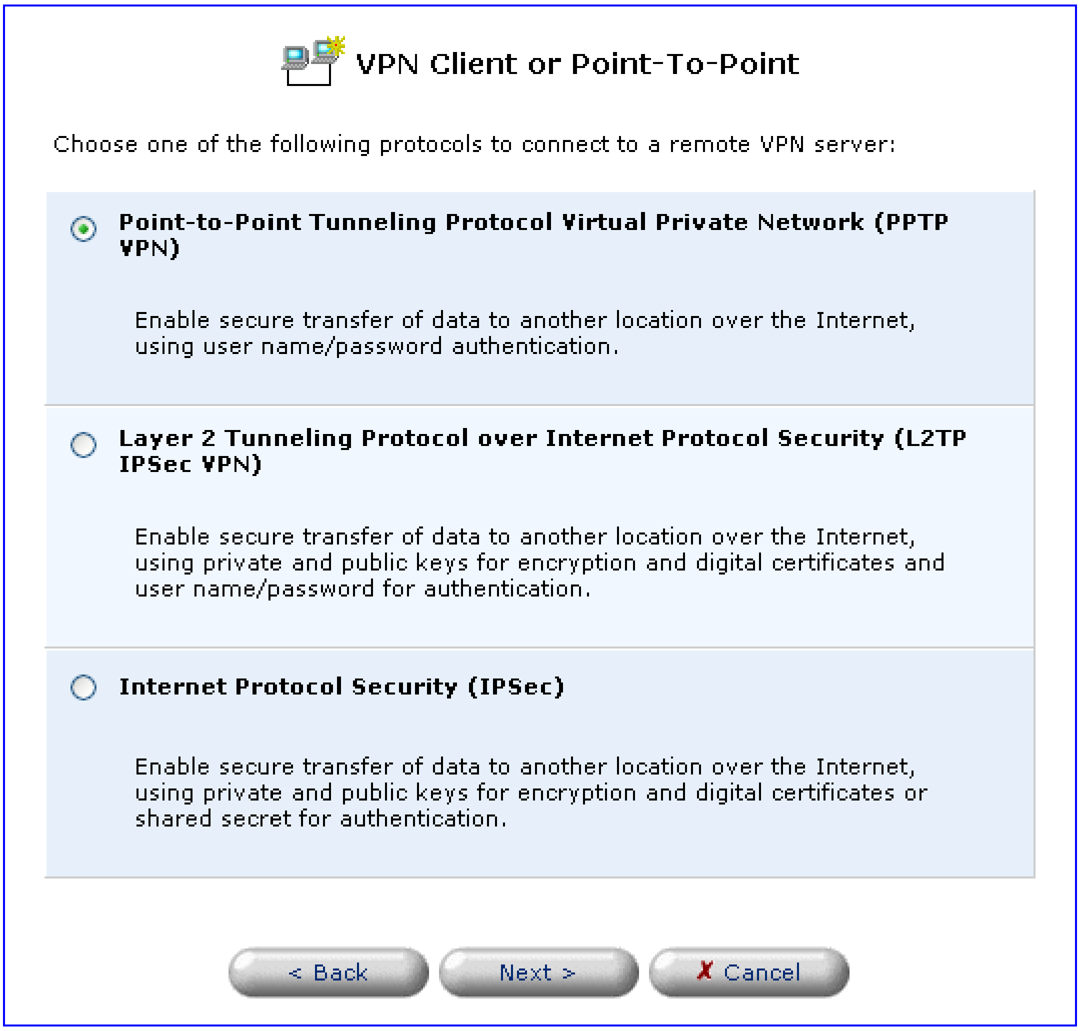
10. Click 'Finish' to save the settings; the new L2TP IPSec VPN connection is added to the network connections list and is configurable like any other connection.

9.4.2 Creating an L2TP IPSec VPN Connection with the Connection Wizard

➢ To create a new L2TP IPSec VPN connection, take these steps:

1. Click the link 'New Connection' in the screen 'Network Connections'; the screen 'Connection Wizard' opens.
2. Select the radio button 'Connect to a Virtual Private Network over the Internet' and click 'Next'; the screen 'Connect to a Virtual Private Network over the Internet' opens.
3. Select the radio button 'VPN Client or Point-To-Point' and click 'Next'; the screen 'VPN Client or Point-To-Point' opens (refer to the figure).

Figure 9-23: VPN Client or Point-To-Point



VPN Client or Point-To-Point

Choose one of the following protocols to connect to a remote VPN server:

● **Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)**

Enable secure transfer of data to another location over the Internet, using user name/password authentication.

○ **Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)**

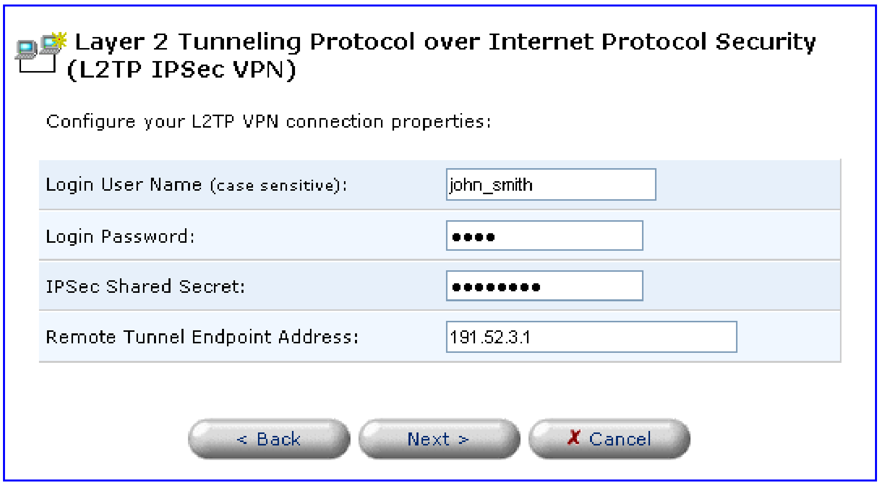
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates and user name/password for authentication.

○ **Internet Protocol Security (IPSec)**

Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates or shared secret for authentication.

4. Select the radio button 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)' and click 'Next'; the screen 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)' opens (refer to the figure).

Figure 9-24: Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)



Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)

Configure your L2TP VPN connection properties:

Login User Name (case sensitive):	john_smith
Login Password:	••••
IPSec Shared Secret:	••••••••
Remote Tunnel Endpoint Address:	191.52.3.1

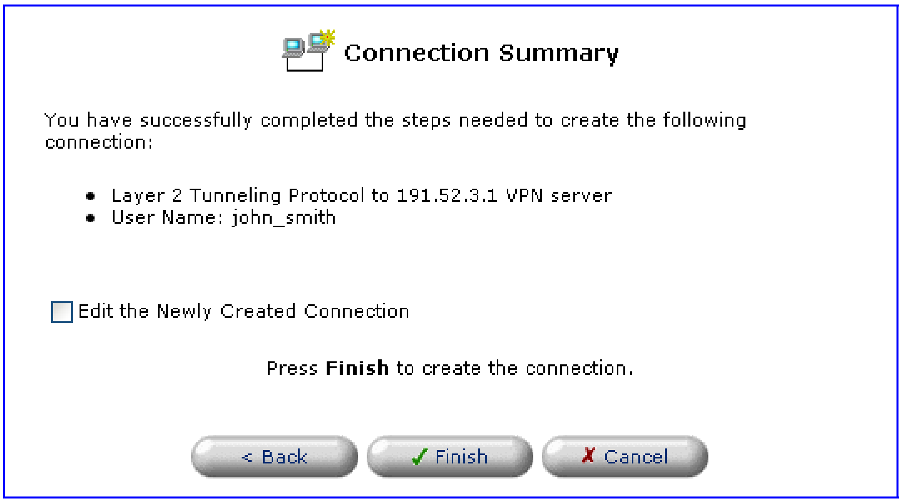
5. Enter the username and password provided by the administrator of the network you are trying to access.

6. Enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.

7. Enter the remote tunnel endpoint address. This would be the IP address or domain name of the remote network computer, which serves as the tunnel's endpoint.

8. Click Next. The 'Connection Summary' screen will appear (see figure 8.184).

Figure 9-25: Connection Summary



Connection Summary

You have successfully completed the steps needed to create the following connection:

- Layer 2 Tunneling Protocol to 191.52.3.1 VPN server
- User Name: john_smith

□ Edit the Newly Created Connection

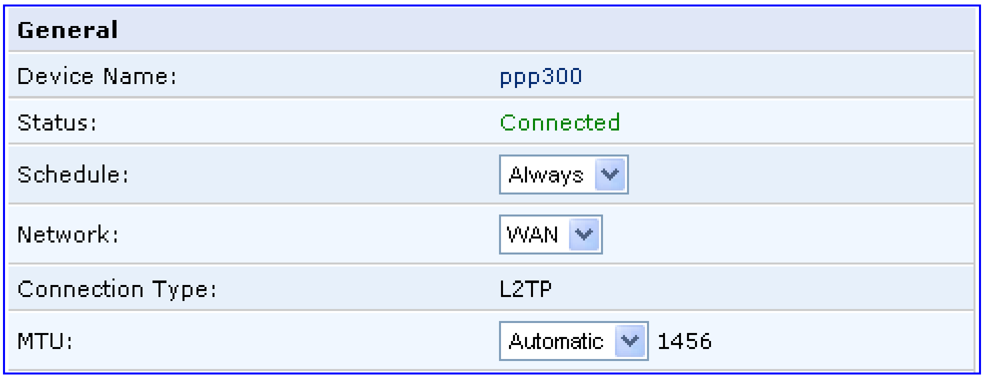
Press **Finish** to create the connection.

9. Check the check box 'Edit the Newly Created Connection' to be routed to the new connection's configuration screen after clicking 'Finish'.

10. Click 'Finish' to save the settings; the new L2TP IPSec VPN connection is added to the network connections list; it is configurable like any other connection.

9.4.3 General

This section displays the connection's general parameters.



General	
Device Name:	ppp300
Status:	Connected
Schedule:	Always
Network:	WAN
Connection Type:	L2TP
MTU:	Automatic 1456

Table 9-9: General Settings

Parameter	Description
Schedule	By default, the connection is always active. However, you can configure scheduler rules (via Advanced>Scheduler Rules) in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, this field changes to a drop-down list, allowing you to choose between the available rules.
Network	Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down list.
MTU	MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to its default (Automatic), the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' for the DHCP to determine the MTU. If you select 'Manual', it is recommended to enter a value in the range of 1200 to 1500.

9.4.4 PPP Configuration

Refer to "PPP Configuration" on page 82

9.4.5 PPP Authentication

Refer to "PPP Authentication" on page 83

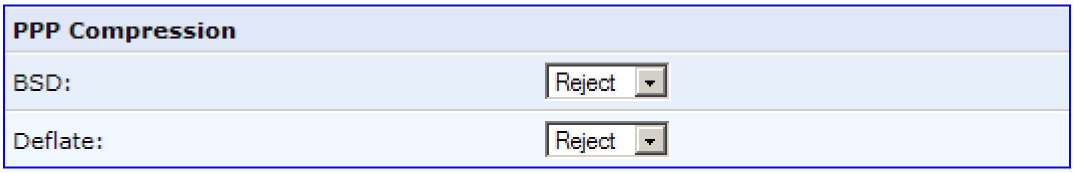
9.4.6 PPP Encryption

Refer to "PPP Encryption" on page 84

9.4.7 PPP Compression

The PPP Compression Control Protocol (CCP) is responsible for configuring, enabling, and disabling data compression algorithms on both ends of the point-to-point link. It is also used to signal a failure of the compression/ decompression mechanism in a reliable manner.

Figure 9-26: PPP Compression



PPP Compression

BSD: Reject

Deflate: Reject

For each compression algorithm, select one of the following from the drop down menu:

Table 9-10: PPTP Compression Parameters

Parameter	Description
Reject	Reject PPP connections with peers that use the compression algorithm.
Allow	Allow PPP connections with peers that use the compression algorithm.
Require	Ensure a connection with a peer is using the compression algorithm.

9.4.8 Internet Protocol

Refer to "Internet Protocol Settings" on page 79

9.4.9 DNS Server

Refer to "DNS Server" on page 80

9.4.10 Routing

Refer to "Routing" on page 80

9.4.11 Internet Connection Firewall

Refer to "Internet Connection Firewall" on page 81

10 VLAN and Bridge Settings

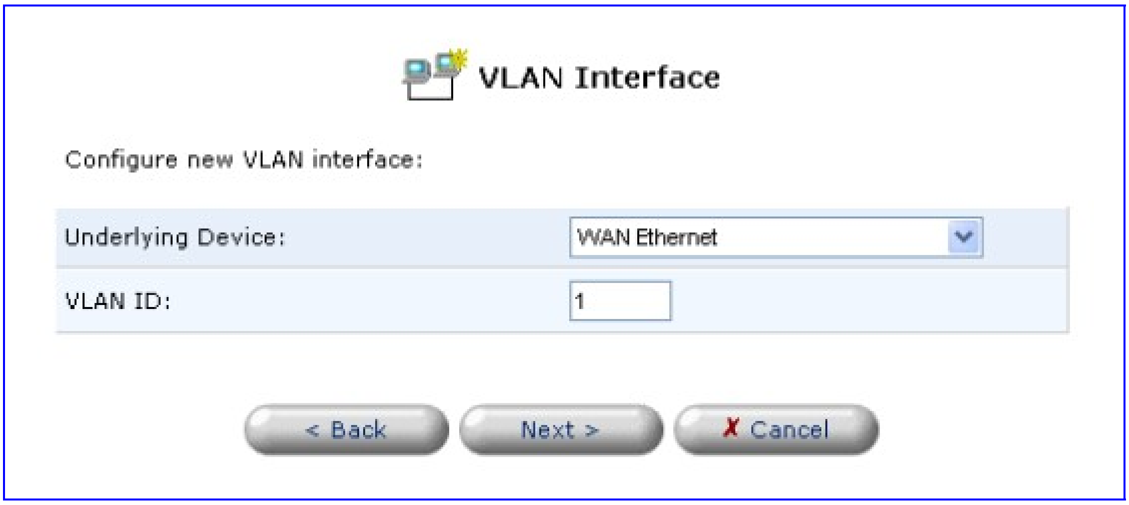
10.1 Virtual LAN Interface (VLAN)

10.1.1 Creation with the Connection Wizard

➢ **To create a new VLAN interface:**

1. Click the New Connection link in the 'Network Connections' screen (refer to the figure); the 'Connection Wizard' screen opens (refer to the figure).
2. Select the Advanced Connection radio button and click Next; the 'Advanced Connection' screen appears (refer to the figure).
3. Select the VLAN Interface radio button and click Next. The 'VLAN Interface' screen appears (refer to the figure).

Figure 10-1: VLAN Interface



VLAN Interface

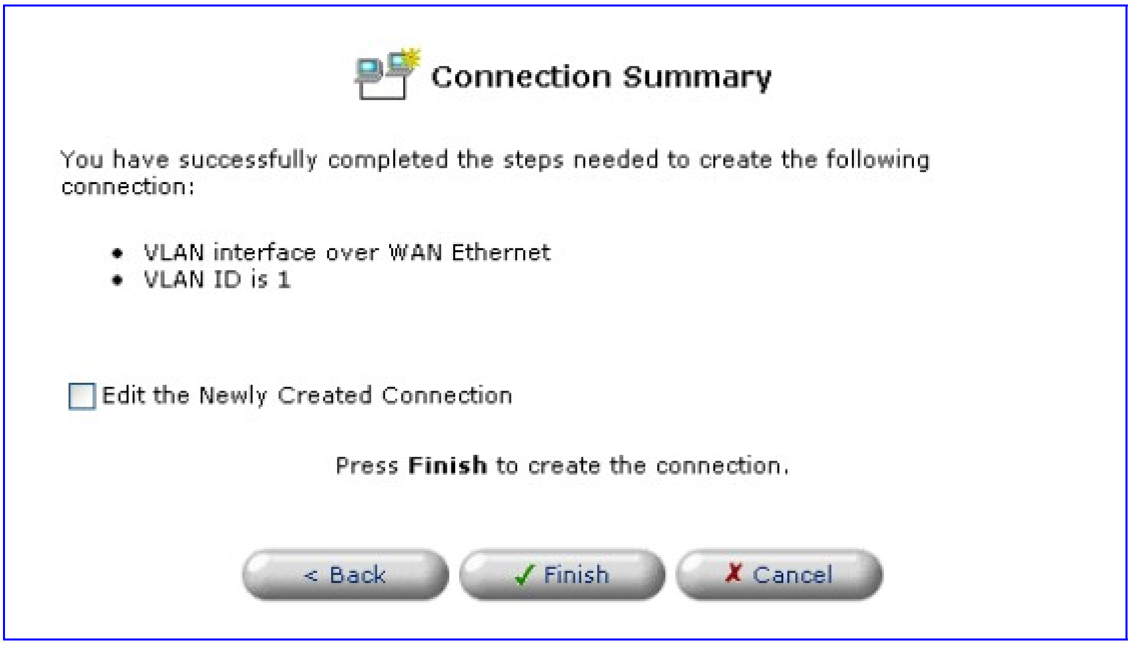
Configure new VLAN interface:

Underlying Device:	WAN Ethernet
VLAN ID:	1

4. Select the underlying device for this interface. The combo box displays the device's Ethernet connections.

5. Enter a value that will serve as the VLAN ID, and click Next; the 'Connection Summary' screen appears (refer to the figure).

Figure 10-2: Connection Summary



Connection Summary

You have successfully completed the steps needed to create the following connection:

- VLAN interface over WAN Ethernet
- VLAN ID is 1

□ Edit the Newly Created Connection

Press **Finish** to create the connection.

6. Check the 'Edit the Newly Created Connection' check box to be routed to the new connection's configuration screen after clicking Finish.

7. Click Finish to save the settings; the new VLAN interface is added to the network connections list; it’s configurable like any other connection.

10.1.2 General

The top part of the configuration window displays general communication parameters. It’s recommended to leave the values in this screen at their defaults unless you’re familiar with the networking concepts they represent. Since your Telephone Adapter is configured to operate with the default values, no parameter modification is necessary. You can configure the following general connection settings:

Table 10-1: VLAN Interface - General Communication Parameters

Parameter	Description
Schedule	By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined (via Advanced>Scheduler Rules), this field changes to a combo box, allowing you to choose between the available rules. To configure scheduler rules, refer to Section 10.11.
Network	Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the combo box. For detailed information, refer to Section 4.2.
Physical Address	The physical address of the network card used for your network. Some cards allow you to change this address.
Clone MAC	Allows you to copy the current MAC address of your PC to the MAC address of this device.
MTU	MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the Telephone Adapter selects the best MTU for your Internet connection. In case you change to manual, you can enter the largest packet size, you should leave this value in the 1200 to 1500 range.
Underlying Connection	The Ethernet device that the connection is implemented over.

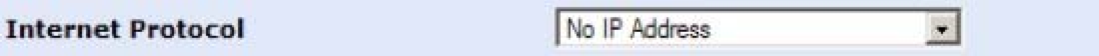
Select one of the following Internet Protocol options from the 'Internet Protocol' drop down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that according to the selection you make in the 'Internet Protocol' drop down menu, the screen will refresh and display relevant configuration settings.

No IP Address	Select 'No IP Address' if you require that your Telephone Adapter has no IP address. This can be useful if you are working in an environment where you are not connected to other networks, such as the Internet.

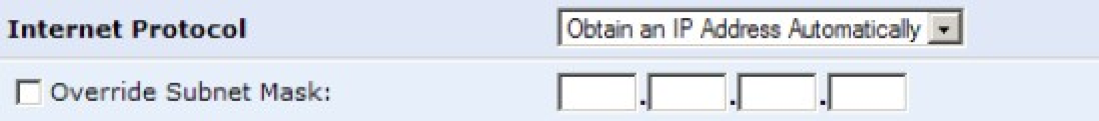
Figure 10-3: Internet Protocol Settings - No IP Address



Internet Protocol	No IP Address

Obtain an IP Address Automatically	Your WAN connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports DHCP, or if you are connecting using a dynamic IP address. The server that assigns the Telephone Adapter with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead. You can press the 'Release' button to release the current leased IP address. Once the address has been released, the button text changes to 'Renew'. Use the 'Renew' button to renew the leased IP address.

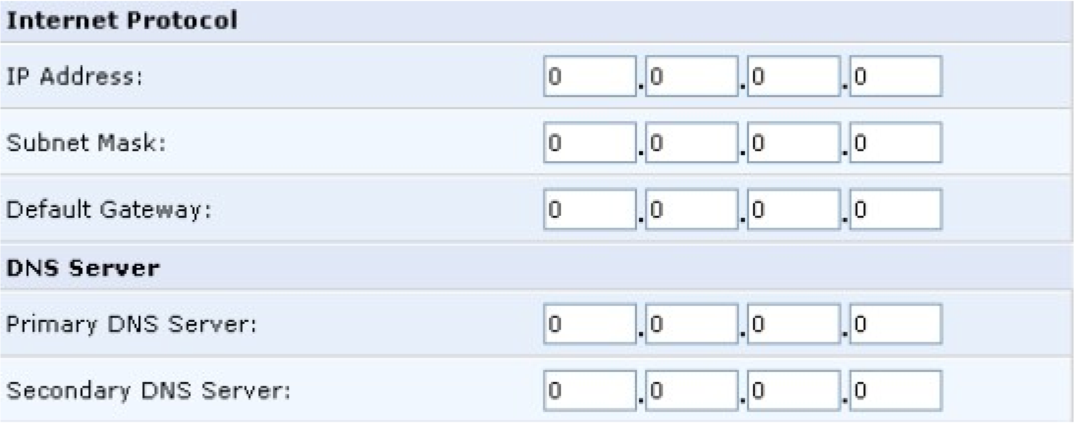
Figure 10-4: Internet Protocol Settings - Automatic IP



Internet Protocol	Obtain an IP Address Automatically
□ Override Subnet Mask:	. . .

Use the Following IP Address	Your WAN connection can be configured using a permanent (static) IP address. Your service provider should provide you with this IP address, subnet mask and the default Telephone Adapter IP address.

Figure 10-5: Internet Protocol Settings . Static IP



Internet Protocol	
IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Default Gateway:	0 . 0 . 0 . 0
DNS Server	
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

10.1.3 IP Address Distribution

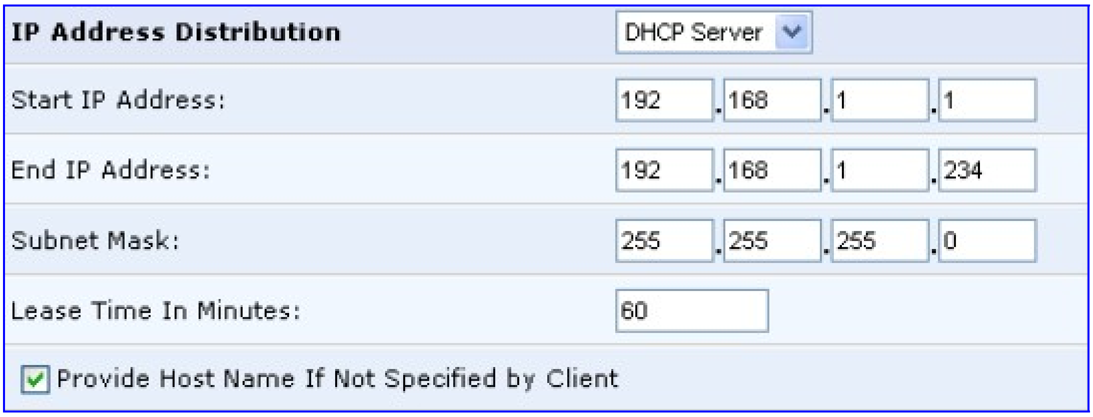
The 'IP Address Distribution' section allows you to configure the device's Dynamic Host Configuration Protocol (DHCP) server parameters. The DHCP automatically assigns IP addresses to network PCs. If you enable this feature, make sure that you also configure your network PCs as DHCP clients. For a comprehensive description of this feature, refer to Section 10.28.

Select one of the following options from the 'IP Address Distribution' combo box:

Table 10-2: IP Address Distribution Parameters

Parameter	Description
DHCP Server	Start IP Address The first IP address that may be assigned to a LAN host. Since the device's default IP address is 192.168.2.1, this address must be 192.168.2.2 or greater.
End IP Address	The last IP address in the range that can be used to automatically assign IP addresses to LAN hosts.
Subnet Mask	A mask used to determine to what subnet an IP address belongs. An example of a subnet mask value is 255.255.0.0.
Lease Time In Minutes	Each device will be assigned an IP address by the DHCP server for a this amount of time, when it connects to the network. When the lease expires the server will determine if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use will become available for other computers on the network.
Provide Host Name If Not Specified by Client	If the DHCP client does not have a host name, the device will automatically assign one for him.

Figure 10-6: IP Address Distribution - DHCP Server



IP Address Distribution	DHCP Server
Start IP Address:	192 . 168 . 1 . 1
End IP Address:	192 . 168 . 1 . 234
Subnet Mask:	255 . 255 . 255 . 0
Lease Time In Minutes:	60

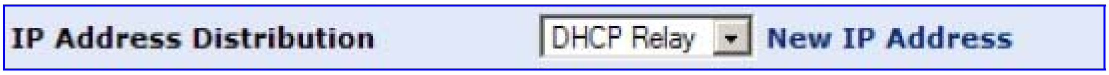
☑ Provide Host Name If Not Specified by Client

Table 10-3: DHCP Relay

DHCP Relay	Your device can act as a DHCP relay in case you would like to dynamically assign IP addresses from a DHCP server other than your Telephone Adapter's DHCP server. Note that when selecting this option you must also change the device's WAN to work in routing mode. For detailed information, refer to Section 10.28.2.

1. After selecting 'DHCP Relay' from the drop down menu, a 'New IP Address' link appears:

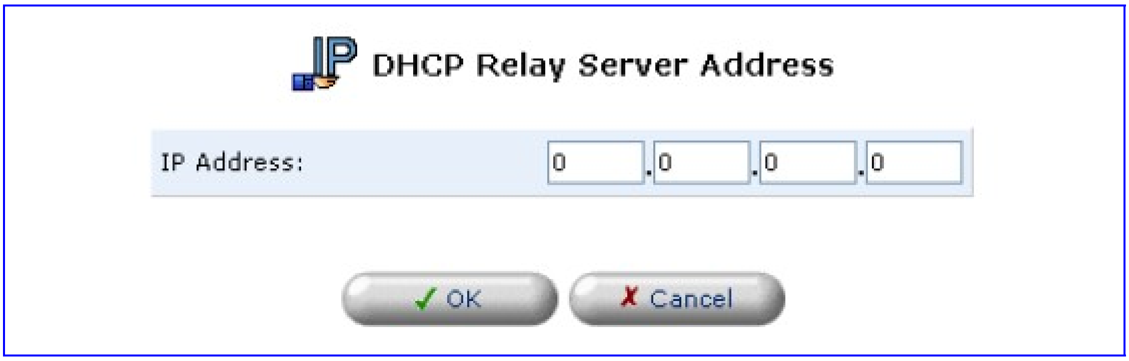
Figure 10-7: IP Address Distribution - DHCP Relay



IP Address Distribution DHCP Relay New IP Address

2. Click the 'New IP Address' link. The 'DHCP Relay Server Address' screen appears:

Figure 10-8: DHCP Relay Server Address



DHCP Relay Server Address

IP Address: 0 . 0 . 0 . 0

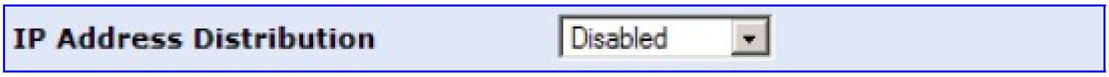
3. Specify the IP address of the DHCP server.

4. Click 'OK' to save the settings.

Table 10-4: Assigning Static IP Addresses to Network Computers

Disabled	Select 'Disabled' from the drop-down list to statically assign IP addresses to your network computers.

Figure 10-9: IP Address Distribution - Disable DHCP



IP Address Distribution Disabled

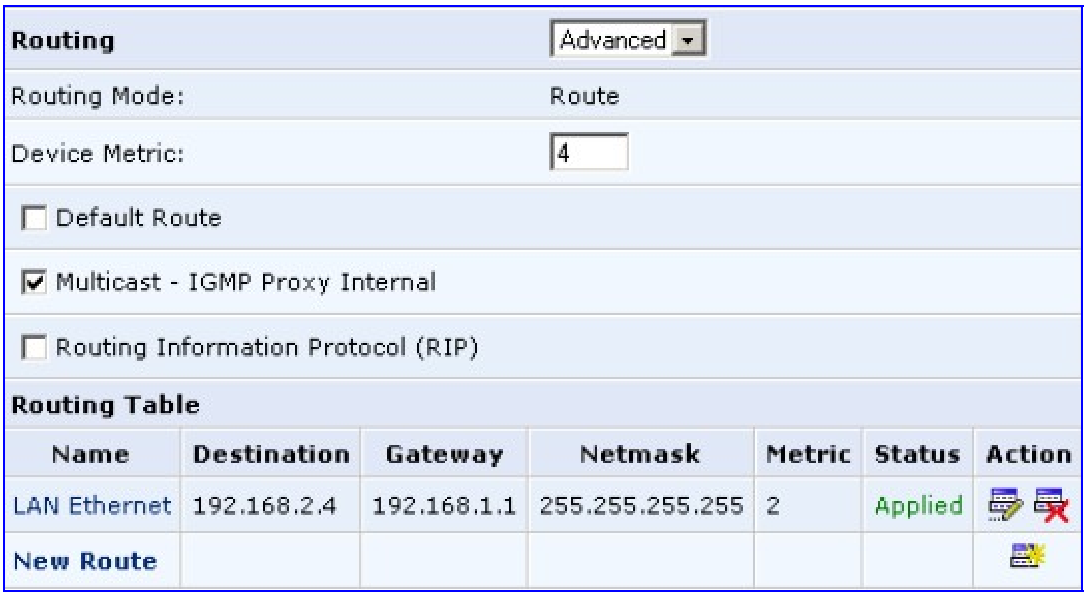
10.1.4 Routing

You can choose to setup your Telephone Adapter to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

Table 10-5: Routing Parameters

Parameter	Description
Routing	Select 'Advanced' or 'Basic' routing.
Routing Mode	Select one of the following Routing modes:
Route	Use route mode if you want your device to function as a router between two networks.
NAT	Network Address Translation (NAT) translates IP addresses to a valid, public address on the Internet. This adds security since internal LAN addresses are not transmitted over the Internet. In addition, NAT allows many addresses to exist behind a single valid address. Use the NAT routing mode if your LAN consists of a single device, otherwise collisions may occur if more than one device attempts to communicate using the same port.
NAPT	Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.
Device Metric	The device metric is a value used by the device to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.
Default Route	Select this check box to define this device as a the default route.
Routing Information Protocol (RIP)	Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, select the following:
Listen to RIP messages	Select 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
Send RIP messages	Select 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.
Multicast	IGMP Proxy Internal IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. IGMP proxy enables the routing of multicast packets according to the IGMP requests of LAN devices asking to join multicast groups. Select the 'Multicast IGMP Proxy Internal' check-box to enable this feature.
Routing Table	Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.

Figure 10-10: Advanced Routing Properties



Routing	Advanced ▾
Routing Mode:	Route
Device Metric:	4

□ Default Route

☑ Multicast - IGMP Proxy Internal

□ Routing Information Protocol (RIP)

Routing Table

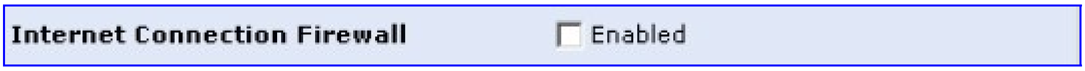
Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Ethernet	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	✎ ✖
New Route						✚

For detailed information on this feature, refer to Section 10.17.

10.1.5 Internet Connection Firewall

Your Telephone Adapter’s firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. For detailed information on your device's security features, refer to Section 5.

Figure 10-11: Internet Connection Firewall

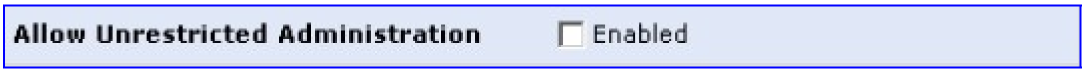


Internet Connection Firewall □ Enabled

10.1.6 Allow Unrestricted Administration

Select this check box to enable users other than those defined as 'Administrator' to change the device's configuration.

Figure 10-12: Allow Unrestricted Administration

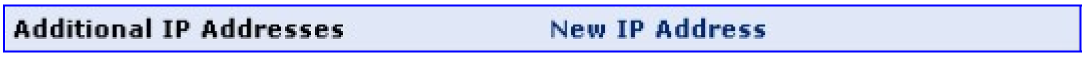


Allow Unrestricted Administration □ Enabled

10.1.7 Additional IP Addresses

You can add alias names (additional IP addresses) to the Telephone Adapter by clicking the 'New IP Address' link. This enables you to access the device using these aliases in addition to 192.168.1.1 and *http://MP-202.home*.

Figure 10-13: Additional IP Addresses



Additional IP Addresses New IP Address

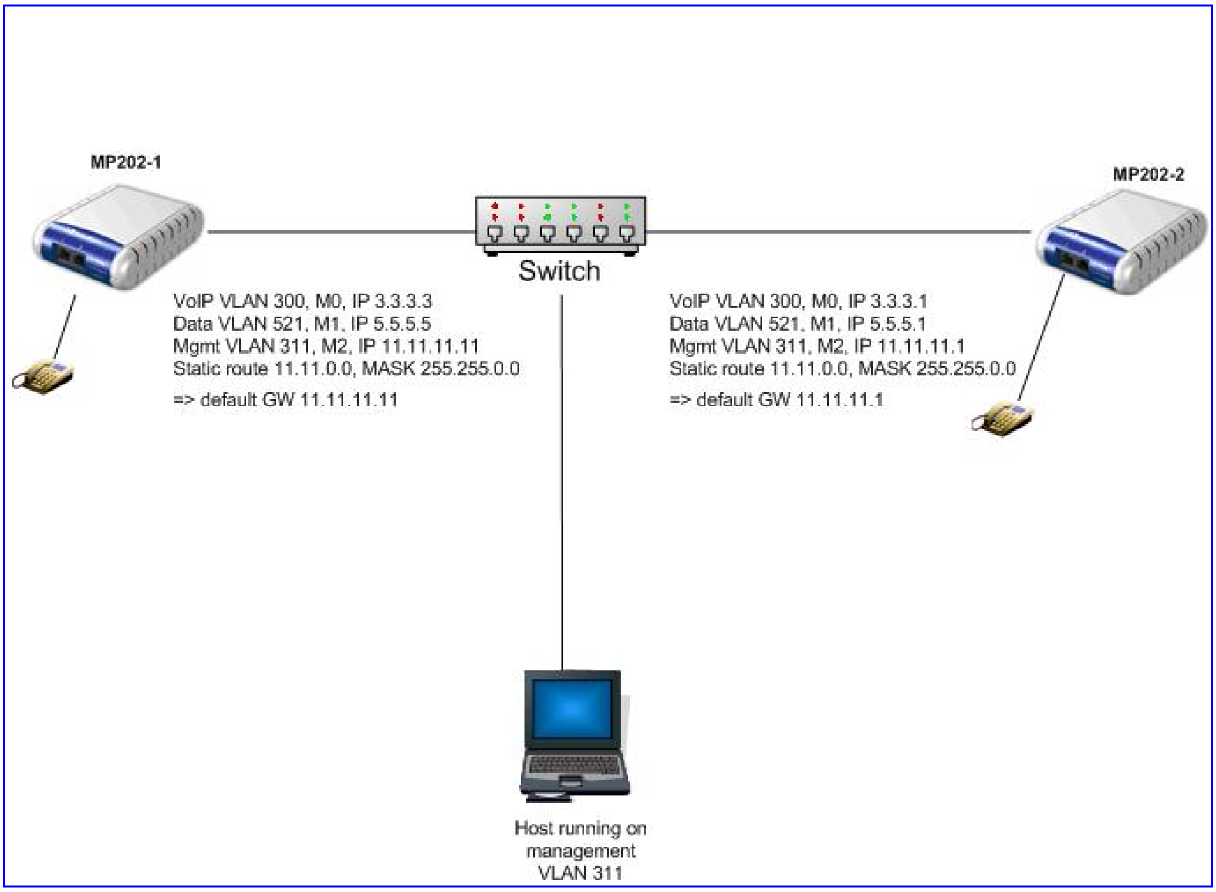
10.1.8 Example of Configuring 3 VLANs: VoIP, Data and Management

This example explains how to configure three separate VLANs: VoIP, data and management.

Setup

Two MP-202s are connected to the switch. Both are configured to use VLAN 300 for VoIP, VLAN 521 for Data and VLAN 311 for management. A station is connected to the switch in VLAN 311 (management).

Figure 10-14: Using VLAN - Setup



VoIP VLAN 300, M0, IP 3.3.3.3
Data VLAN 521, M1, IP 5.5.5.5
Mgmt VLAN 311, M2, IP 11.11.11.11
Static route 11.11.0.0, MASK 255.255.0.0
=> default GW 11.11.11.11

VoIP VLAN 300, M0, IP 3.3.3.1
Data VLAN 521, M1, IP 5.5.5.1
Mgmt VLAN 311, M2, IP 11.11.11.1
Static route 11.11.0.0, MASK 255.255.0.0
=> default GW 11.11.11.1

➢ To configure separate VLANs for VoIP, Data and Management packets:

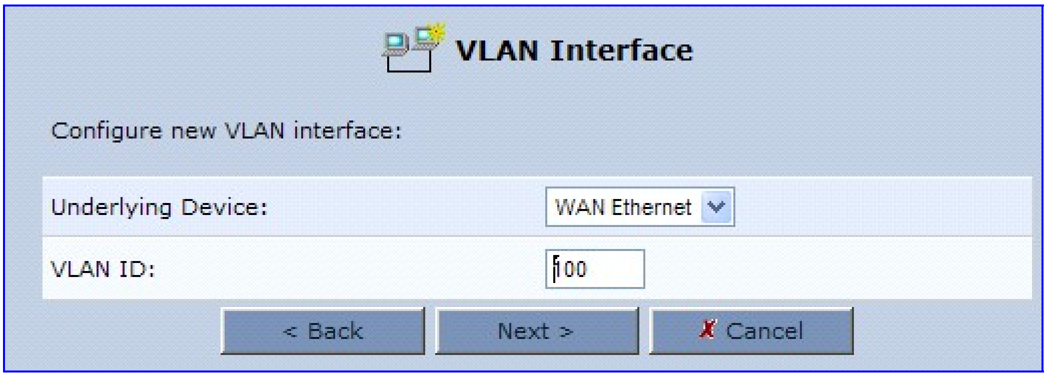
1. (For MP202-1) Open menu Advanced > Remote Administration; open 'Using Primary HTTP Port (80)' and 'Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)'
2. For VOIP, add VLAN ID 300. Set the new WAN interface to use static route 3.3.3.3. Choose advanced route. In ‘advanced route’, choose ROUTE mode, device metric = 0 and check the 'default gateway' check box.
3. For Data, add VLAN ID 521. Set the new WAN interface to use static route 5.5.5.5. Choose advanced route. In 'advanced route', choose NAPT mode, device metric = 1 and check the 'default gateway' check box.
4. For Management, add VLAN ID 311. Set the new WAN interface to use static route 11.11.11.11. Choose advanced route. In 'advanced route', choose ROUTE mode, device metric = 2 and check the 'default gateway' check box.
5. Add static route. Do so for all packets with destination IP 11.11.x.x, to use default the device whose address is 11.11.11.11.
6. To deny access to web management for all interfaces except VLAN 311, add an 'input rule' in 'advanced filtering' and deny all HTTP packets. Do this for each interface except the interface with VLAN 311.
7. Repeat the same steps for MP202-2. Use a different IP address.
8. To access the web management for both MP-202-1 and MP-202-2, connect a PC that works on the same VLAN management (311).

Defining a VLAN, Configuring its Interface

➢ To define an interface VLAN:

1. Open menu Network Connections > New Connection > Advanced Connection > VLAN Interface; the screen VLAN Interface opens (refer to the figure).

Figure 10-15: Example of Using VLAN - VLAN Interface Screen



VLAN Interface

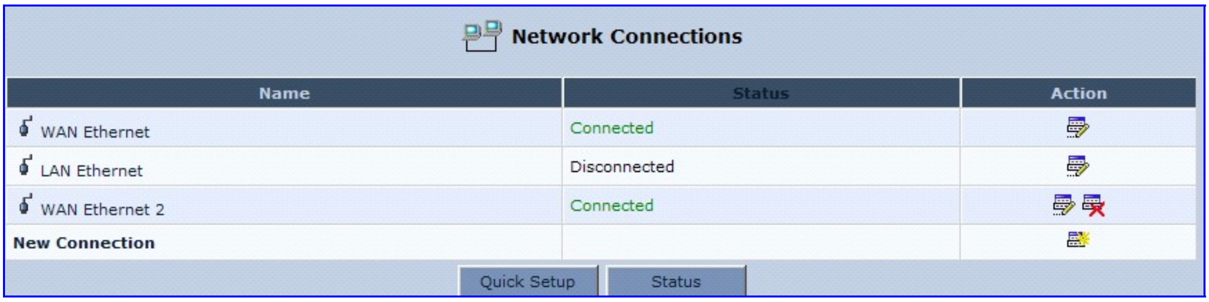
Configure new VLAN interface:

Underlying Device: WAN Ethernet

VLAN ID: 100

2. Define a VLAN ID for each device. Verify that you've got a new interface on the WAN side (WAN Ethernet 2) (refer to the figure below).

Figure 10-16: Verifying a New Interface on the WAN Side

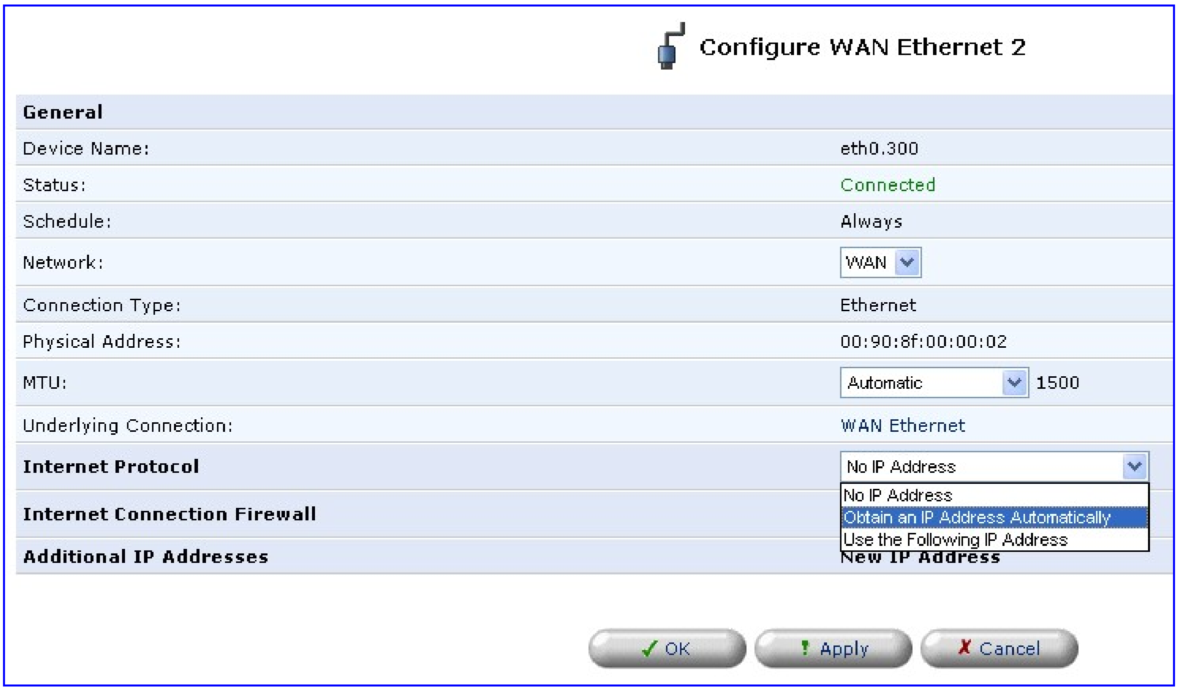


Network Connections

Name	Status	Action
WAN Ethernet	Connected	
LAN Ethernet	Disconnected	
WAN Ethernet 2	Connected	
New Connection		

3. Enter the new interface by clicking the Action icon (shown in the screen above); the screen shown below opens.

Figure 10-17: Configuring WAN Ethernet



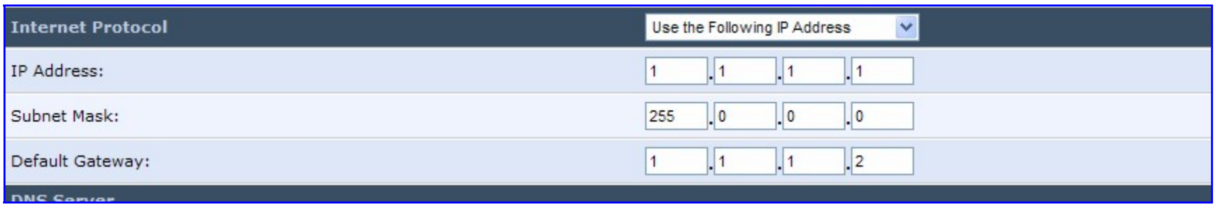
Configure WAN Ethernet 2

General	
Device Name:	eth0.300
Status:	Connected
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00:90:8f:00:00:02
MTU:	Automatic 1500
Underlying Connection:	WAN Ethernet
Internet Protocol	No IP Address
Internet Connection Firewall	
Additional IP Addresses	New IP Address

No IP Address
Obtain an IP Address Automatically
Use the Following IP Address
✓ OK
! Apply
✗ Cancel

4. Assign an IP address (static / DHCP) to the new interface. Configure the parameter 'Internet Protocol' to the Static IP option of 'Use the Following IP Address'; the screen shown below opens.

Figure 10-18: Use the Following IP Address



Internet Protocol	Use the Following IP Address
IP Address:	1 . 1 . 1 . 1
Subnet Mask:	255 . 0 . 0 . 0
Default Gateway:	1 . 1 . 1 . 2
DNS Server	

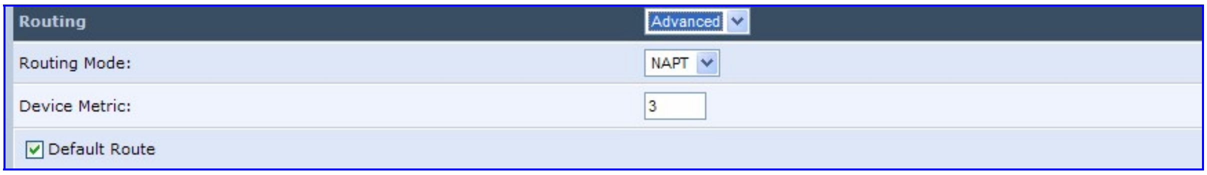
5. Define an IP address for each device and click Apply and OK.

Changing the Routing Mode

➢ To change the routing mode:

1. (For all VOIP packets needing to be transferred within the VoIP VLAN) Open menu Network Connections > WAN Ethernet 2 > Settings; the figure shown below opens.

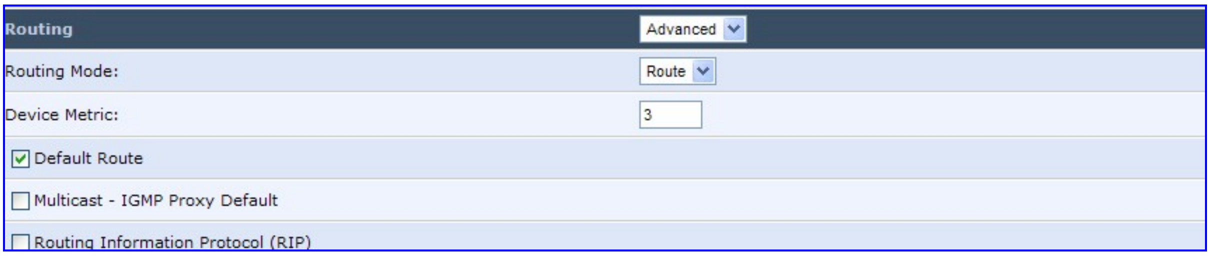
Figure 10-19: Routing - Advanced



Routing	Advanced
Routing Mode:	NAPT
Device Metric:	3
☑ Default Route	

2. In the Routing drop-down list, change the mode to 'Advanced'; extended parameters are displayed (refer to the figure below).

Figure 10-20: Routing - Advanced - Extended Parameters



Routing	Advanced
Routing Mode:	Route
Device Metric:	3
☑ Default Route	
☐ Multicast - IGMP Proxy Default	
☐ Routing Information Protocol (RIP)	

3. Configure parameter 'Routing Mode' (NAT or Route). Choose 'Route' and check the check box 'Default Route' in order to use the VoIP VLAN.

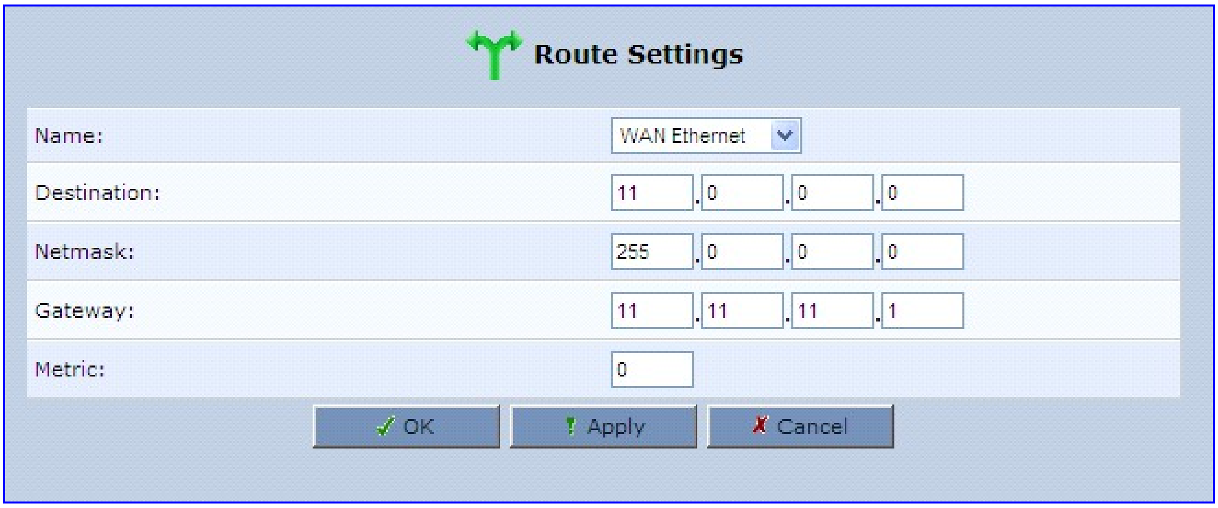
4. Configure 'Device Metric' to be the lower than the default metric (default = 3).

Adding a Static Route

➢ To add a static route:

1. Open menu Advanced > Routing and click link 'New Route'; the screen shown below opens.

Figure 10-21: Route Settings



Route Settings

Name:	WAN Ethernet
Destination:	11.0.0.0
Netmask:	255.0.0.0
Gateway:	11.11.11.1
Metric:	0

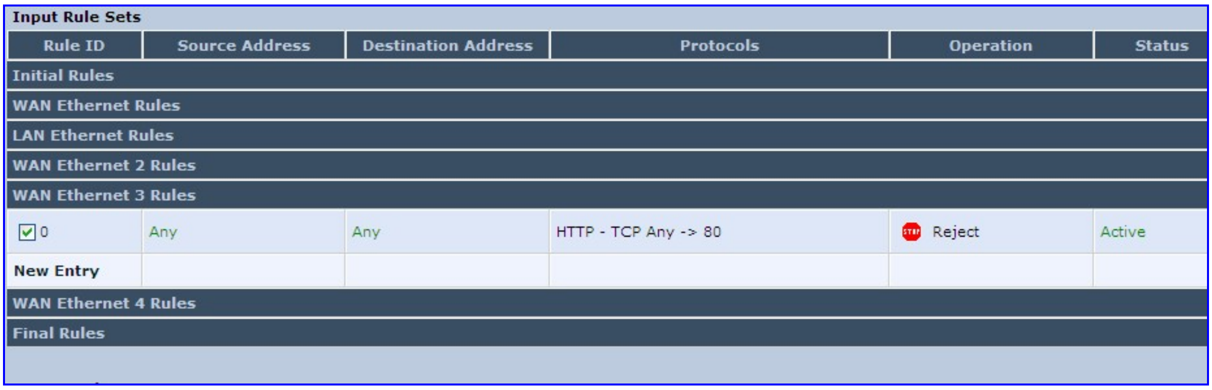
2. From the 'Name' drop-down list, choose 'WAN Ethernet'; configure the parameters Destination, Netmask and Gateway.

Adding a Security Input Rule

➢ To add a security input rule:

1. Open menu Security > tab Advanced Filtering; the screen containing section 'Input Rule Sets' (shown below) opens.

Figure 10-22: Input Rule Sets

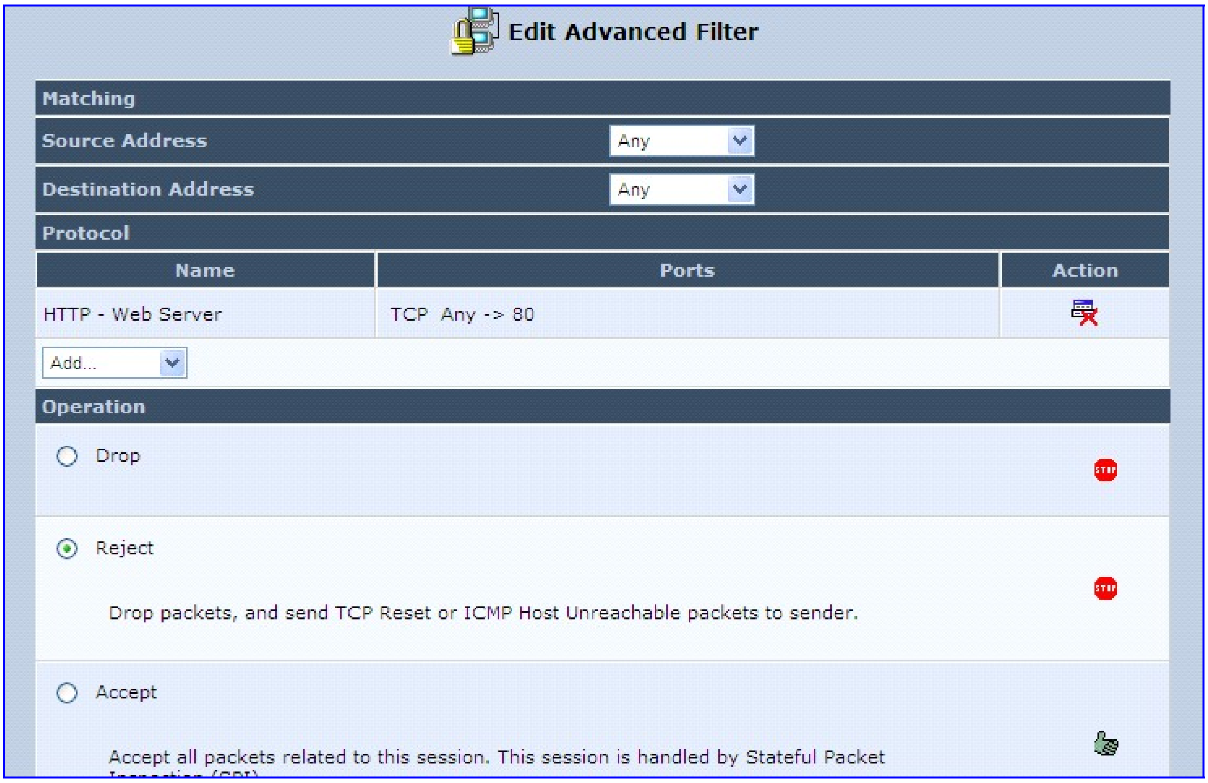


Input Rule Sets

Rule ID	Source Address	Destination Address	Protocols	Operation	Status
Initial Rules					
WAN Ethernet Rules					
LAN Ethernet Rules					
WAN Ethernet 2 Rules					
WAN Ethernet 3 Rules					
☑ 0	Any	Any	HTTP - TCP Any -> 80	Reject	Active
New Entry					
WAN Ethernet 4 Rules					
Final Rules					

2. Add a new entry for the interface; choose what the filter will be determined by (Source IP, Destination IP or Protocol). In the example shown in the figure below, Port 80 (HTTP) is rejected.

Figure 10-23: Edit Advanced Filter



Edit Advanced Filter

Matching

Source Address: Any

Destination Address: Any

Protocol

Name	Ports	Action
HTTP - Web Server	TCP Any -> 80	

Add...

Operation

○ Drop

● Reject

Drop packets, and send TCP Reset or ICMP Host Unreachable packets to sender.

○ Accept

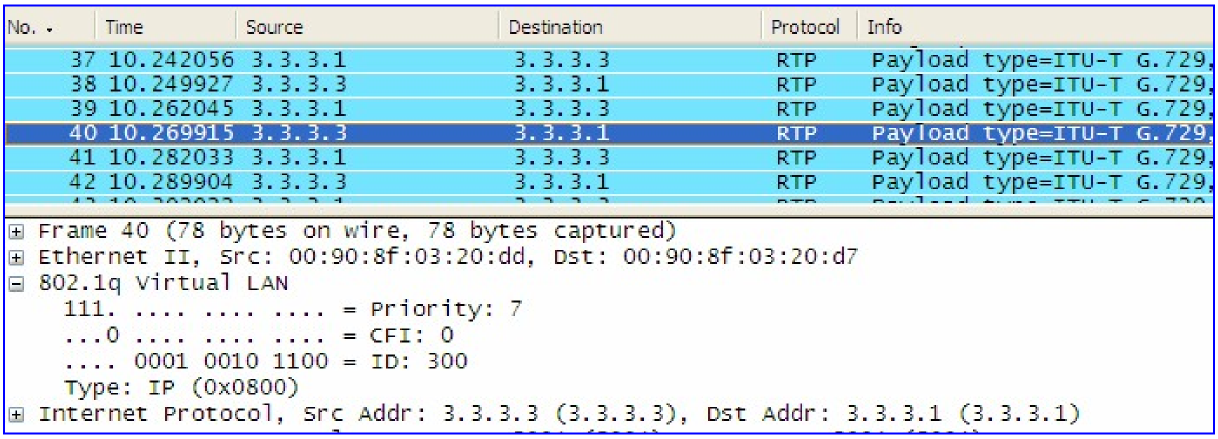
Accept all packets related to this session. This session is handled by Stateful Packet Inspection (SPI).

Testing the 3-VLAN Setup

➢ To test the 3-VLAN setup:

1. Place a VOIP call. Verify that the VOIP is using 802.1q/p, that the VLAN ID is 300 and that the IP is 3.3.x.x (refer to the screen shown below).

Figure 10-24: Testing the Setup

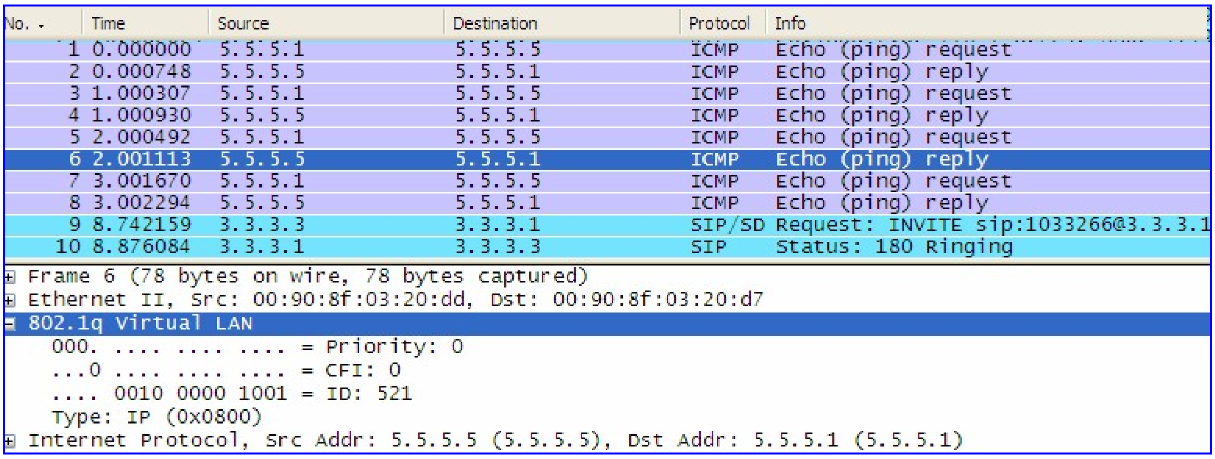


```
No. -  Time       Source     Destination  Protocol  Info
  37 10.242056 3.3.3.1     3.3.3.3      RTP       Payload type=ITU-T G.729,
  38 10.249927 3.3.3.3     3.3.3.1      RTP       Payload type=ITU-T G.729,
  39 10.262045 3.3.3.1     3.3.3.3      RTP       Payload type=ITU-T G.729,
  40 10.269915 3.3.3.3     3.3.3.1      RTP       Payload type=ITU-T G.729,
  41 10.282033 3.3.3.1     3.3.3.3      RTP       Payload type=ITU-T G.729,
  42 10.289904 3.3.3.3     3.3.3.1      RTP       Payload type=ITU-T G.729,

⊞ Frame 40 (78 bytes on wire, 78 bytes captured)
⊞ Ethernet II, Src: 00:90:8f:03:20:dd, Dst: 00:90:8f:03:20:d7
⊟ 802.1q Virtual LAN
    111. .... .... .... = Priority: 7
    ...0 .... .... .... = CFI: 0
    .... 0001 0010 1100 = ID: 300
    Type: IP (0x0800)
⊞ Internet Protocol, Src Addr: 3.3.3.3 (3.3.3.3), Dst Addr: 3.3.3.1 (3.3.3.1)
```

2. Connect a PC to the LAN port of MP202 (1 or 2) and send traffic (ICMP). Verify that the ICMP traffic is tagged (802.1q) and that it is using VLAN 521.

Figure 10-25: Testing the Setup

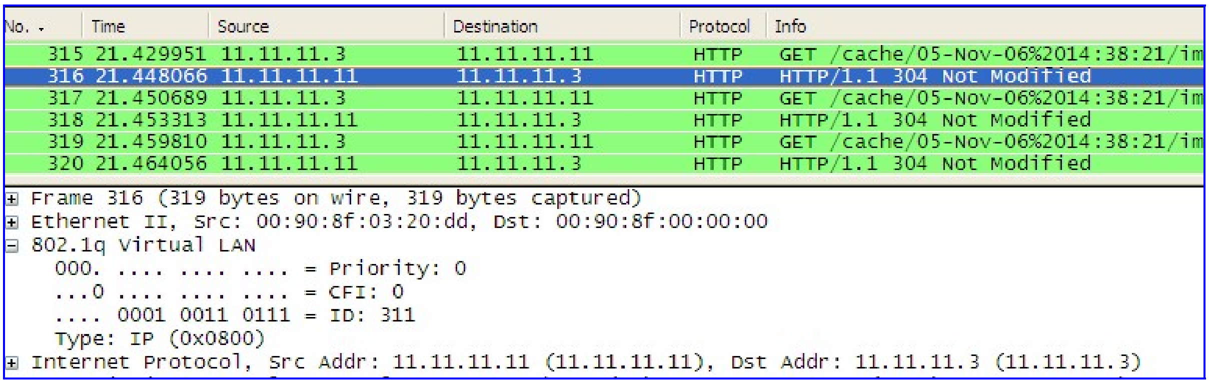


```
No. -   Time        Source     Destination  Protocol  Info
   1 0.000000   5.5.5.1    5.5.5.5      ICMP      Echo (ping) request
   2 0.000748   5.5.5.5    5.5.5.1      ICMP      Echo (ping) reply
   3 1.000307   5.5.5.1    5.5.5.5      ICMP      Echo (ping) request
   4 1.000930   5.5.5.5    5.5.5.1      ICMP      Echo (ping) reply
   5 2.000492   5.5.5.1    5.5.5.5      ICMP      Echo (ping) request
   6 2.001113   5.5.5.5    5.5.5.1      ICMP      Echo (ping) reply
   7 3.001670   5.5.5.1    5.5.5.5      ICMP      Echo (ping) request
   8 3.002294   5.5.5.5    5.5.5.1      ICMP      Echo (ping) reply
   9 8.742159   3.3.3.3    3.3.3.1      SIP/SD    Request: INVITE sip:1033266@3.3.3.1
  10 8.876084   3.3.3.1    3.3.3.3      SIP       Status: 180 Ringing
```

```
⊞ Frame 6 (78 bytes on wire, 78 bytes captured)
⊞ Ethernet II, Src: 00:90:8f:03:20:dd, Dst: 00:90:8f:03:20:d7
⊟ 802.1q Virtual LAN
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0010 0000 1001 = ID: 521
    Type: IP (0x0800)
⊞ Internet Protocol, Src Addr: 5.5.5.5 (5.5.5.5), Dst Addr: 5.5.5.1 (5.5.5.1)
```

3. Connect the management PC to VLAN 311 and verify that all management traffic is carried in this VLAN (refer to the figure below).

Figure 10-26: Testing the Setup



```
No. -   Time         Source        Destination   Protocol  Info
  315 21.429951 11.11.11.3    11.11.11.11   HTTP      GET /cache/05-Nov-06%2014:38:21/im
  316 21.448066 11.11.11.11   11.11.11.3    HTTP      HTTP/1.1 304 Not Modified
  317 21.450689 11.11.11.3    11.11.11.11   HTTP      GET /cache/05-Nov-06%2014:38:21/im
  318 21.453313 11.11.11.11   11.11.11.3    HTTP      HTTP/1.1 304 Not Modified
  319 21.459810 11.11.11.3    11.11.11.11   HTTP      GET /cache/05-Nov-06%2014:38:21/im
  320 21.464056 11.11.11.11   11.11.11.3    HTTP      HTTP/1.1 304 Not Modified
```

```
⊞ Frame 316 (319 bytes on wire, 319 bytes captured)
⊞ Ethernet II, Src: 00:90:8f:03:20:dd, Dst: 00:90:8f:00:00:00
⊟ 802.1q Virtual LAN
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0001 0011 0111 = ID: 311
    Type: IP (0x0800)
⊞ Internet Protocol, Src Addr: 11.11.11.11 (11.11.11.11), Dst Addr: 11.11.11.3 (11.11.11.3)
```

10.2 WAN-LAN Bridge

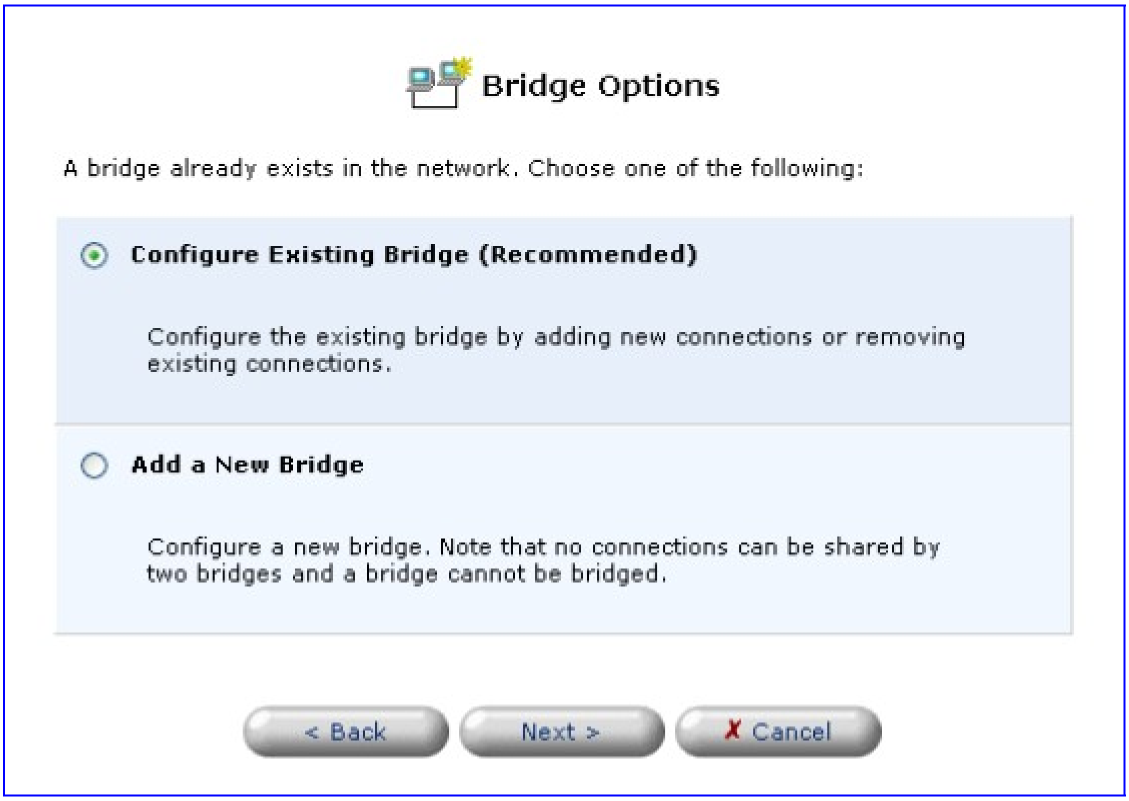
WAN bridge creates a bridge over WAN and LAN devices. In this way, PCs on the (ProductNameGeneric)'s LAN side can get IP addresses that are known on the WAN side.

10.2.1 Creation with the Connection Wizard

➢ **To configure an existing bridge or create a new one:**

1. Click the link 'New Connection' in the screen 'Network Connections'; the screen 'Connection Wizard' opens.
2. Select the radio button 'Advanced Connection' and click 'Next'; the screen 'Advanced Connection' opens.
3. Select the radio button 'Network Bridging' and click 'Next'; the screen 'Bridge Options' opens (refer to the figure below).

Figure 10-27: Bridge Options



Bridge Options

A bridge already exists in the network. Choose one of the following:

● **Configure Existing Bridge (Recommended)**

Configure the existing bridge by adding new connections or removing existing connections.

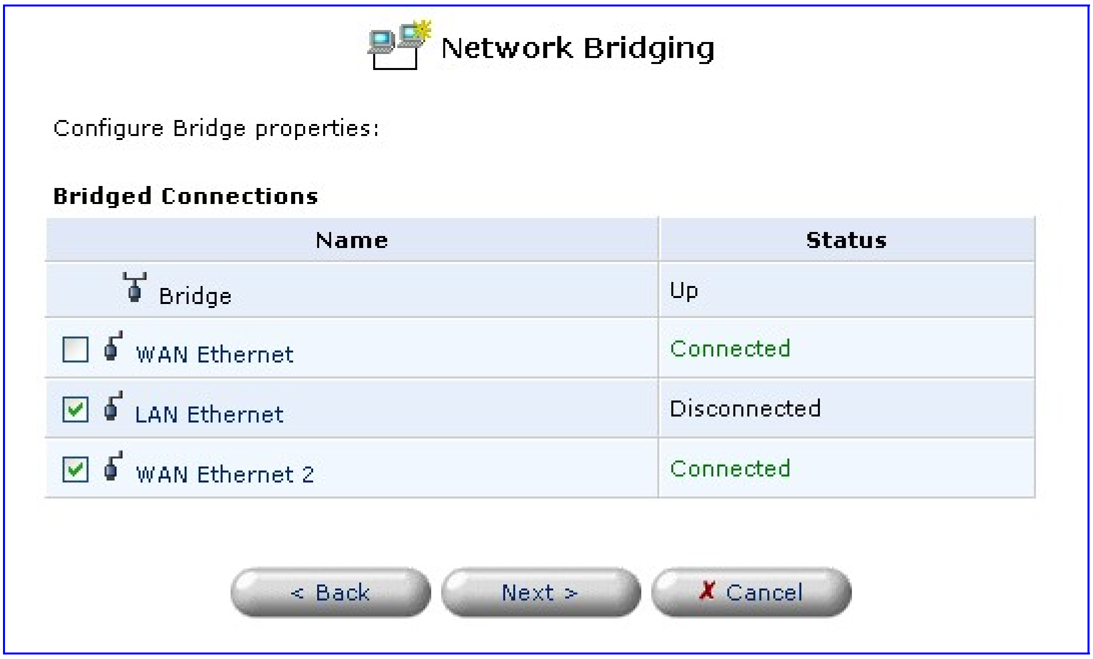
○ **Add a New Bridge**

Configure a new bridge. Note that no connections can be shared by two bridges and a bridge cannot be bridged.

4. Select whether to configure an existing bridge (this option will only appear if a bridge exists) or to add a new one:

1. Configure Existing Bridge
   Select this option and click 'Next'; the screen 'Network Bridging' opens (refer to the figure below) allowing you to add new connections or remove existing ones, by checking or unchecking their respective check boxes.

Figure 10-28: Network Bridging



Network Bridging

Configure Bridge properties:

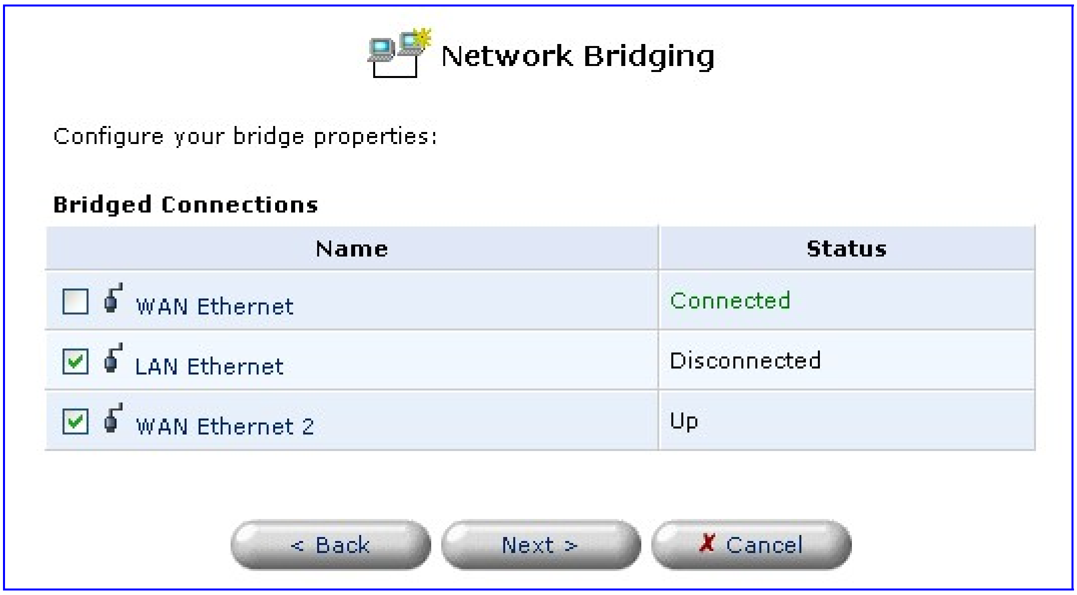
Bridged Connections

Name	Status
Bridge	Up
□ WAN Ethernet	Connected
☑ LAN Ethernet	Disconnected
☑ WAN Ethernet 2	Connected

For example, checking the WAN check box will create a LAN-WAN bridge.

2. Add a New Bridge
   Select this option and click 'Next'; a different 'Network Bridging' screen opens (refer to the figure below) allowing you to add a bridge over the unbridged connections, by checking their respective check boxes.

Figure 10-29: WLAN-LAN - Network Bridging



Network Bridging

Configure your bridge properties:

Bridged Connections

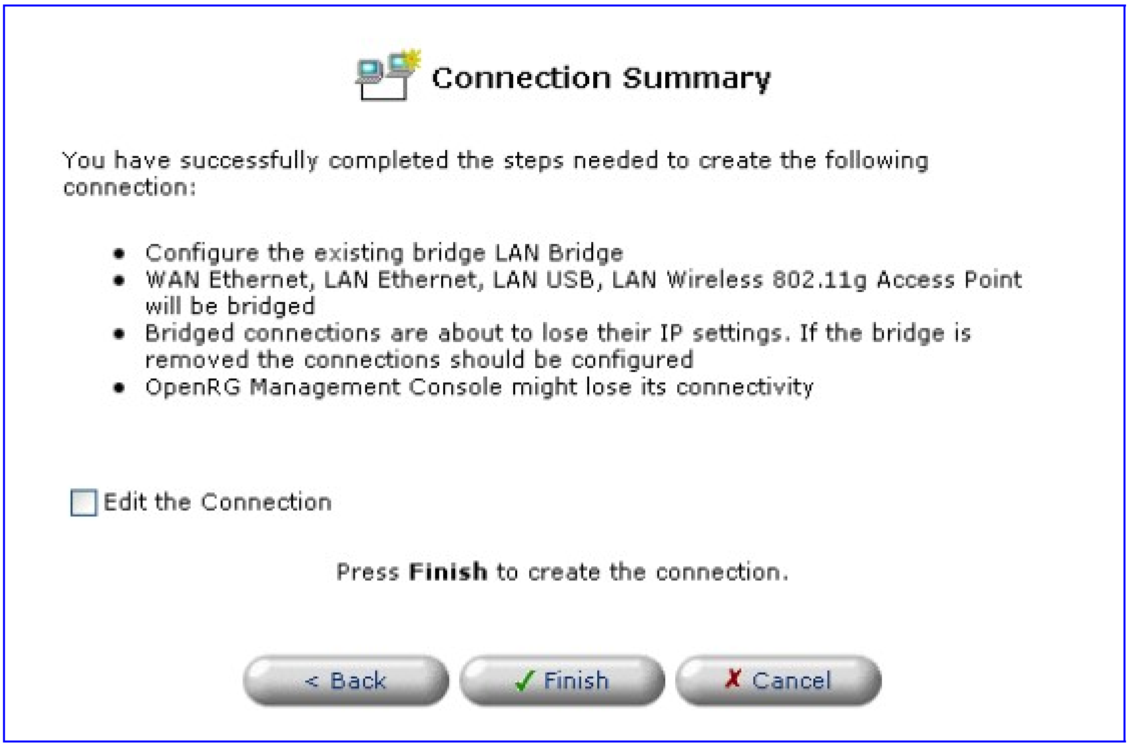
Name	Status
□ WAN Ethernet	Connected
☑ LAN Ethernet	Disconnected
☑ WAN Ethernet 2	Up

Important notes:

- The same connections cannot be shared by two bridges.
- A bridge cannot be bridged.
- Bridged connections will lose their IP settings.

5. Click 'Next'; the screen 'Connection Summary' opens (refer to the figure below), corresponding to your changes.

Figure 10-30: Connection Summary - Configure Existing Bridge



Connection Summary

You have successfully completed the steps needed to create the following connection:

- Configure the existing bridge LAN Bridge
- WAN Ethernet, LAN Ethernet, LAN USB, LAN Wireless 802.11g Access Point will be bridged
- Bridged connections are about to lose their IP settings. If the bridge is removed the connections should be configured
- OpenRG Management Console might lose its connectivity

□ Edit the Connection

Press **Finish** to create the connection.

6. Check the check box 'Edit the Newly Created Connection' to be routed to the new connection's configuration screen after clicking 'Finish'.
7. Click 'Finish' to save the settings; the new bridge is added to the network connections list; it's configurable like any other bridge.

10.2.2 General

Refer to "General" on page 100.

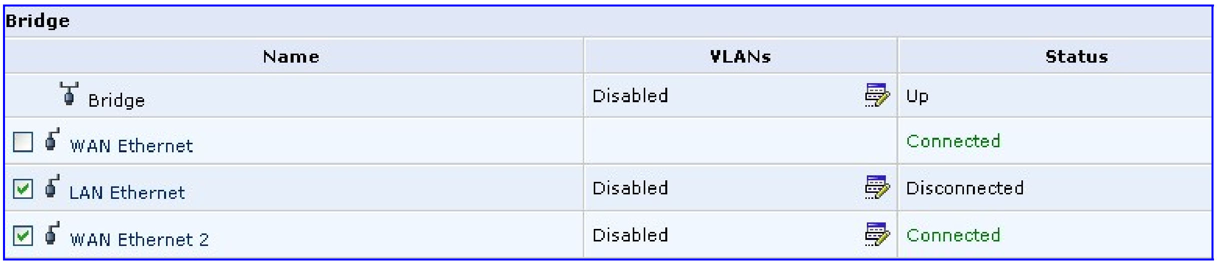
10.2.3 Internet Protocol Settings

Refer to "Internet Protocol Settings" on page 79

10.2.4 Bridge Settings

The bridge section allows you to specify the LAN and WAN devices that you would like to join under the network bridge. Click the icon 'Edit' on the VLAN column to assign the network connections to specific Virtual LANS. Select the check box 'STP' to enable the Spanning Tree Protocol on the device. You should use this to ensure that there are no loops in your network configuration, and apply these settings if your network consists of multiple switches, or other bridges apart from those created by the Telephone Adapter.

Figure 10-31: Bridge Settings



Bridge

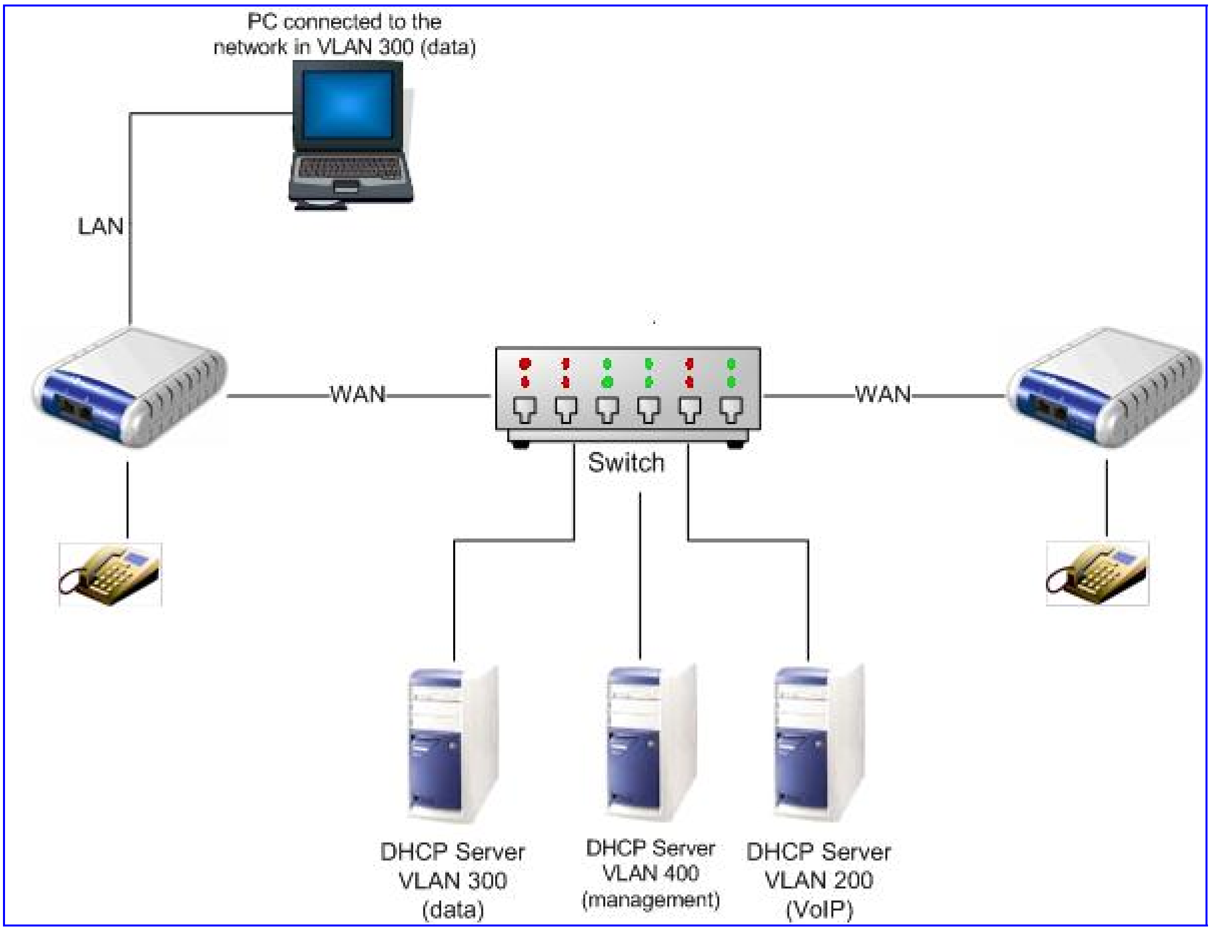
Name	VLANs	Status
Bridge	Disabled	Up
□ WAN Ethernet		Connected
☑ LAN Ethernet	Disabled	Disconnected
☑ WAN Ethernet 2	Disabled	Connected

10.2.5 Examples of Configuring VLANs in Bridge Mode

10.2.5.1 Example 1 - Configuring 3 VLANs: VoIP, Data and Management

This example explains how to configure the MP-202 to use 3 separate VLANs (for VOIP, data and management) in bridge mode.

Figure 10-32: Example of Using Bridge Mode and Configuring VLANs


PC connected to the network in VLAN 300 (data)
LAN
WAN
Switch
WAN
DHCP Server VLAN 300 (data)
DHCP Server VLAN 400 (management)
DHCP Server VLAN 200 (VoIP)

Setup

Two MP-202s are connected to the switch. Both are configured to use VLAN 200 for VOIP, VLAN 300 for Data and VLAN 400 for Management. Three DHCP servers are connected to the same switch (optional; you can use a static IP address for each VLAN). One uses VLAN 200, the second, VLAN 300, and the third, VLAN 400.

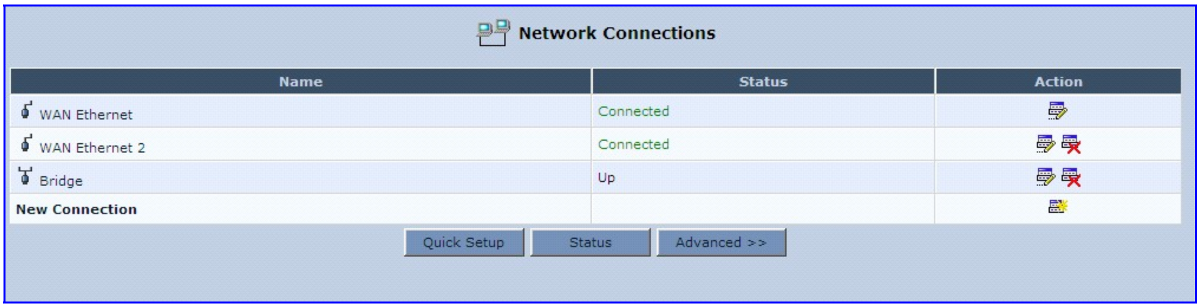
➢ To configure 3 separate VLANs in bridge mode:

1. (For MP202-1 & MP202-2; refer to the figure above) Connect the PC to MP202-1 LAN NIC and use static IP address 192.168.2.10 for your PC.
2. In Internet Explorer, browse to http://192.168.2.1

3. Open menu Advanced > Remote Administration. Check the check boxes 'Using Primary HTTP Port (80)' and 'Allow Incoming ICMP Echo Requests' (to allow HTTP and ICMP from the WAN interface)

4. For data, configure VLAN ID 300 and then configure it to 'Obtain IP Address Automatically' (refer to the figure below) (optionally, you can use a static IP address).

Figure 10-33: Network Connections

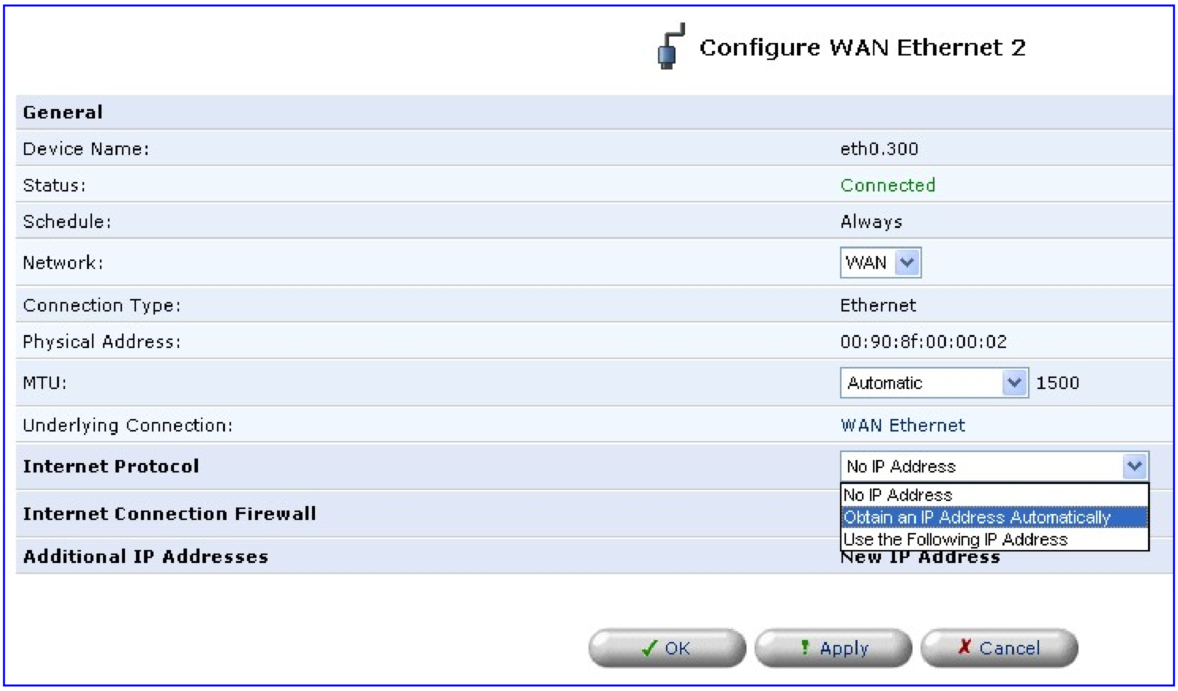

Network Connections

Name	Status	Action
WAN Ethernet	Connected	
WAN Ethernet 2	Connected	
Bridge	Up	
New Connection		

5. For VOIP, configure VLAN ID 200 and then configure it to 'Obtain IP Address Automatically' (optionally, you can use a static IP address).

6. For management, configure VLAN ID 400 and then configure it to 'Obtain IP Address Automatically' (optionally, you can use a static IP address). The figure below shows how to obtain DHCP on the interface.

Figure 10-34: Configuring WAN Ethernet

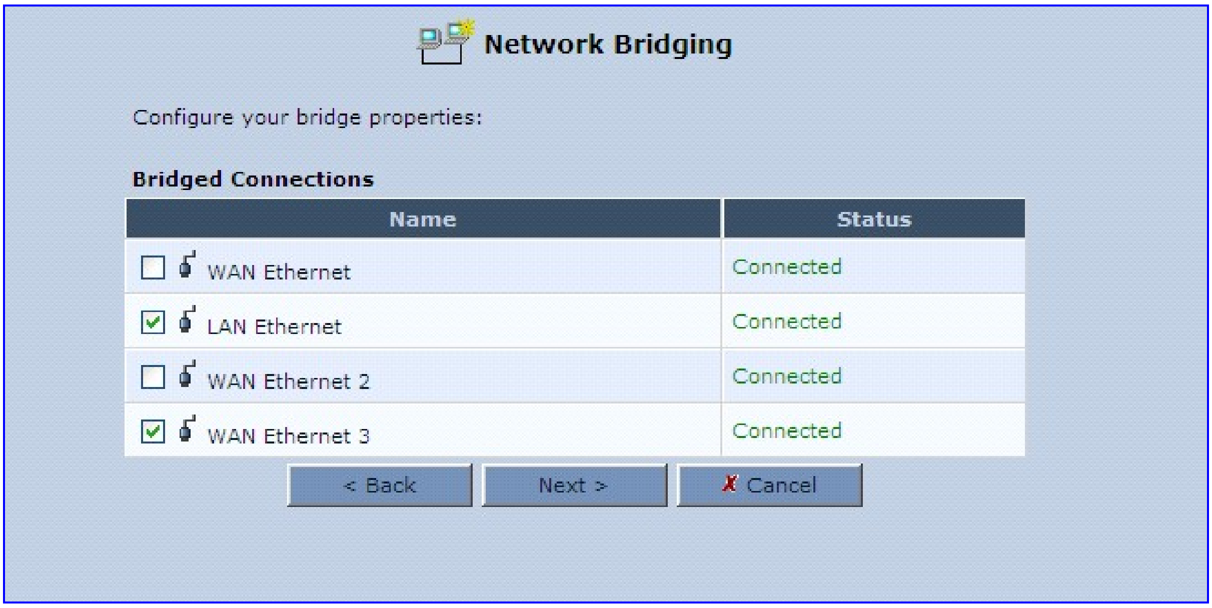

Configure WAN Ethernet 2

General	
Device Name:	eth0.300
Status:	Connected
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00:90:8f:00:00:02
MTU:	Automatic 1500
Underlying Connection:	WAN Ethernet
Internet Protocol	No IP Address
Internet Connection Firewall	
Additional IP Addresses	New IP Address

No IP Address
Obtain an IP Address Automatically
Use the Following IP Address
✓ OK
! Apply
✗ Cancel

7. Define a new network bridge. Define a network bridge by checking the check boxes of LAN Ethernet and WAN Ethernet 3 (VLAN Interface 300) in the screen 'Network Bridging' under 'Bridged Connections' (refer to the figure below).

Figure 10-35: Network Bridging



Network Bridging

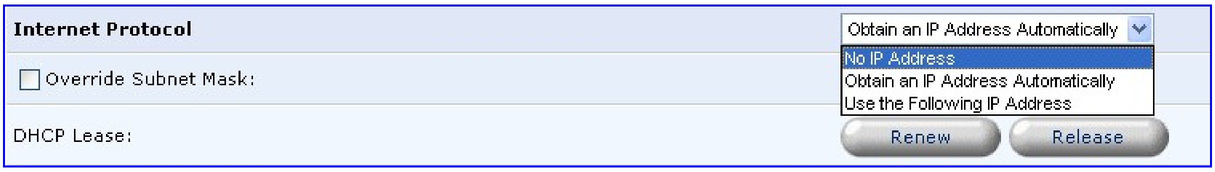
Configure your bridge properties:

Bridged Connections

Name	Status
□ WAN Ethernet	Connected
☑ LAN Ethernet	Connected
□ WAN Ethernet 2	Connected
☑ WAN Ethernet 3	Connected

8. Set the bridge to use 'No IP Address'. Click Apply and OK and then click OK again.

Figure 10-36: No IP Address



Internet Protocol: Obtain an IP Address Automatically

□ Override Subnet Mask:

DHCP Lease:

No IP Address
Obtain an IP Address Automatically
Use the Following IP Address
Renew
Release

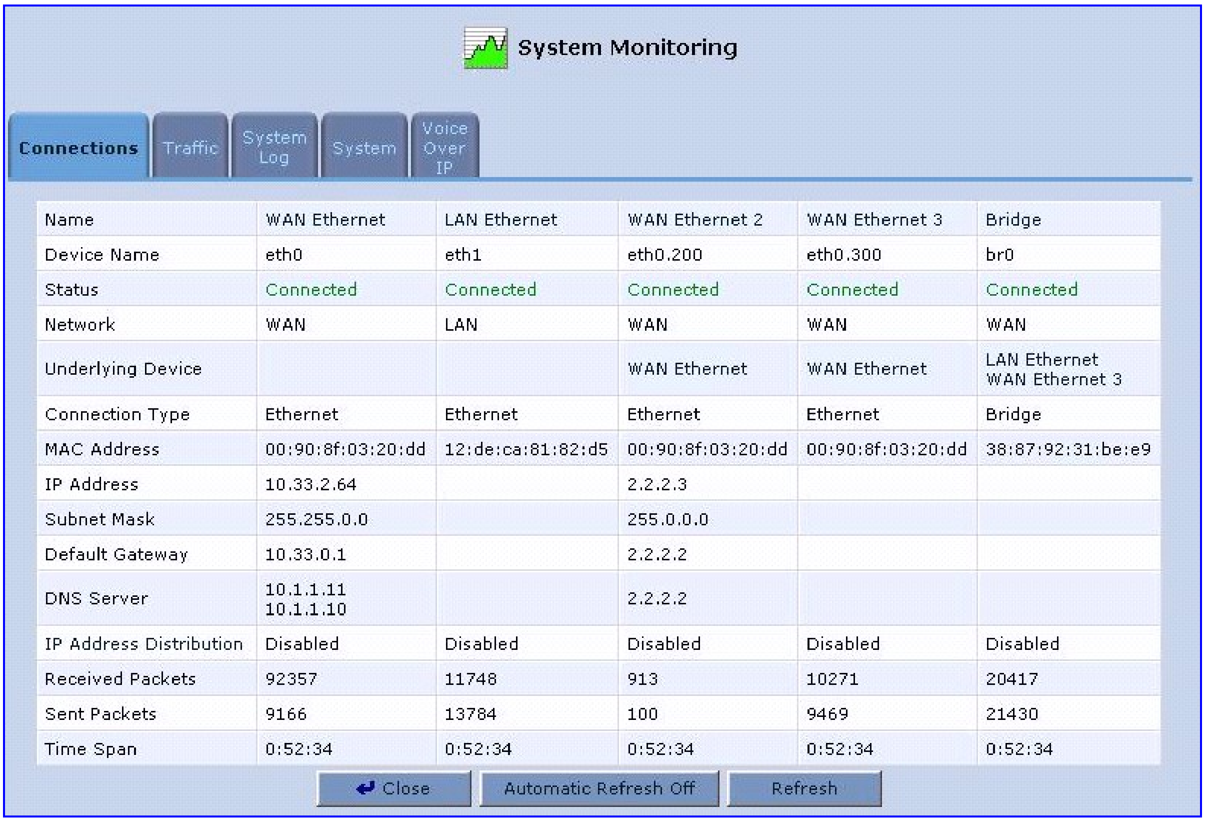
9. Reboot the MP-202 (optional).

10. Ensure that the PC is connected to the LAN port of the MP-202 and then configure it to 'Obtain IP Address Automatically'; all data from the LAN port will be in VLAN 300.

11. To access the web from the WAN, you must be in VLAN 400 and use the VLAN 400 IP address.

12. To access the web from the LAN, set your PC to a static IP address 192.168.2.2-254; the figure below shows the System Monitoring screen.

Figure 10-37: System Monitoring



Name	WAN Ethernet	LAN Ethernet	WAN Ethernet 2	WAN Ethernet 3	Bridge
Device Name	eth0	eth1	eth0.200	eth0.300	br0
Status	Connected	Connected	Connected	Connected	Connected
Network	WAN	LAN	WAN	WAN	WAN
Underlying Device			WAN Ethernet	WAN Ethernet	LAN Ethernet WAN Ethernet 3
Connection Type	Ethernet	Ethernet	Ethernet	Ethernet	Bridge
MAC Address	00:90:8f:03:20:dd	12:de:ca:81:82:d5	00:90:8f:03:20:dd	00:90:8f:03:20:dd	38:87:92:31:be:e9
IP Address	10.33.2.64		2.2.2.3		
Subnet Mask	255.255.0.0		255.0.0.0		
Default Gateway	10.33.0.1		2.2.2.2		
DNS Server	10.1.1.11 10.1.1.10		2.2.2.2		
IP Address Distribution	Disabled	Disabled	Disabled	Disabled	Disabled
Received Packets	92357	11748	913	10271	20417
Sent Packets	9166	13784	100	9469	21430
Time Span	0:52:34	0:52:34	0:52:34	0:52:34	0:52:34

Testing the Setup

13. Place a VOIP call and see that the VOIP is using 802.1q/p and that the VID is 200.

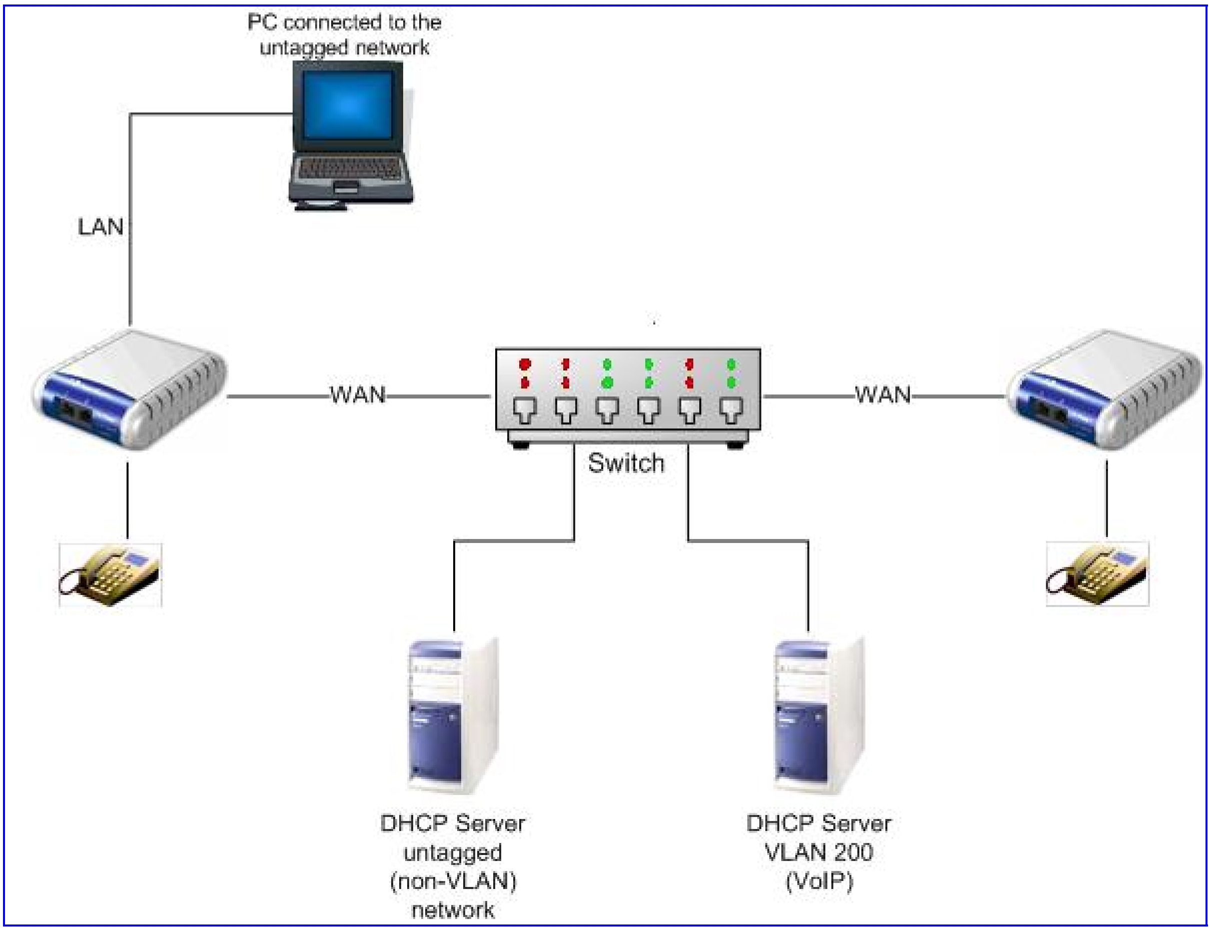
14. Ping from the PC (behind MP202-1) to the network; you'll see that the data traffic is using 802.1q and that the VID is 300.

15. Connect a PC to the network in VLAN 400; verify that you can access VLAN 400 from the WAN interface.

10.2.5.2 Example 2 - Configuring Tagged VoIP, Untagged Data Traffic

This example explains how to configure the MP-202 to tag VoIP traffic and untag data traffic in bridge mode.

Figure 10-38: Example of Tagging Voice and Untagging Data


PC connected to the untagged network
LAN
WAN
WAN
Switch
DHCP Server untagged (non-VLAN) network
DHCP Server VLAN 200 (VoIP)

Setup

Two MP-202s are connected to the switch. Both are configured to use VLAN 200 for VoIP and non-VLAN traffic for data. Two DHCP servers are connected to the same switch. One is in a VLAN 200 network; the other is in a non-VLAN network.

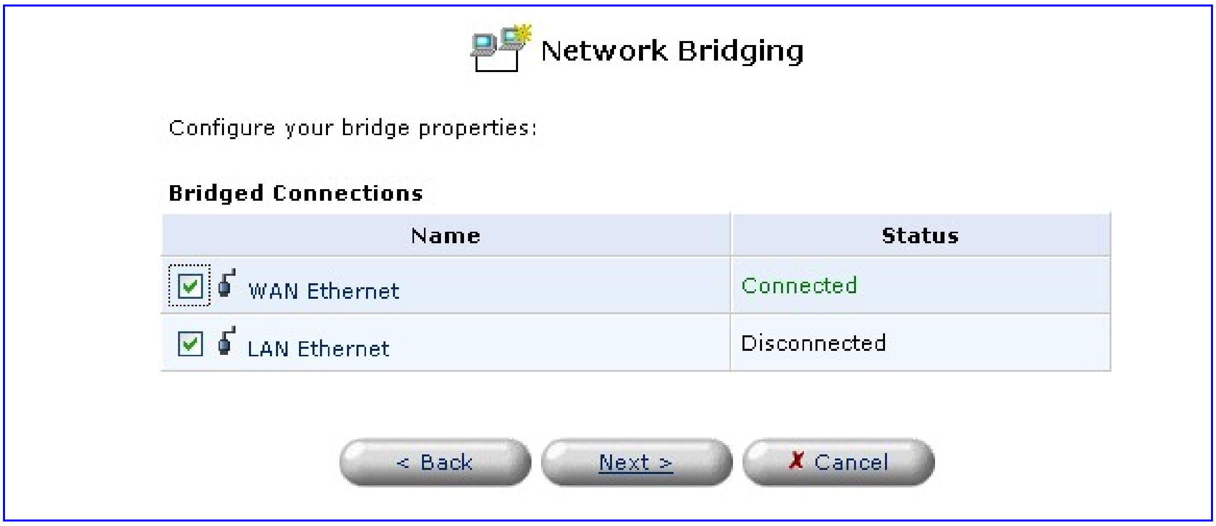
➢ To configure tagging for VoIP and untagging for data in bridge mode:

For MP202-1 and MP202-2

1. Connect the PC to the LAN NIC and use static IP address 192.168.2.2-254 for your PC.
2. In Internet Explorer, browse to http://192.168.2.1
3. Open menu Advanced > Remote Administration. Check the check boxes 'Using Primary HTTP Port (80)' and 'Allow Incoming ICMP Echo Requests' (to allow HTTP and ICMP from the WAN interface)

4. Add a network bridge: In the screen 'Network Bridging', check LAN Ethernet and WAN Ethernet (refer to the figure below).

Figure 10-39: WAN/LAN Bridge



Network Bridging

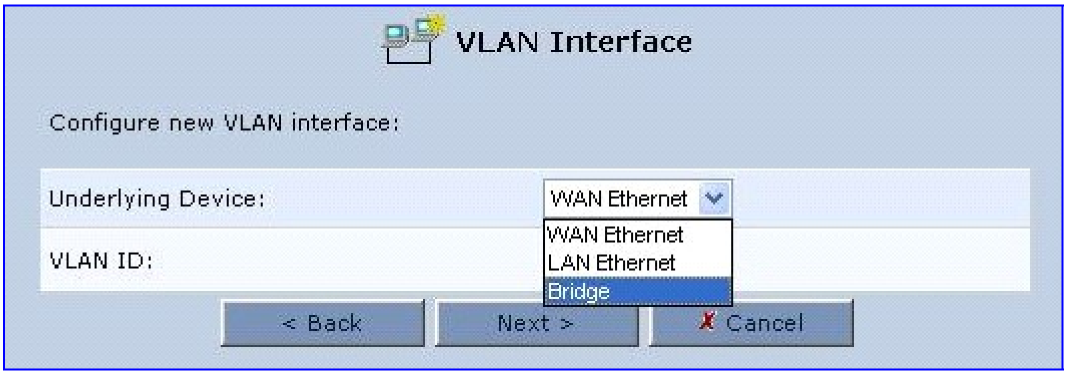
Configure your bridge properties:

Bridged Connections

Name	Status
☑ WAN Ethernet	Connected
☑ LAN Ethernet	Disconnected

5. For VoIP, add VLAN Interface 200 (VID 200) and choose option 'Bridge' in the drop-down list of parameter 'Underlying Device' (refer to the figure below).

Figure 10-40: VLAN Interface Screen



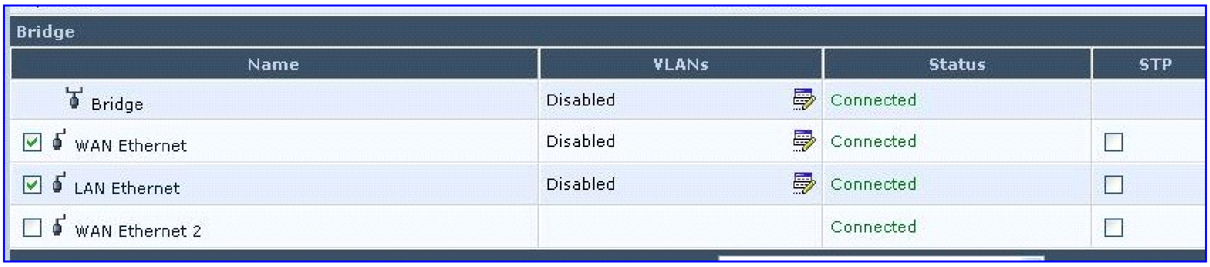
VLAN Interface

Configure new VLAN interface:

Underlying Device:	WAN Ethernet
VLAN ID:	

6. Set the bridge interface: In the 'Bridge' section of the Network Connection screen, edit the 'Bridge' and 'WAN' interfaces to enable VLAN for all VLAN IDs (refer to the screen below).

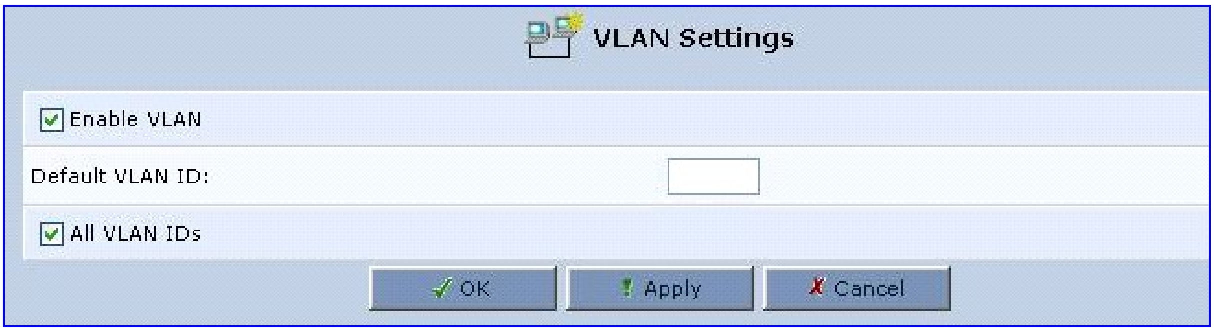
Figure 10-41: Bridge Section of the Screen



Bridge

Name	VLANs	Status	STP
Bridge	Disabled	Connected	
☑ WAN Ethernet	Disabled	Connected	□
☑ LAN Ethernet	Disabled	Connected	□
□ WAN Ethernet 2		Connected	□

Figure 10-42: VLAN Settings



VLAN Settings

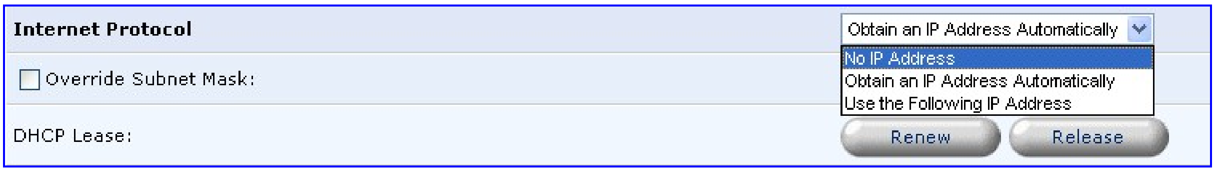
☑ Enable VLAN

Default VLAN ID:

☑ All VLAN IDs

7. Set the bridge to use 'No IP Address'. Click Apply and OK and then click OK again.

Figure 10-43: No IP Address



Internet Protocol: Obtain an IP Address Automatically

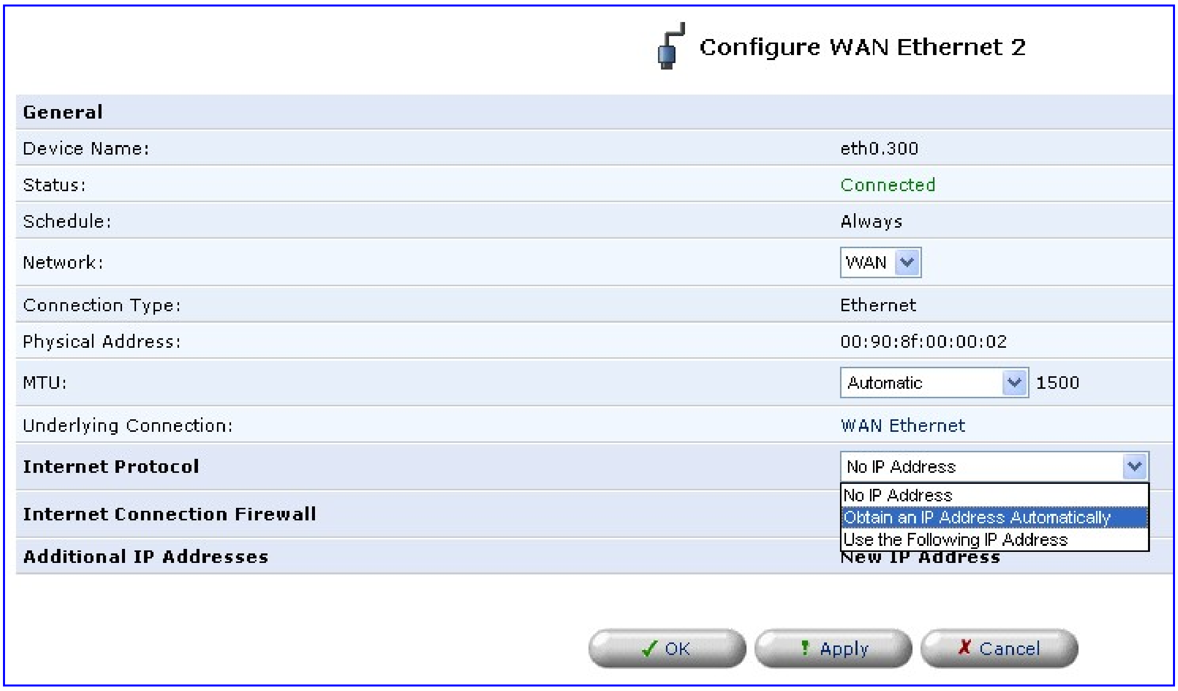
No IP Address
Obtain an IP Address Automatically
Use the Following IP Address

□ Override Subnet Mask:

DHCP Lease:

8. For WAN Ethernet 2 (VLAN ID 200), configure this interface to Obtain IP Address Automatically. Optionally, you can choose option 'Use the Following IP Address' for a static IP address.

Figure 10-44: Configuring WAN Ethernet



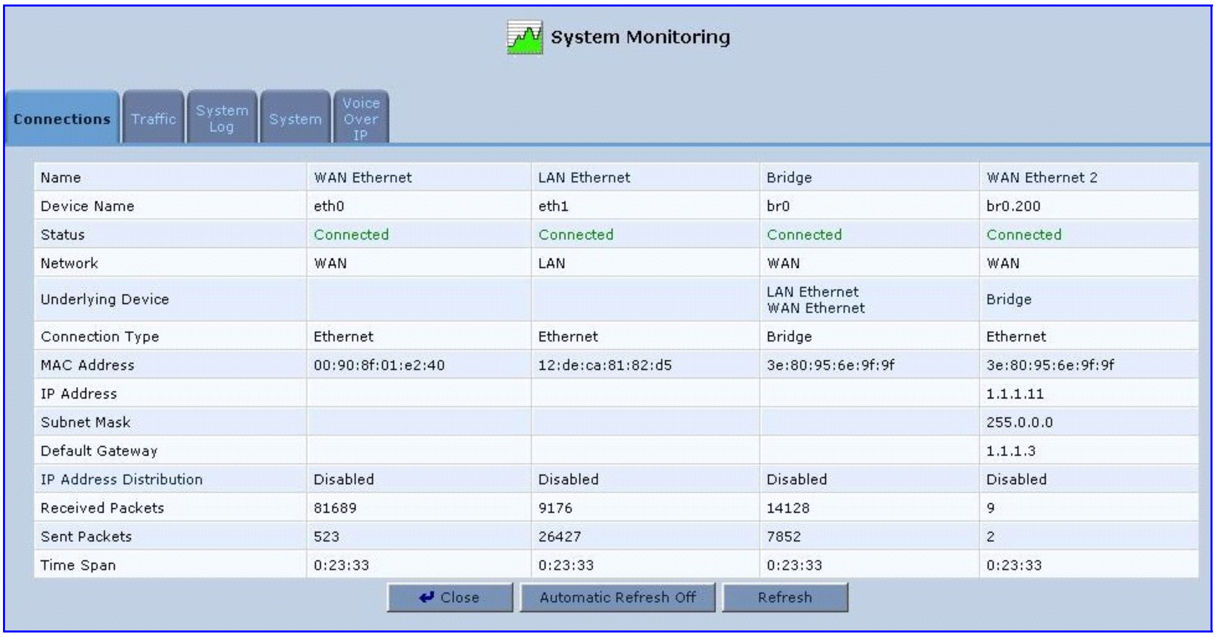
Configure WAN Ethernet 2

General	
Device Name:	eth0.300
Status:	Connected
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00:90:8f:00:00:02
MTU:	Automatic 1500
Underlying Connection:	WAN Ethernet
Internet Protocol	No IP Address
Internet Connection Firewall	
Additional IP Addresses	**New IP Address**

No IP Address
Obtain an IP Address Automatically
Use the Following IP Address
✓ OK
! Apply
✗ Cancel

9. Set your PC to use DHCP address; the figure below shows how the 'System Monitoring' screen should look.

Figure 10-45: System Monitoring



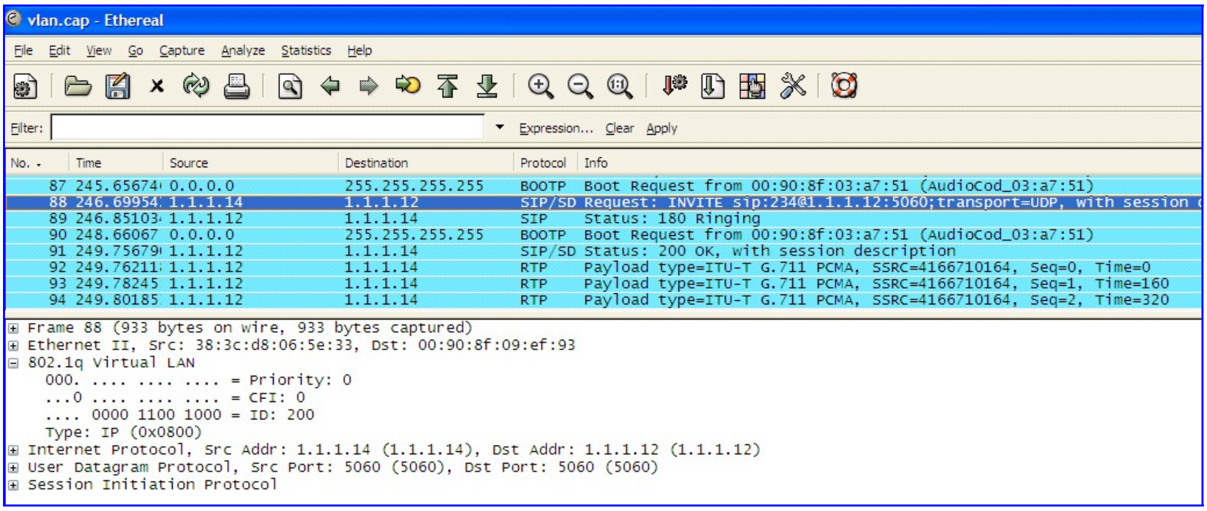
System Monitoring

Name	WAN Ethernet	LAN Ethernet	Bridge	WAN Ethernet 2
Device Name	eth0	eth1	br0	br0.200
Status	Connected	Connected	Connected	Connected
Network	WAN	LAN	WAN	WAN
Underlying Device			LAN Ethernet WAN Ethernet	Bridge
Connection Type	Ethernet	Ethernet	Bridge	Ethernet
MAC Address	00:90:8f:01:e2:40	12:de:ca:81:82:d5	3e:80:95:6e:9f:9f	3e:80:95:6e:9f:9f
IP Address				1.1.1.11
Subnet Mask				255.0.0.0
Default Gateway				1.1.1.3
IP Address Distribution	Disabled	Disabled	Disabled	Disabled
Received Packets	81689	9176	14128	9
Sent Packets	523	26427	7852	2
Time Span	0:23:33	0:23:33	0:23:33	0:23:33

Testing the Setup

1. Place a VoIP call and verify that VOIP is using 802.1q/p and that the VID is 200.

Figure 10-46: Testing the Setup


vlan.cap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

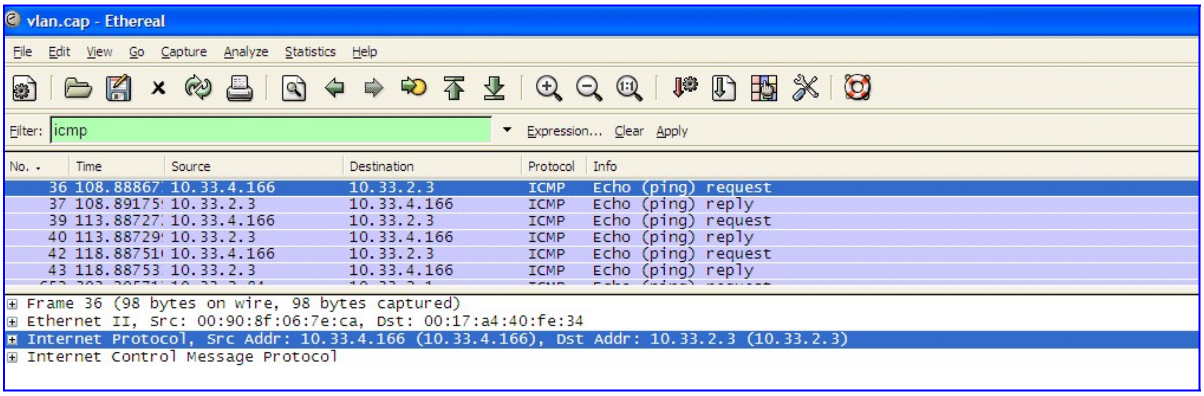
Filter:

```
No. .  Time       Source     Destination      Protocol Info
   87 245.65674  0.0.0.0    255.255.255.255  BOOTP    Boot Request from 00:90:8f:03:a7:51 (AudioCod_03:a7:51)
   88 246.69954  1.1.1.14   1.1.1.12         SIP/SD   Request: INVITE sip:234@1.1.1.12:5060;transport=UDP, with session
   89 246.85103  1.1.1.12   1.1.1.14         SIP      Status: 180 Ringing
   90 248.66067  0.0.0.0    255.255.255.255  BOOTP    Boot Request from 00:90:8f:03:a7:51 (AudioCod_03:a7:51)
   91 249.75679  1.1.1.12   1.1.1.14         SIP/SD   Status: 200 OK, with session description
   92 249.76211  1.1.1.12   1.1.1.14         RTP      Payload type=ITU-T G.711 PCMA, SSRC=4166710164, Seq=0, Time=0
   93 249.78245  1.1.1.12   1.1.1.14         RTP      Payload type=ITU-T G.711 PCMA, SSRC=4166710164, Seq=1, Time=160
   94 249.80185  1.1.1.12   1.1.1.14         RTP      Payload type=ITU-T G.711 PCMA, SSRC=4166710164, Seq=2, Time=320
```

```
⊞ Frame 88 (933 bytes on wire, 933 bytes captured)
⊞ Ethernet II, Src: 38:3c:d8:06:5e:33, Dst: 00:90:8f:09:ef:93
⊟ 802.1q Virtual LAN
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 1100 1000 = ID: 200
    Type: IP (0x0800)
⊞ Internet Protocol, Src Addr: 1.1.1.14 (1.1.1.14), Dst Addr: 1.1.1.12 (1.1.1.12)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊞ Session Initiation Protocol
```

2. Ping from the PC (connected to the LAN port of the MP-202) and verify that the data traffic (ICMP) is untagged (refer to the screen below).

Figure 10-47: Testing the Setup


vlan.cap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: icmp

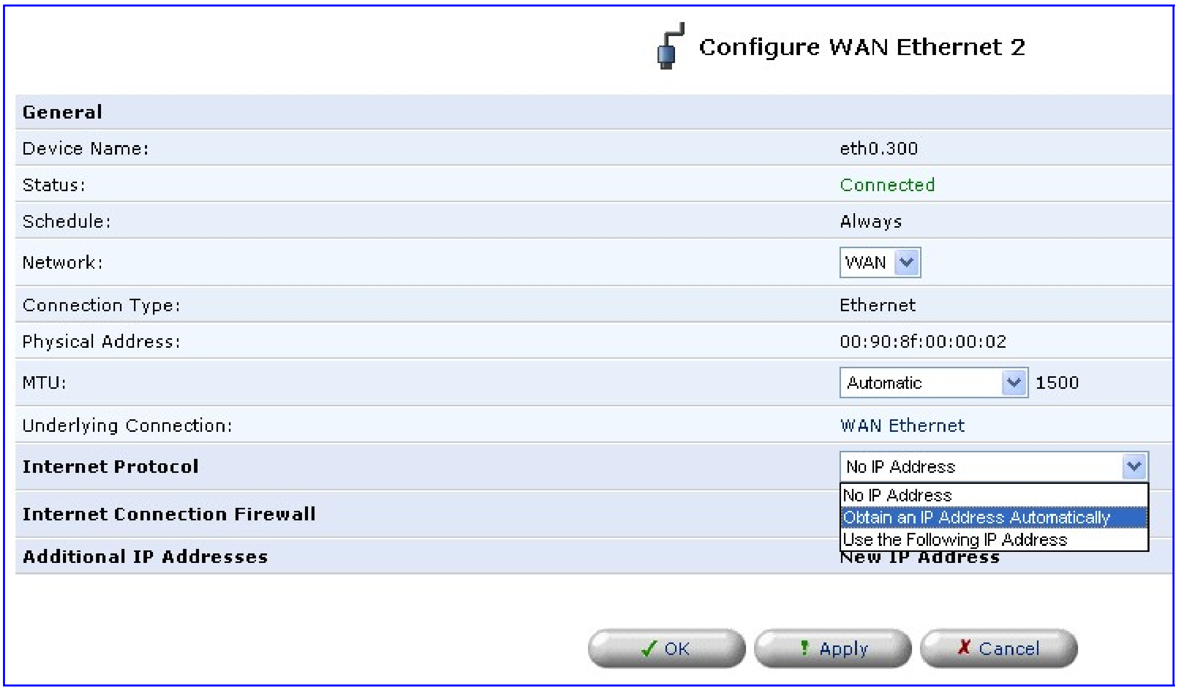
```
No. .  Time        Source       Destination   Protocol Info
   36 108.88867  10.33.4.166  10.33.2.3     ICMP     Echo (ping) request
   37 108.89175  10.33.2.3    10.33.4.166   ICMP     Echo (ping) reply
   39 113.88727  10.33.4.166  10.33.2.3     ICMP     Echo (ping) request
   40 113.88729  10.33.2.3    10.33.4.166   ICMP     Echo (ping) reply
   42 118.88751  10.33.4.166  10.33.2.3     ICMP     Echo (ping) request
   43 118.88753  10.33.2.3    10.33.4.166   ICMP     Echo (ping) reply
```

```
⊞ Frame 36 (98 bytes on wire, 98 bytes captured)
⊞ Ethernet II, Src: 00:90:8f:06:7e:ca, Dst: 00:17:a4:40:fe:34
⊞ Internet Protocol, Src Addr: 10.33.4.166 (10.33.4.166), Dst Addr: 10.33.2.3 (10.33.2.3)
⊞ Internet Control Message Protocol
```

10.2.5.3 Example 3 - Configuring VoIP and Data in the Same VLAN

➢ To configure VoIP and data in the same VLAN:

1. For VoIP and data, configure a VLAN ID and then configure each to 'Obtain IP Address Automatically' (refer to the figure below) (optionally, you can use a static IP address).



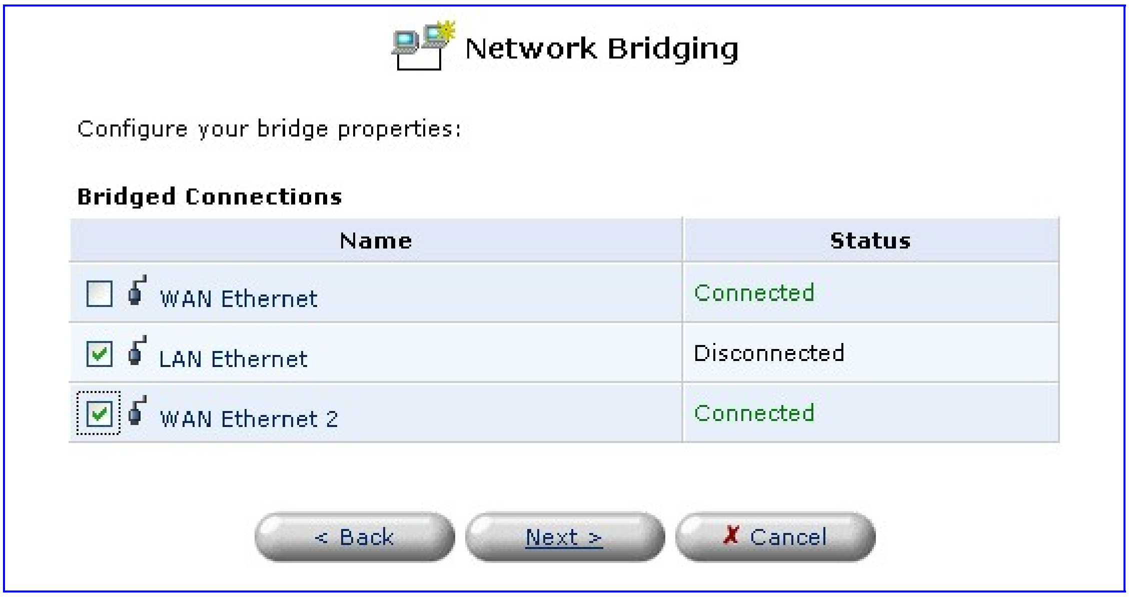
Configure WAN Ethernet 2

General	
Device Name:	eth0.300
Status:	Connected
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00:90:8f:00:00:02
MTU:	Automatic 1500
Underlying Connection:	WAN Ethernet
Internet Protocol	No IP Address
Internet Connection Firewall	
Additional IP Addresses	New IP Address

No IP Address
Obtain an IP Address Automatically
Use the Following IP Address
✓ OK
! Apply
✗ Cancel

2. Define a new network bridge. Define it by checking the check boxes of LAN Ethernet and the new VLAN Interface that you defined (refer to the figure below).

Figure 10-48: VoIP and Data on same VLAN



Network Bridging

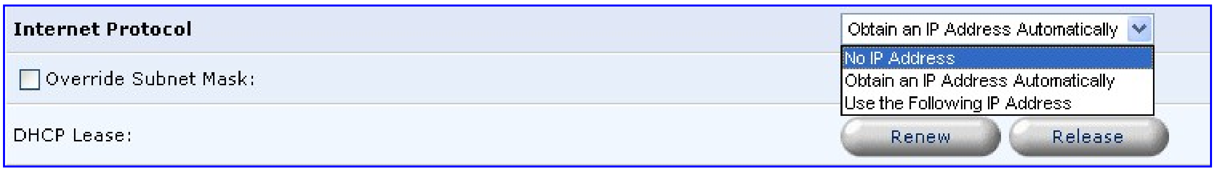
Configure your bridge properties:

Bridged Connections

Name	Status
□ WAN Ethernet	Connected
☑ LAN Ethernet	Disconnected
☑ WAN Ethernet 2	Connected

3. Go to the regular WAN and change the mode to 'No IP Address'

Figure 10-49: No IP Address



Internet Protocol: Obtain an IP Address Automatically

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

□ Override Subnet Mask:

DHCP Lease: Renew Release

If your configuration is correct, all data from the LAN and VoIP should be sent in the same VLAN.

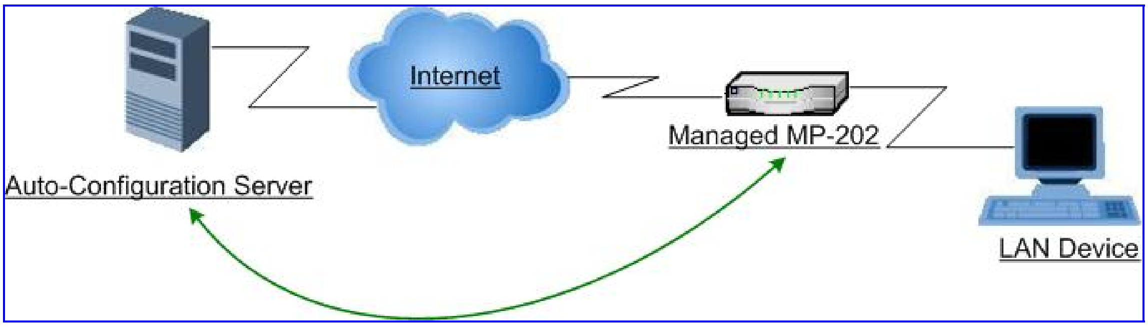
11 TR-069 CPE WAN Management Protocol

11.1 Overview

TR-069 is a WAN management protocol intended for communication between Customer Premise Equipment (CPE) or residential devices (such as the MP-202), and an Auto-Configuration Server (ACS). It defines a mechanism that encompasses secure auto configuration of CPE, and also incorporates other CPE management functions into a common framework.

In simpler terms, TR-069 is a protocol that enables remote server management of the MP-202. Such a protocol is useful, for example, for remotely and securely controlling the MP-202 by the CPE provider.

Figure 11-1: TR-069 CPE WAN Management Protocol



The TR-069 protocol allows an ACS to provision a CPE or collection of CPE based on a variety of criteria. The provisioning mechanism includes specific provisioning parameters and a general mechanism for adding vendor-specific provisioning capabilities as needed. The provisioning mechanism allows CPE provisioning at the time of initial connection to the broadband access network, and the ability to re-provision at any subsequent time. This includes support for asynchronous ACS-initiated re-provisioning of CPE. TR-069 defines several Remote Procedure Call (RPC) methods, as well as a large number of parameters, which may be set or read. Some of these methods and parameters are defined as mandatory. TR-098 is the DSLHome Internet Gateway Device Version 1.1 Data Model for TR-069.

11.2 TR-069 Parameter List

The DSL Forum TR-069 Technical Report species the TR-069 full parameter list, including the parameter type and description. For further information, refer to http://www.dslforum.org/aboutdsl/Technical_Reports/TR-069.pdf

Following is the list of the TR-069 objects supported by the MP-202. Objects that are partly supported have a detailed list of their implemented parameters. If not specified, the listed object is fully implemented.

- InternetGatewayDevice.
- InternetGatewayDevice.ManagementServer.
  - URL
  - Username

  - Password
  - PeriodicInformEnable
  - PeriodicInformInterval
  - PeriodicInformTime
  - ParameterKey
  - ConnectionRequestURL
  - ConnectionRequestUsername
  - ConnectionRequestPassword
- InternetGatewayDevice.DeviceInfo.
  - Manufacturer
  - ManufacturerOUI
  - ModelName
  - Description
  - Product Class
  - SerialNumber
  - HardwareVersion
  - SoftwareVersion
  - SpecVersion
  - ProvisioningCode
  - UpTime
  - DeviceLog
- InternetGatewayDevice.LANDevice.{i}
- InternetGatewayDevice.LANDevice.{i}.LANHostCongManagement.
  - DHCPServerEnable
  - MinAddress
  - MaxAddress
  - SubnetMask
  - DNSServers
- InternetGatewayDevice.LANDevice.{i}.Hosts.
- InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i}.
  - IPAddress
  - AddressSource
  - MACAddress
  - HostName
  - InterfaceType

- InternetGatewayDevice.LANDevice.{i}.LANEthernetInterfaceConfig.{}.
    - Status
    - MACAddress
    - MaxBitRate
- InternetGatewayDevice.LANDevice.{i}.LANEthernetInterfaceConfig. {}.Stats.
- InternetGatewayDevice.WANDevice.{i}.
- InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.
    - EnabledForInternet
    - WANAccessType
    - Layer1UpstreamMaxBitRate
    - Layer1DownstreamMaxBitRate
    - PhysicalLinkStatus
    - TotalBytesSent
    - TotalBytesReceived
    - TotalPacketsSent
    - TotalPacketsReceived
- InternetGatewayDevice.WANDevice.{i}.WANDSLConnectionManagement.
- InternetGatewayDevice.WANDevice.{i}.WANDSLConnectionManagement. ConnectionService.{i}.
- InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.
- InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.
    - WANDSLLinkCong.
    - Enable
    - LinkStatus
    - LinkType
    - AutoCong
    - DestinationAddress
    - ATMTransmittedBlocks
    - ATMReceivedBlocks
- InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.
    - WANPPPConnection.{i}.
    - Enable
    - ConnectionStatus
    - ConnectionType
    - Name
    - Uptime

- Username
- Password
- ExternalIPAddress
- DNSServers
- TransportType
- PPPoEACName
- PPPoEServiceName

The MP-202 supports the following Remote Procedure Calls (RPCs):

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- GetParameterNames
- SetParameterAttributes
- GetParameterAttributes
- AddObject
- DeleteObject
- Download
- Reboot

Note that the implementation of SetParameterAttributes is empty; MP-202 does not implement access control nor notifications as defined in the specification.

11.2.1 Viewing, Changing TR-069 Parameters Using the CLI

TR-069 parameters can be viewed and configured via the CLI. This section presents a specific example of how to view and change TR-069 parameters. Use the example as a guide.

➢ To run CLI commands:

1. Open Telnet
2. Access the system from a PC connected to the LAN port of the MP-202 Telnet 192.168.2.1
3. Enter the administrator user and password.

➢ To view the current TR-069 settings, run these commands:

```
rg_conf_print manufacturer/vendor_name
rg_conf_print manufacturer/vendor_oui
rg_conf_print manufacturer/product_class
rg_conf_print manufacturer/model_number
rg_conf_print manufacturer/hardware/serial_num
rg_conf_print cwmp/acs_url
rg_conf_print cwmp/username
rg_conf_print_obscure cwmp/password
rg_conf_print cwmp/conn_req_username
rg_conf_print_obscure cwmp/conn_req_password
```

➢ To change a TR-069 parameter, use the following API:

```
rg_conf_set manufacturer/vendor_name CompanyName
rg_conf_set manufacturer/vendor_oui 12AB56 (Organizationally
Unique Identifier; AudioCodes' OUI is 00908F)
rg_conf_set manufacturer/product_class MP-20X
rg_conf_set manufacturer/model_number MP-20X
rg_conf_set manufacturer/hardware/serial_num 123456
rg_conf_set cwmp/acs_url http://acsurl.com
rg_conf_set cwmp/username cpe
rg_conf_set_obscure cwmp/password 123456
rg_conf_set cwmp/conn_req_username acl
rg_conf_set_obscure cwmp/conn_req_password 123
```

➢ If a parameter is changed, activate the following CLI commands:

```
rg_conf_set  cwmp/enabled  1
reconf 1
```

➢ To stop and restart the TR-69 client, use the following CLI commands:

```
cwmp_session_start
cwmp_session_stop
```

Table 11-1: TR-069 Parameter Descriptions

Name	Type	Description
Manufacturer	String(64)	Manufacturer of the device (for display only).
OUI	String(6)	Organizationally unique identifier of the device manufacturer. Represented as a six hexadecimal-digit value using all upper-case letters and including any leading zeros. The value MUST be a valid OUI.
ProductClass	String(64)	Identifier of the class of product for which the serial number applies. That is, for a given manufacturer, this parameter is used to identify the product or class of product over which the parameter SerialNumber is unique.
SerialNumber	String(64)	Identifier of the particular device that is unique for the indicated class of product and manufacturer.

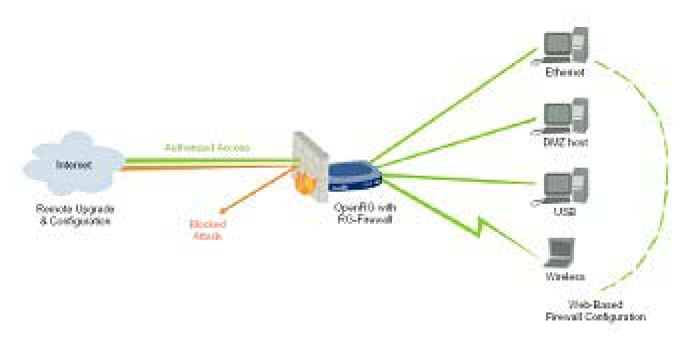
Reader's Notes

12 Security

The MP-202's security suite includes comprehensive and robust security services: Stateful Packet Inspection Firewall, user authentication protocols and password protection mechanisms. These features together allow users to connect their computers to the Internet and simultaneously be protected from the security threats of the Internet.

The firewall, which is the cornerstone of your Telephone Adapter's security suite, has been exclusively tailored to the needs of the residential/office user and has been pre-configured to provide optimum security (refer to the figure below).

Figure 12-1: Firewall in Action



The MP-202 firewall provides both the security and flexibility that home and office users seek. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as Internet gaming and video-conferencing.

Additional features, including surfing restrictions and access control, can also be easily configured locally by the user through a user-friendly Web-based interface, or remotely by a service provider.

The MP-202 firewall supports advanced filtering, designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN network devices.

The Web-based management screens in the Security section feature the following:

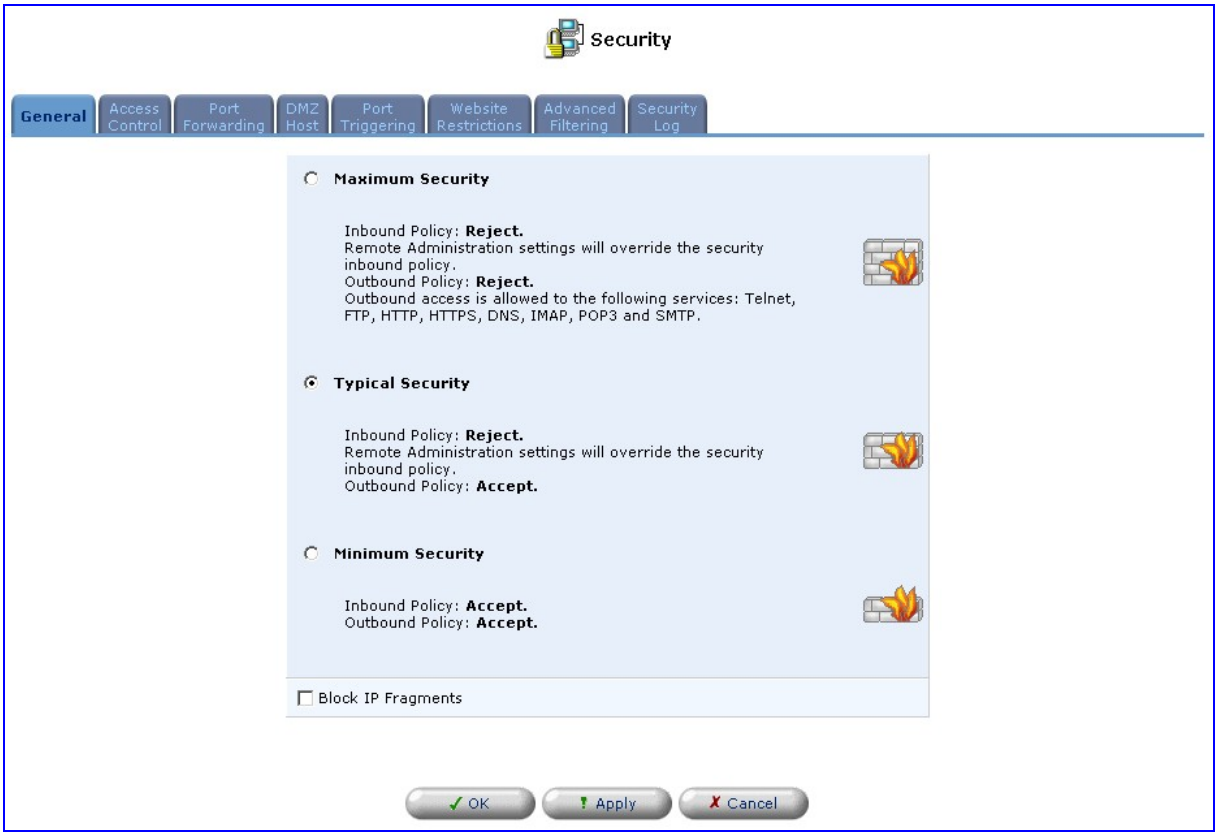
- The 'General' screen allows you to choose the security level for the firewall (refer to" General Security Level Settings" on page 136)
- The 'Access Control' screen can be used to restrict access from the home network to the Internet (refer to "Local Servers (Port Forwarding)" on page 140).
- The 'Port Forwarding' screen can be used to enable access from the Internet to specified services provided by computers in the home network and special Internet applications (refer to "Port Forwarding" on page 140)
- The 'DMZ Host' screen allows you to configure a LAN host to receive all traffic arriving at your Telephone Adapter, which does not belong to a known session (refer to" Port Triggering" on page 145).
- The 'Port Triggering' screen allows you to define port triggering entries, to dynamically open the firewall for some protocols or ports. (refer to "Remote Administration" on page 163).

- The 'Website Restrictions' allows you to block LAN access to a certain host or web site on the Internet. (refer to "Website Restrictions" on page 148).
- 'Advanced Filtering' allows you to implicitly control the firewall setting and rules (refer to "Advanced Filtering" on page 151).
- 'Security Log' allows you to view and configure the firewall Log (refer to Security Log).

12.1 General Security Level Settings

Use the 'Security Settings' screen to configure the Telephone Adapter's basic security settings (refer to the figure below).

Figure 12-2: General Security Level Settings



○ Maximum Security

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Reject.**
Outbound access is allowed to the following services: Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

● Typical Security

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Accept.**

○ Minimum Security

Inbound Policy: **Accept.**
Outbound Policy: **Accept.**

□ Block IP Fragments

The firewall regulates the flow of data between the home network and the Internet. Both incoming and outgoing data are inspected and then either accepted (allowed to pass through the MP-202) or rejected (barred from passing through the MP-202) according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing home users access to the Internet services that they require.

The firewall rules specify what types of services available on the Internet may be accessed from the home network and what types of services available in the home network may be accessed from the Internet. Each request for a service that the firewall receives, whether originating in the Internet or from a computer in the home network, is checked against the set of firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, then all subsequent data associated with this request (a "session") will also be allowed to pass, regardless of its direction.

For example, when you point your Web browser to a Web page on the Internet, a request is sent out to the Internet for this page. When the request reaches the MP-202, the firewall will identify the request type and origin--HTTP and a specific PC in your home network, in this case. Unless you have configured access control to block requests of this type from this computer, the firewall will allow this request to pass out onto the Internet (refer to "WAN PPPoE" on page 82 for more on setting access controls). When the Web page is returned from the Web server the firewall will associate it with this session and allow it to pass, regardless of whether HTTP access from the Internet to the home network is blocked or permitted.

Note that it is the *origin of the request*, not subsequent responses to this request, that determines whether a session can be established or not.

You can choose from among three pre-defined security levels for the MP-202: Minimum, Typical, and Maximum (the default setting). The table below summarizes the behavior of the MP-202 for each of the three security levels.

Table 12-1: Behavior for the Three Security Levels

Security Level	Requests Originating in the WAN (Incoming Traffic)	Requests Originating in the LAN (Outgoing Traffic)
Maximum Security (Default)	Blocked: No access to home network from Internet, except as configured in the Local Servers, DMZ host and Remote Access screens	Limited: Only commonly- used services, such as Web- browsing and e-mail, are permitted
Typical Security	Blocked: No access to home network from Internet, except as configured in the Local Servers, DMZ host and Remote Access screens	Unrestricted: All services are permitted, except as configured in the Access Control screen
Minimum Security	Unrestricted: Permits full access from Internet to home network; all connection attempts permitted.	Unrestricted: All services are permitted, except as configured in the Access Control screen

These services include Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

The list of allowed services at 'Maximum Security' mode can be edited in the screen" 'Access Contro"l on page 138'.

Some applications (such as some Internet messengers and Peer-To-Peer client applications) tend to use these ports if they cannot connect with their own default ports. When applying this behaviour, these applications will not be blocked outbound, even at Maximum Security Level.

➢ To configure the MP-202's security settings:

(Refer to the figure 'General Security Level Settings')

1. Choose from among the three predefined security levels described in the table above. 'Maximum Security' is the default setting.

   Using the Minimum Security setting may expose the home network to significant security risks, and thus should only be used, when necessary, for short periods of time.

2. Check the 'Block IP Fragments' box in order to protect your home network from a common type of hacker attack that could make use of fragmented data packets to sabotage your home network. Note that VPN over IPSec and some UDP-based services make legitimate use of IP fragments. You will need to allow IP fragments to pass into the home network in order to make use of these select services.

3. Click 'OK' to save the changes.

12.2 Access Control

You may want to block specific computers within the home network (or even the whole network) from accessing certain services on the Internet. For example, you may want to prohibit one computer from surfing the Web, another computer from transferring files using FTP, and the whole network from receiving incoming e-mail.

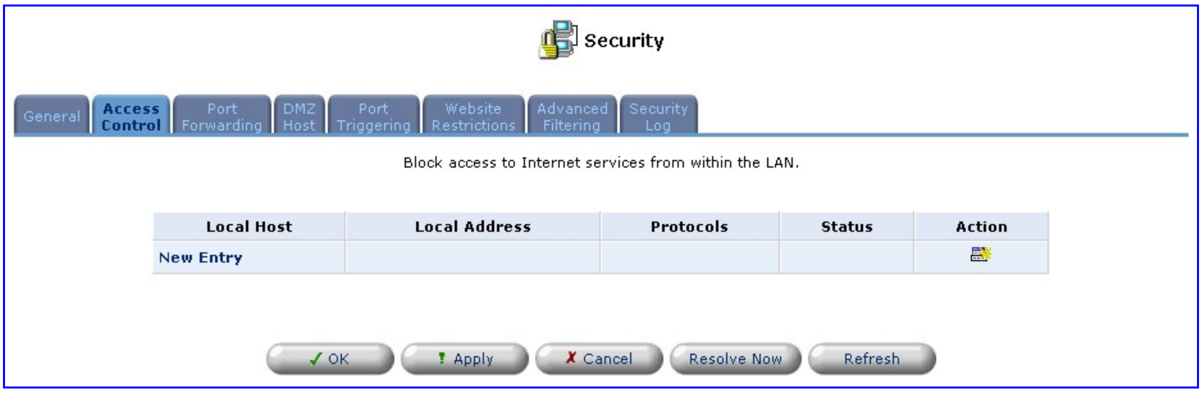
Access Control defines restrictions on the types of requests that may pass from the home network out to the Internet, and thus may block traffic flowing in both directions. In the e-mail example given above, you may prevent computers in the home network from receiving e-mail by blocking their *outgoing* requests to POP3 servers on the Internet.

There are services you should consider blocking, such as popular game and file sharing servers. For example, to ensure that your employees do not put your business at risk from illegally traded copyright files, you may want to block several popular P2P and file sharing applications.

➢ To view and allow/restrict these services:

1. In the 'Security' screen (refer to the figure above), click tab 'Access Control'; the screen 'Access Control' opens (refer to the figure below).

Figure 12-3: Access Control

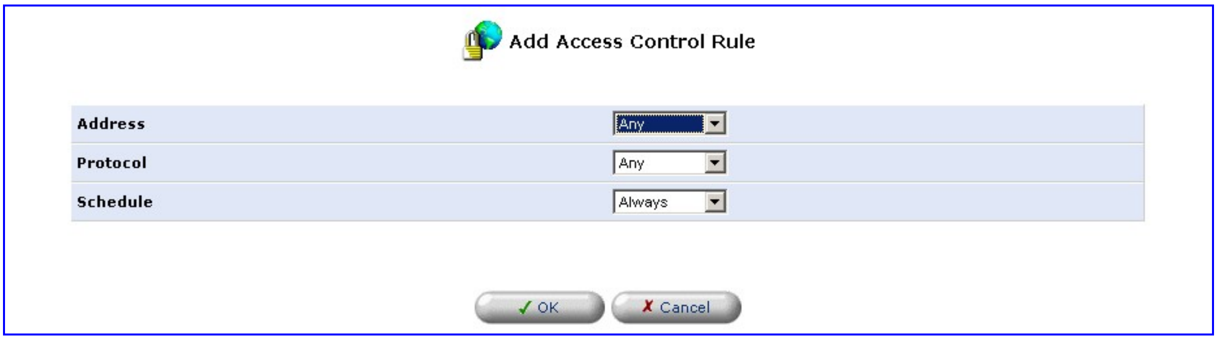


Block access to Internet services from within the LAN.

Local Host	Local Address	Protocols	Status	Action
New Entry				

2. Click the link 'New Entry'; the screen 'Add Access Control Rule' opens (refer to the figure below).

Figure 12-4: Add Access Control Rule



Add Access Control Rule

Address	Any
Protocol	Any
Schedule	Always

3. The parameter 'Address' enables you to specify the computer or group of computers for which you would like to apply the access control rule. You can select between any or a specifc computer address in your LAN. If you choose the 'Specify Address' option, the screen will refresh, and an 'Add' link appears. Click it to specify a computer address. Specify an address by creating a 'Network Object'.

4. The parameter 'Protocol' lets you select or specify the type of protocol to be used. In addition to the list of popular protocols it provides, you may also choose any or a specifc protocol. If you choose option 'Specify Protocol', the screen refreshes and an 'Add' link appears. Click it to specify a protocol address.

5. The parameter 'Schedule' allows you to define the time period during which this rule will take effect. You can select between 'Always' or a specific schedule. If you choose the option 'Specify Schedule', the screen refreshes and an 'Add' link appears. Click it to specify a schedule.

6. Click OK to save your settings; the 'Access Control' screen displays a summary of the rule that you just added. Click 'Edit' to edit the access control rule for the service; the screen 'Edit Service' opens.

7. Select the network group to which you would like to apply the rule and the schedule during which the rule will take effect.

8. Click 'OK' to save your changes and return to the 'Access Control' screen.

You can disable an access control rule and make the service available without having to remove the service from 'Access Control'. This can be useful when making the service only temporarily available and when expecting to reinstate the restriction in the future.

- To temporarily disable rule, clear the check box adjacent to the service name.
- To reinstate the restriction at a later time, recheck it.
- To remove a rule, click the action icon 'Remove' for the service; the service is removed from 'Access Control'.

Note: When Web Filtering is enabled, HTTP services cannot be blocked by Access Control.

12.3 Port Forwarding

In its default state, the gateway blocks all external users from connecting to or communicating with your network. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may want to expose your network to the Internet in certain limited and controlled ways in order to enable some applications to work from the LAN (game, voice and chat applications, for example) and to enable Internet-access to servers in the home network. The Port Forwarding feature supports both of these functionalities.

The 'Port Forwarding' screen lets you define the applications that require special handling by the gateway. You must select the application's protocol and the local IP address of the computer that will be using or providing the service. If required, you can add new protocols in addition to the most common ones provided by the gateway.

For example, to use an FTP application on one of your PCs, select 'FTP' from the list and enter the local IP address or host name of the designated computer; all FTP-related data arriving at the gateway from the Internet is then forwarded to the specified computer.

Similarly, to grant Internet users access to servers inside your home network, you must identify each service that you want to provide and the PC that will provide it. For example, to host a Web server inside the home network you must select 'HTTP' from the list of protocols and enter the local IP address or host name of the computer that will host the Web server. When an Internet user points her browser to the external IP address of the gateway, it forwards the incoming HTTP request to the computer that is hosting the Web server.

Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated. If for example you have a Web server running on your PC on port 8080 and you want to grant access to this server to anyone who accesses the gateway via HTTP, do the following:

- Define a port forwarding rule for the HTTP service, with the PC's IP or host name.
- Specify 8080 in the field 'Forward to Port'.

All incoming HTTP traffic will now be forwarded to the PC running the Web server on port 8080.

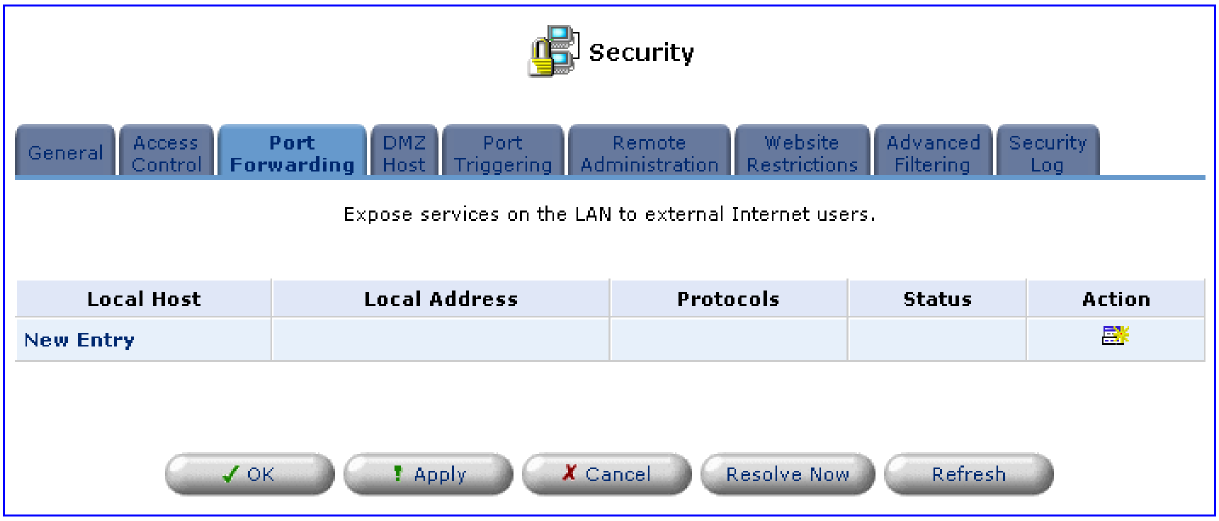
When setting a port forwarding service, you must ensure that the port is not already in use by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP - the port used by the gateway's VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents.

Note: Some applications, such as FTP, TFTP, PPTP and H323, require the support of special specific Application Level Gateway (ALG) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. OpenRG is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network.
The ALG is automatically assigned based on the destination port.

➢ To add a new port forwarding service:

1. Select the tab 'Port Forwarding' in the screen 'Security'; the screen 'Port Forwarding' opens (refer to the figure).

Figure 12-5: Port Forwarding

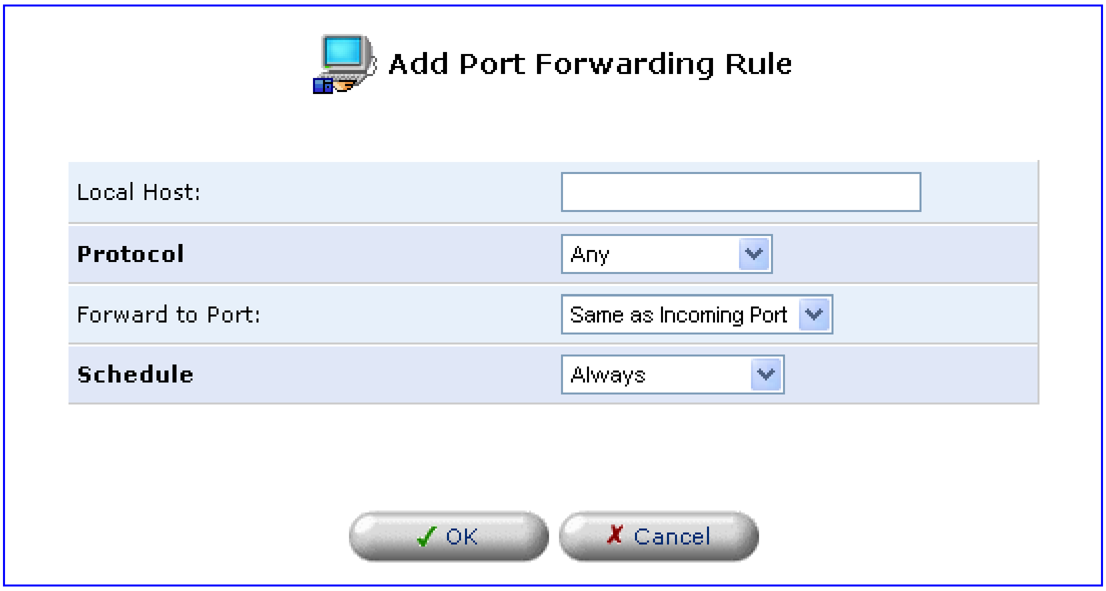


Expose services on the LAN to external Internet users.

Local Host	Local Address	Protocols	Status	Action
New Entry				

2. Click the link 'New Entry'; the screen 'Add Port Forwarding Rule' opens (refer to the figure).

Figure 12-6: Add Port Forwarding Rule

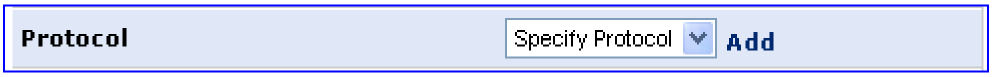


Local Host:	
Protocol	Any
Forward to Port:	Same as Incoming Port
Schedule	Always

3. Enter the IP address or the host name of the computer that will provide the service (the 'server'). Note that only one LAN computer can be assigned to provide a specific service or application.

The Protocol combo box lets you select or specify the type of protocol that will be used. In addition to the list of popular protocols it provides, you may also choose any or a specific protocol. If you choose the option 'Specify Protocol', the screen refreshes and an 'Add' link appears:

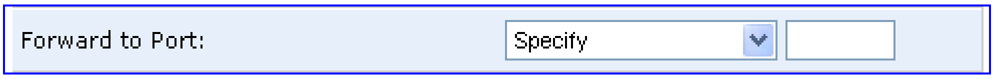
Figure 12-7: Add a Specific Protocol



Protocol Specify Protocol ▾ **Add**

4. Click the link 'Add' to specify a protocol; by default, the gateway forwards traffic to the same port as the incoming port. To redirect traffic to a different port, select the option 'Specify'; the screen refreshes and an additional field appears, enabling you to enter the port number:

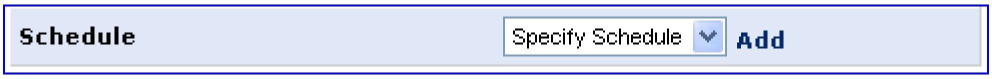
Figure 12-8: Forward to a Specific Port



Forward to Port: Specify ▾

5. To define the time period during which this rule will take effect, select The in the drop-down list 'Schedule' between 'Always' or a specific schedule. If you choose the option 'Specify Schedule', the screen refreshes and an 'Add' link appears:

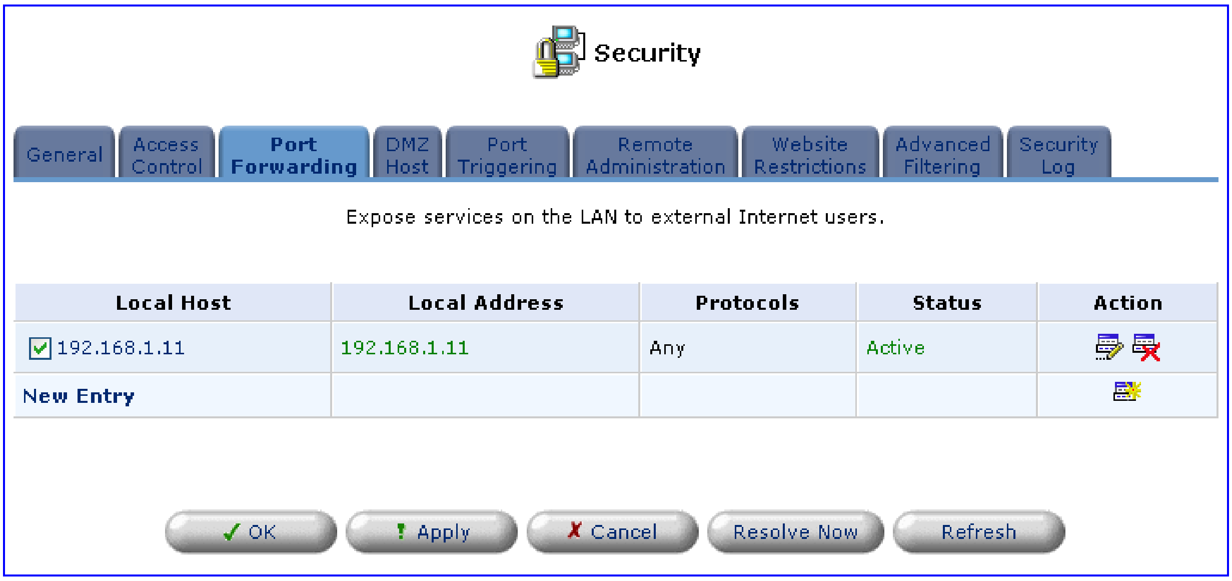
Figure 12-9: Add a Specific Schedule



Schedule Specify Schedule ▾ **Add**

6. Click 'Add' to specify a protocol and click 'OK' to save your changes; the screen 'Port Forwarding' displays a summary of the rule that you just added (refer to the figure).

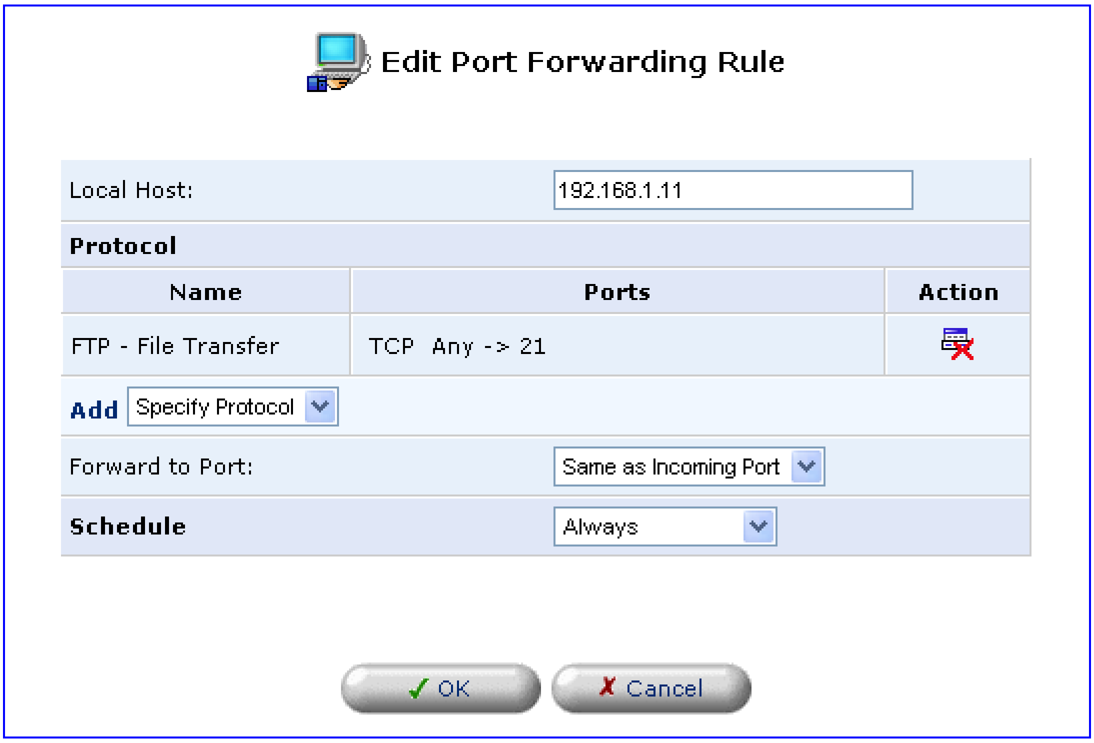
Figure 12-10: Port Forwarding Rule



Expose services on the LAN to external Internet users.

Local Host	Local Address	Protocols	Status	Action
☑ 192.168.1.11	192.168.1.11	Any	Active	
New Entry				

7. Edit the port forwarding rule by modifying its entry under column 'Local Host' in the screen 'Port Forwarding'. To modify an entry, click the action icon 'Edit' for the rule; the screen 'Edit Port Forwarding Rule' opens (refer to the figure). This screen allows you to edit all the parameters that you configured when creating the port forwarding rule.



Edit Port Forwarding Rule

Local Host: 192.168.1.11

Protocol

Name	Ports	Action
FTP - File Transfer	TCP Any -> 21	☒

Add Specify Protocol

Forward to Port: Same as Incoming Port

Schedule Always

8. Click 'OK' to save your changes and return to the screen 'Port Forwarding'.

9. You can disable a port forwarding rule to make a service unavailable without having to remove the rule from the screen 'Port Forwarding'. This can be useful when making the service temporarily unavailable and when expecting to reinstate it in the future.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, reselect the check box.
- To remove a rule, click the action icon 'Remove' for the service; the service is permanently removed.

How many computers can use a service or play a game simultaneously? All computers on the network can use a specific service as clients simultaneously. Being a client means that the computer within the network initiates the connection - for example, opens an FTP connection with an FTP server on the Internet. But only one computer can serve as a server, meaning responding to requests from computers on the Internet. Assigning a specific computer as a server is done in the Port Forwarding section of Web-based management.

12.4 DMZ Host

The DMZ (Demilitarized) Host feature allows one local computer to be exposed to the Internet.

Designate a DMZ host to:

- Use a special-purpose Internet service, such as an on-line game or video-conferencing program, that is not present in the Local Servers list and for which no port range information is available.
- To expose one computer to all services, without restriction, irrespective of security.

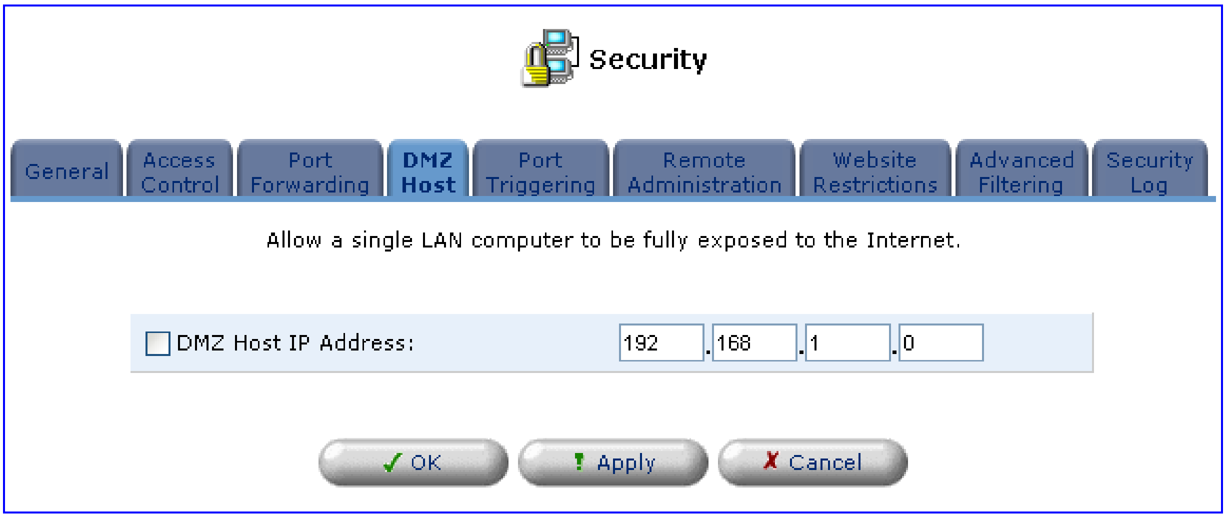
Warning: A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

An incoming request for access to a service in the home network, such as a Web-server, is fielded by the MP-202. The MP-202 will forward this request to the DMZ host (if one is designated) unless the service is being provided by another PC in the home network (assigned in Local Servers), in which case that PC will receive the request instead.

➢ To designate a local computer as a DMZ Host:

1. Click tab 'DMZ Host'; the screen 'DMZ Host' opens (refer to the figure).

Figure 12-11: DMZ Host



Allow a single LAN computer to be fully exposed to the Internet.

☐ DMZ Host IP Address: 192 . 168 . 1 . 0

2. Enter the local IP address of the computer to be designated as a DMZ host. Note that only one LAN computer can be a DMZ host at any time.
3. Click 'OK' to save your changes and return to the screen 'DMZ Host'.

You can disable the DMZ host so that it will not be fully exposed to the Internet, but keep its IP address recorded on the 'DMZ Host' screen. This may be useful if you wish to disable the DMZ host but expect that you will want to enable it again in the future.

- To disable the DMZ host so that it will not be fully exposed to the Internet, clear the check-box next to the DMZ IP designation and click 'OK'.
- To re-enable the DMZ host later, recheck the check-box.

12.5 Port Triggering

Port triggering can be used for dynamic port forwarding configuration. By setting port triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering since the outbound traffic triggers to which ports inbound traffic is directed.

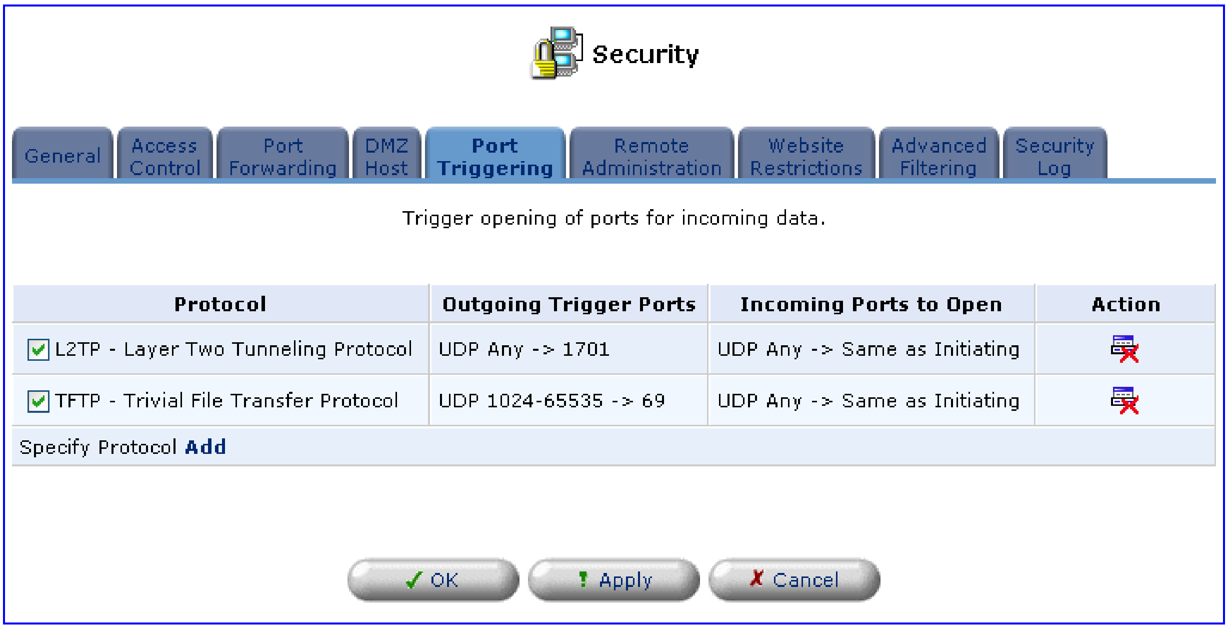
For example, consider a gaming server that is accessed using UDP protocol on port 2222. The gaming server responds by connecting the user using UDP on port 3333 when starting gaming sessions. In such a case you must use port triggering, since this scenario conflicts with the following default firewall settings:

- The firewall blocks inbound traffic by default.
- The server replies to the gateway's IP, and the connection is not sent back to your host, since it is not part of a session.

To solve this, you need to define a Port Triggering entry, which allows inbound traffic on UDP port 3333, only after a LAN host generated traffic to UDP port 2222. This results in accepting the inbound traffic from the gaming server and sending it back to the LAN Host which originated the outgoing traffic to UDP port 2222.

Select the tab 'Port Triggering' in the 'Security' screen; the screen 'Port Triggering' opens (refer to the figure). The screen lists all port triggering entries.

Figure 12-12: Port Triggering



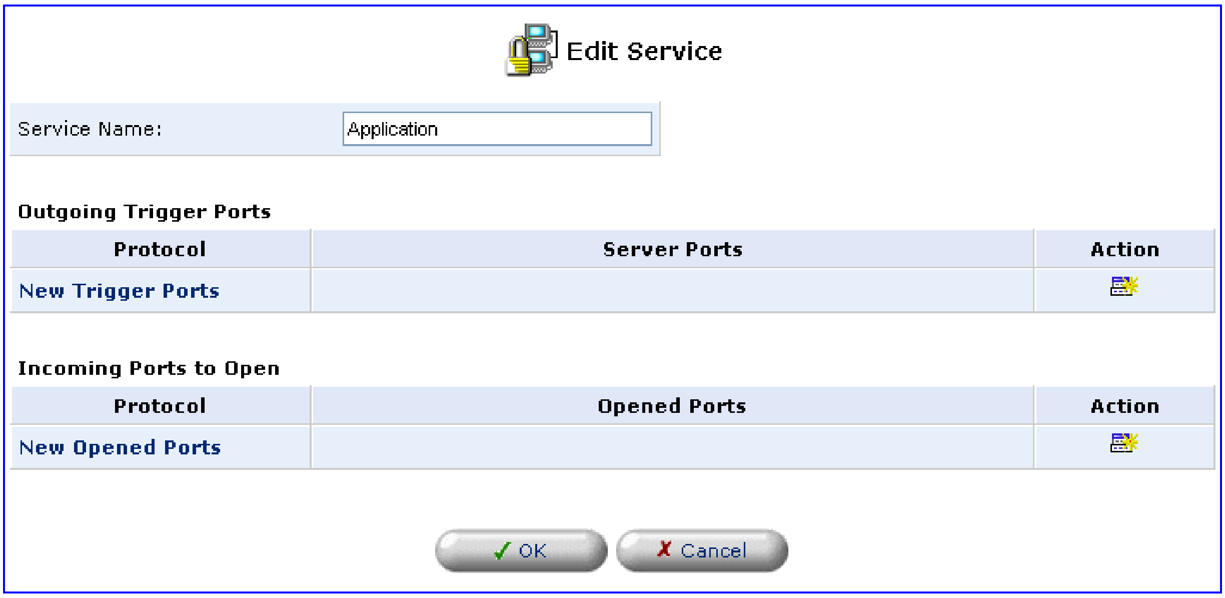
Trigger opening of ports for incoming data.

Protocol	Outgoing Trigger Ports	Incoming Ports to Open	Action
☑ L2TP - Layer Two Tunneling Protocol	UDP Any -> 1701	UDP Any -> Same as Initiating	✗
☑ TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	UDP Any -> Same as Initiating	✗
Specify Protocol **Add**			

➢ To add an entry for the gaming example above:

1. Click the link 'Add' to add an entry; the screen 'Edit Service' opens (refer to the figure).

Figure 12-13: Adding Port Triggering Rules



Edit Service

Service Name: Application

Outgoing Trigger Ports

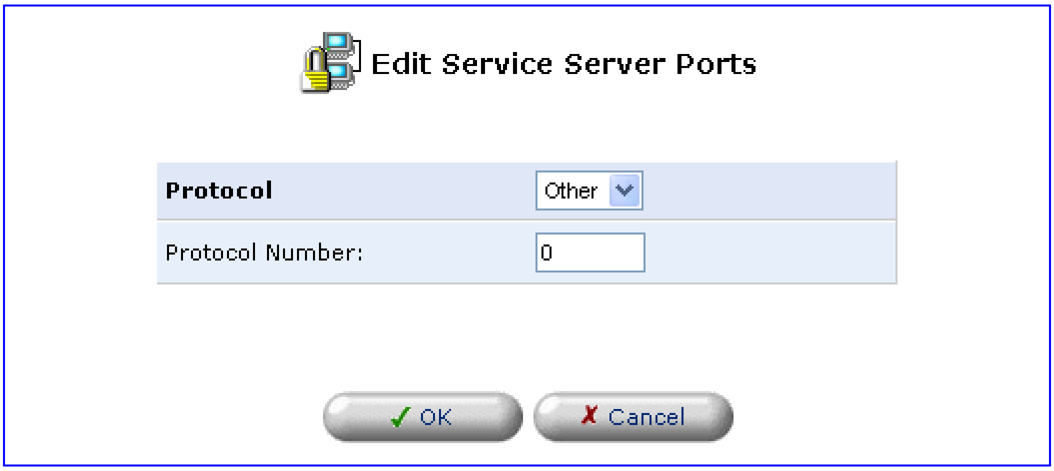
Protocol	Server Ports	Action
New Trigger Ports		

Incoming Ports to Open

Protocol	Opened Ports	Action
New Opened Ports		

2. Enter a name for the service (e.g., 'game_server') and click the link 'New Trigger Ports'; the screen 'Edit Service Server Ports' opens (refer to the figure).

Figure 12-14: Edit Service Server Ports



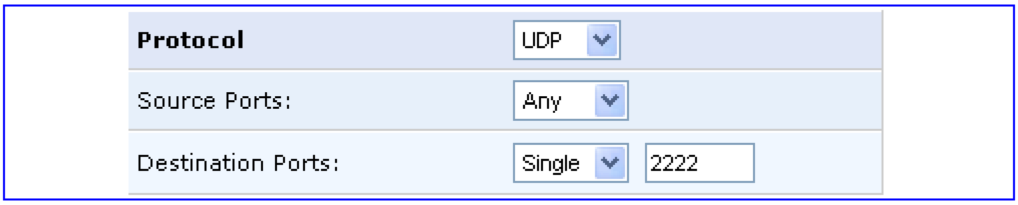
Edit Service Server Ports

Protocol	Other
Protocol Number:	0

3. In the Protocol combo-box, select UDP; the screen refreshes, providing source and destination port options (refer to the figure).

4. Leave the Source Ports combo-box at its default 'Any'. In the drop-down list 'Destination Ports', select 'Single'; the screen refreshes again, providing an additional field in which you should enter '2222' as the destination port.

Figure 12-15: Edit Service Server Ports

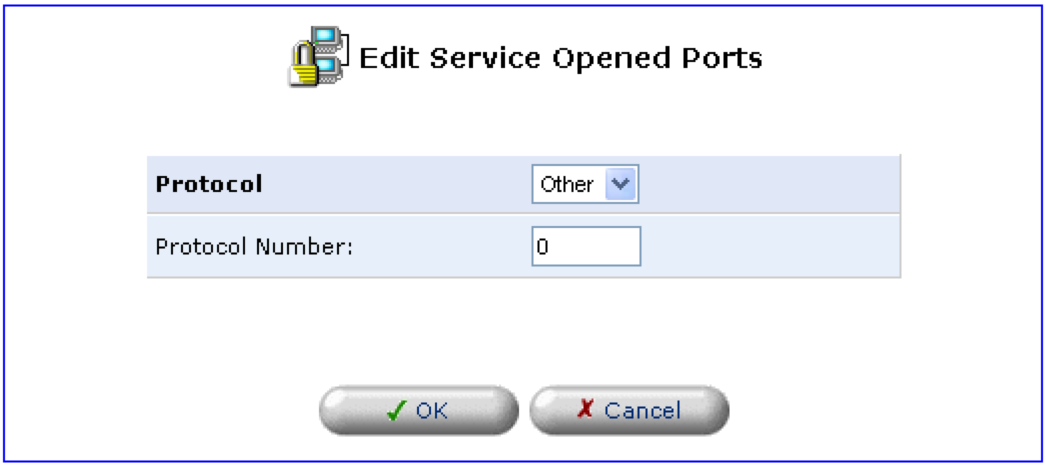


Protocol	UDP	
Source Ports:	Any	
Destination Ports:	Single	2222

5. Click 'OK' to save the settings.

6. In the screen 'Edit Service', click the link 'New Opened Ports'; the screen 'Edit Service Opened Ports' opens (refer to the figure).

Figure 12-16: Edit Service Opened Ports

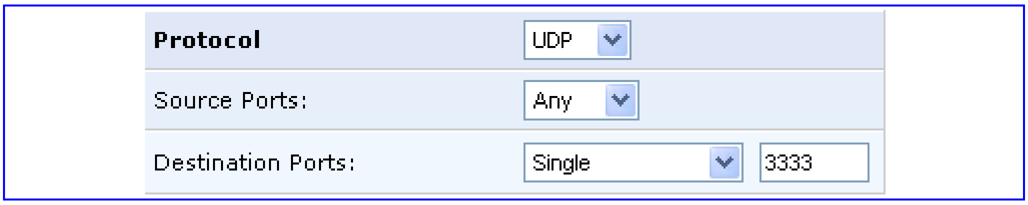


Edit Service Opened Ports

Protocol	Other
Protocol Number:	0

7. Similar to the trigger ports screen, select UDP as the protocol, leave the source port at 'Any', and enter a 3333 as the single destination port (refer to the figure).

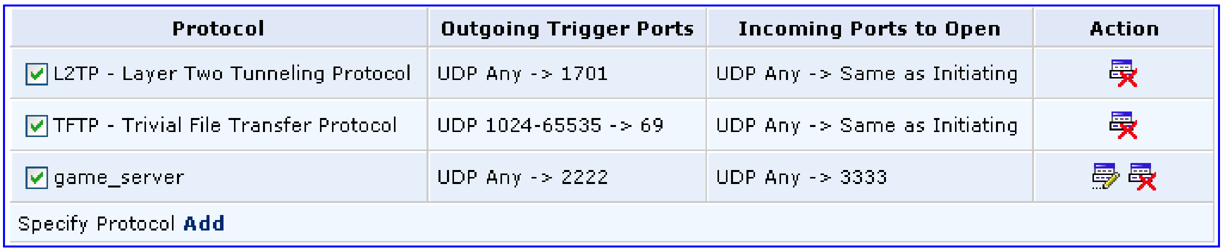
Figure 12-17: Edit Service Opened Ports



Protocol	UDP	
Source Ports:	Any	
Destination Ports:	Single	3333

8. Click 'OK' to save the settings; the screen 'Edit Service' presents your entered information. Click 'OK' again to save the port triggering rule; the screen 'Port Triggering' now includes the new port triggering entry (refer to the figure).

Figure 12-18: New Port Triggering Rule



Protocol	Outgoing Trigger Ports	Incoming Ports to Open	Action
☑ L2TP - Layer Two Tunneling Protocol	UDP Any -> 1701	UDP Any -> Same as Initiating	✖
☑ TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	UDP Any -> Same as Initiating	✖
☑ game_server	UDP Any -> 2222	UDP Any -> 3333	✎ ✖
Specify Protocol **Add**			

You can disable a port triggering rule without having to remove it from the screen 'Port Triggering'.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it later, simply reselect the check box.
- To remove a rule, click the action icon 'Remove' for the service; the service is permanently removed.

There may be a few default port triggering rules listed when you first access the port triggering screen. Note that disabling these rules may result in impaired gateway functionality.

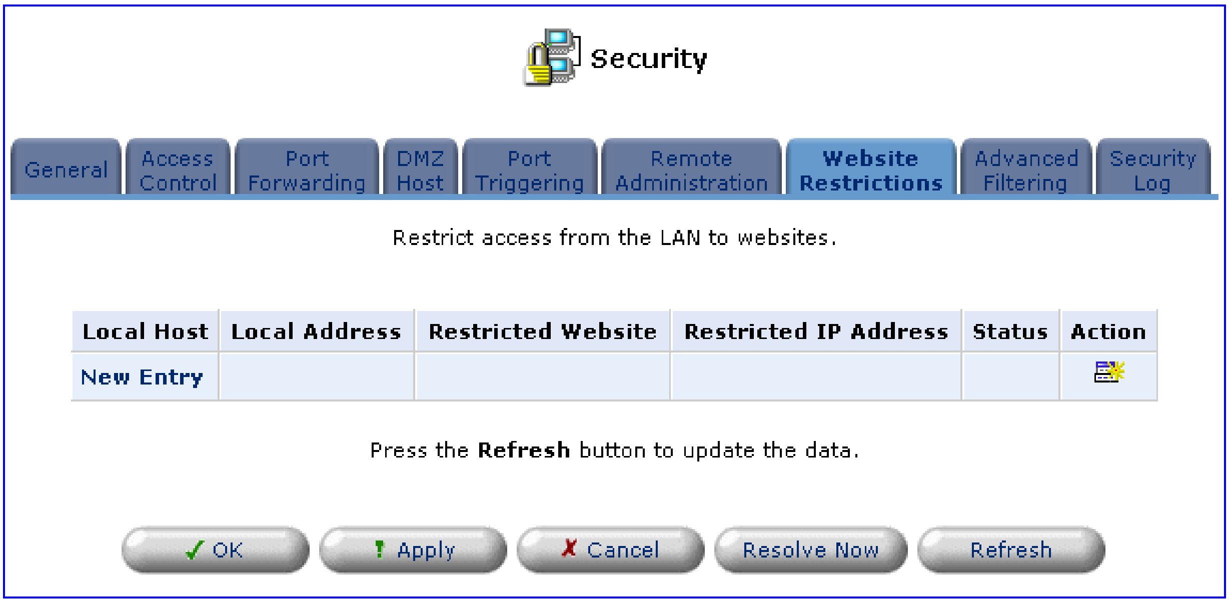
12.6 Website Restrictions

You can configure the gateway to block specific Internet websites so that they cannot be accessed from computers in the home network. Moreover, restrictions can be applied to a comprehensive and automatically-updated table of sites to which access is not recommended.

➢ To block access to a website:

1. Click the tab 'Website Restrictions' in the screen 'Security' (refer to the figure).

Figure 12-19: Website Restrictions



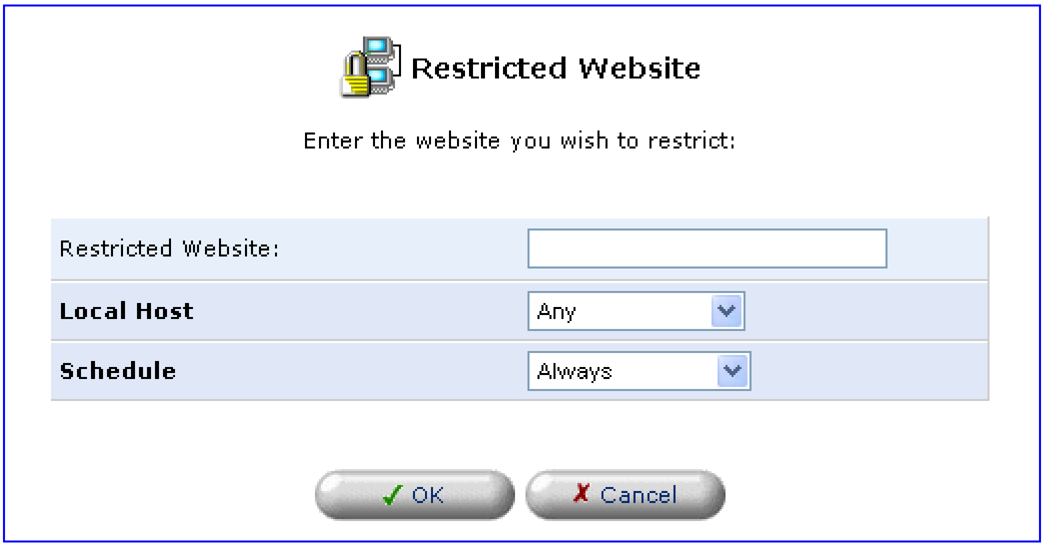
Restrict access from the LAN to websites.

Local Host	Local Address	Restricted Website	Restricted IP Address	Status	Action
New Entry					

Press the **Refresh** button to update the data.

2. Click the link 'New Entry'; the 'Restricted Website' screen opens (refer to the figure).

Figure 12-20: Restricted Website



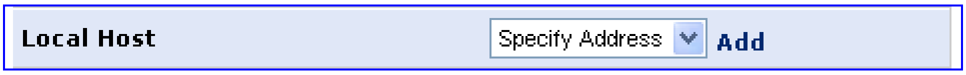
Enter the website you wish to restrict:

Restricted Website:	
Local Host	Any
Schedule	Always

3. Enter the website address (IP address or URL) that you would like to make inaccessible from your home network (all Web pages within the site will also be blocked). If the website address has multiple IP addresses, the gateway will resolve all additional addresses and automatically add them to the restrictions table.

The Local Host combo box provides you the ability to specify the computer or group of computers for which you would like to apply the website restriction. You can select between any or a specific computer address in your LAN. If you choose the option 'Specify Address', the screen will refresh and a link 'Add' appears:

Figure 12-21: Add a Specific Host

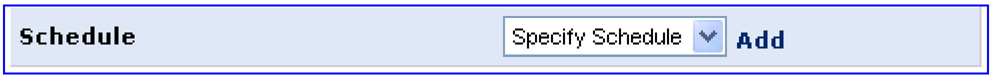


Local Host Specify Address Add

4. Click the link 'Add' to specify a computer address. Specify an address creating a 'Network Object'.

   The parameter Schedule allows you to define the time period during which this rule will take effect. You can select between 'Always' or a specific schedule. If you choose the option 'Specify Schedule', the screen will refresh and an 'Add' link will appear:

Figure 12-22: Add a Specific Schedule



Schedule Specify Schedule Add

5. Click the link 'Add' to specify a protocol. Click 'OK' to save the settings; you're returned to the previous screen while the gateway attempts to find the site. 'Resolving...' will appear in the Status column while the site is being located (the URL is 'resolved' into one or more IP addresses).
6. Click the 'Refresh' button to update the status if necessary. If the site is successfully located, 'Resolved' will appear in the status bar; if not, 'Hostname Resolution Failed' will appear.

➢ If the gateway fails to locate the website:

1. Use a Web browser to verify that the website is available. If it is, then you probably entered the website address incorrectly.
2. If the website is unavailable, return to the screen 'Website Restrictions' later and click the button 'Resolve Now' to verify that the website can be found and blocked by the gateway.
3. You can edit the website restriction by modifying its entry under the column 'Local Host' in the screen 'Website Restrictions'.

➢ To modify an entry:

1. Click the action icon 'Edit' for the restriction; the screen 'Restricted Website' opens (refer to the figure). Modify the website address, group or schedule as required.
2. Click 'OK' to save your changes and return to the screen 'Website Restrictions'.

➢ To ensure that all current IP addresses corresponding to the restricted websites are blocked:

1. Click button 'Resolve Now'; the gateway checks each of the restricted website addresses and ensures that all IP addresses at which this website can be found are included in the IP addresses column.

You can disable a restriction to make a website available again without having to remove it from the screen 'Website Restrictions'. This can be useful when making the website temporarily available and when expecting to block it again in the future.

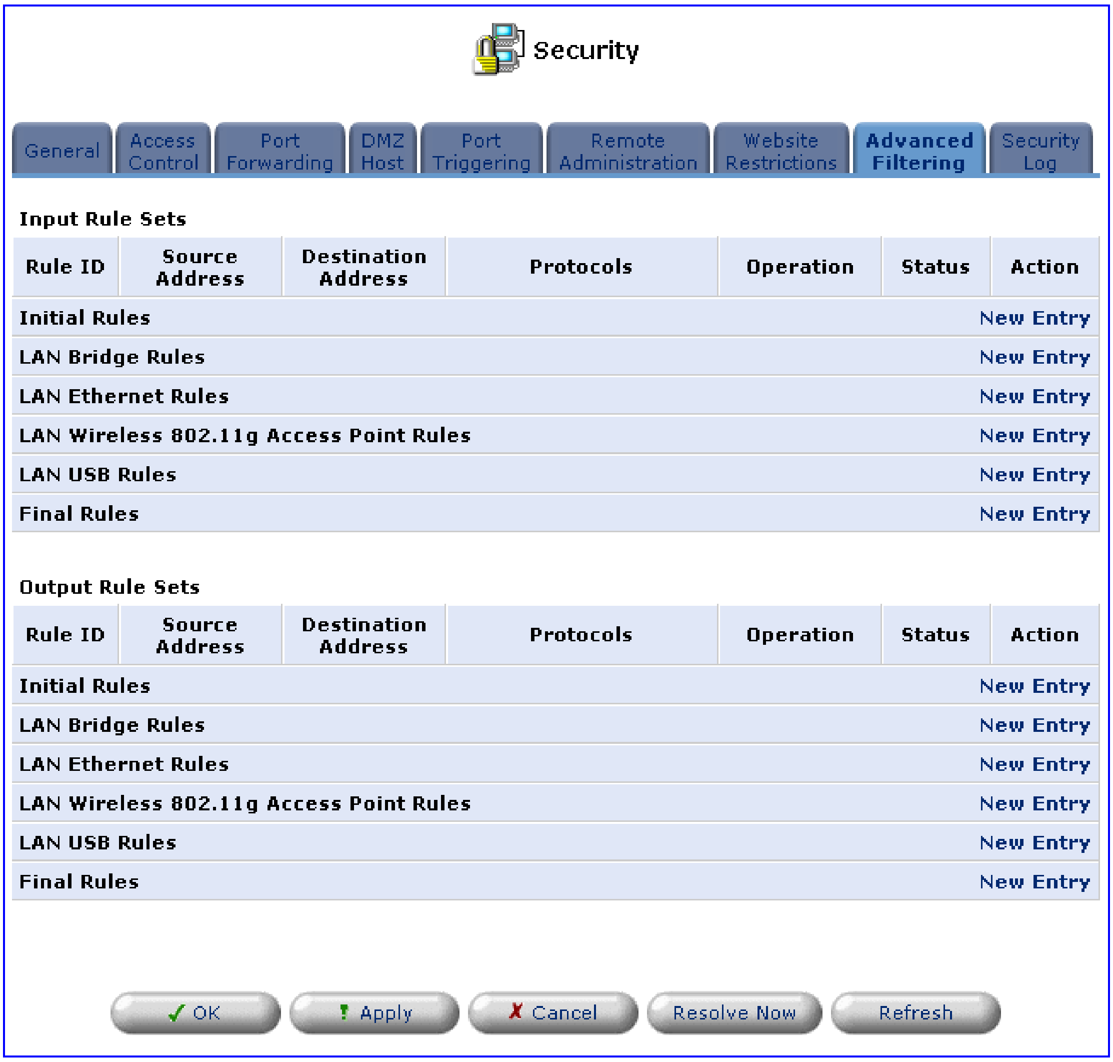
- To temporarily disable a rule, clear the check box adjacent to the service name.
- To reinstate it at a later time, recheck the check box.
- To remove a rule, click the action icon 'Remove' for the service; the service will be permanently removed.

12.7 Advanced Filtering

Advanced filtering is designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN devices.

To view the gateway's advanced filtering options, click the tab 'Advanced Filtering' in the 'Security' screen; the screen 'Advanced Filtering' opens (refer to the figure).

Figure 12-23: Advanced Filtering



Input Rule Sets

Rule ID	Source Address	Destination Address	Protocols	Operation	Status	Action
Initial Rules						New Entry
LAN Bridge Rules						New Entry
LAN Ethernet Rules						New Entry
LAN Wireless 802.11g Access Point Rules						New Entry
LAN USB Rules						New Entry
Final Rules						New Entry

Output Rule Sets

Rule ID	Source Address	Destination Address	Protocols	Operation	Status	Action
Initial Rules						New Entry
LAN Bridge Rules						New Entry
LAN Ethernet Rules						New Entry
LAN Wireless 802.11g Access Point Rules						New Entry
LAN USB Rules						New Entry
Final Rules						New Entry

This screen is divided into two identical sections, one for 'Input Rule Sets' and the other for 'Output Rule Sets', which are for configuring inbound and outbound traffic, respectively. Each section is comprised of subsets, which can be grouped into three main subjects:

1. Initial rules - rules defined here will be applied first, on all gateway devices.
2. Network devices rules - rules can be defined per each gateway device.
3. Final rules - rules defined here will be applied last, on all gateway devices.

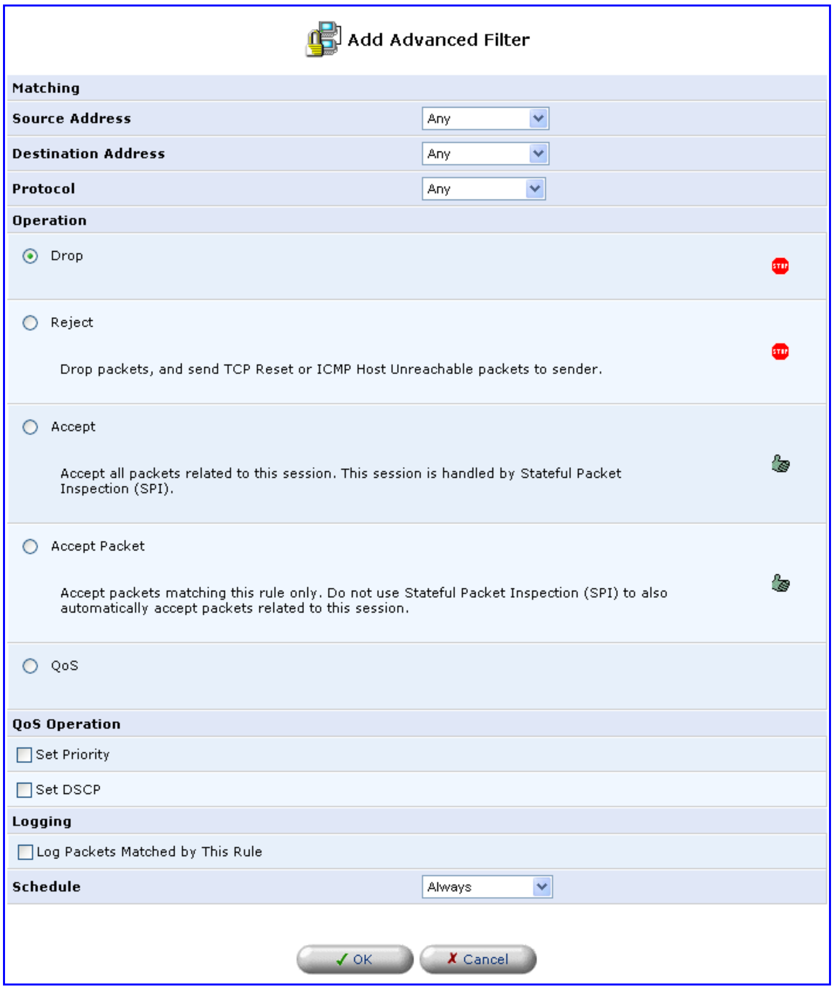
> **Note:** The order of the firewall rules' appearance in the screen 'Advanced Filtering' represents the sequence by which they will be applied.

Numerous rules are automatically inserted by the firewall to provide improved security and block harmful attacks.

➢ To configure an advanced filtering rule:

1. After choosing the traffic direction and the device on which to set the rule, click the appropriate link 'New Entry'; the screen 'Add Advanced Filter' opens (refer to the figure).

Figure 12-24: Add Advanced Filter



Add Advanced Filter

Matching	
Source Address	Any
Destination Address	Any
Protocol	Any
Operation	

● Drop

○ Reject

Drop packets, and send TCP Reset or ICMP Host Unreachable packets to sender.

○ Accept

Accept all packets related to this session. This session is handled by Stateful Packet Inspection (SPI).

○ Accept Packet

Accept packets matching this rule only. Do not use Stateful Packet Inspection (SPI) to also automatically accept packets related to this session.

○ QoS

QoS Operation

□ Set Priority

□ Set DSCP

Logging

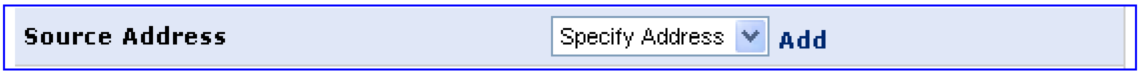
□ Log Packets Matched by This Rule

Schedule	Always

➢ To apply rules:

1. Use the screen section 'Matching' to define a match between IP addresses and a traffic protocol.
2. Configure the source address of the packets sent to or received from the network object (computer A in the above example). To add an address, select the option 'Specify Address' from the drop-down list; the screen refreshes and a link 'Add' appears (refer to the figure).

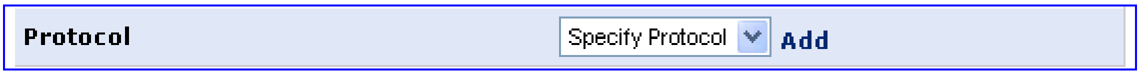
Figure 12-25: Specify Source Address



Source Address Specify Address Add

3. Click the link 'Add'; this commences a sequence that adds a new network object.
4. Configure the destination address of the packets sent to or received from the network object. This address can be configured in the same manner as the source address.
5. Choose a specific traffic protocol from the 'Protocol' drop-down list or add a new one. To add a new traffic protocol, choose the 'Specify Protocol' option in the drop-down list; the screen refreshes and a link 'Add' appears (refer to the figure).

Figure 12-26: Specify Protocol

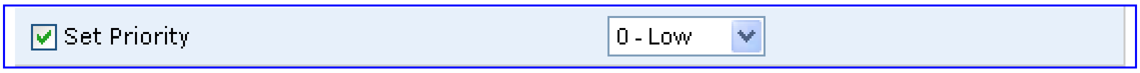


Protocol Specify Protocol Add

6. Click the link 'Add'; this commences a sequence that adds a new protocol.
7. In the screen section 'Operation', define what action the rule will take; check one of the following radio buttons:
   - Drop - Deny access to packets that match the source and destination IP addresses and service ports defined in 'Matching'.
   - Reject - Deny access to packets that match the source and destination IP addresses and service ports defined in 'Matching' and sends and sends an ICMP error or a TCP reset to the origination peer.
   - Accept - Allow access to packets that match the source and destination IP addresses and service ports defined in 'Matching'. The data transfer session will be handled using Stateful Packet Inspection (SPI).
   - Accept Packet - Allow access to packets that match the source and destination IP addresses and service ports defined in 'Matching'. The data transfer session will not be handled using Stateful Packet Inspection (SPI), meaning that other packets that match this rule will not be automatically allowed access. For example, this can useful when creating rules that allow broadcasting.
   - QoS - Select this check-box to define QoS Operation for the rule (the following section).

8. Under the screen section 'QoS Operation', set rule priority with Quality of Service by checking the check box (to add a priority to the rule); the screen refreshes (refer to the figure), allowing you to select between one of eight priority levels, zero being the lowest and seven the highest (each priority level is mapped to low/medium/high priority). This sets the priority of a packet on the connection matching the rule, while routing the packet.

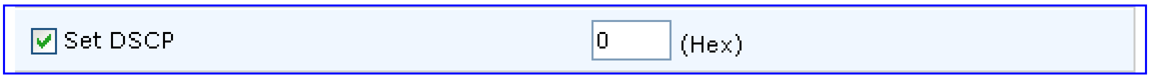
Figure 12-27: Set Priority Rule



☑ Set Priority 0 - Low

9. Check the check box 'Set DSCP' to mark a DSCP value on packets matching this rule; the screen refreshes (refer to the figure), allowing you to enter the hexadecimal value of the DSCP.

Figure 12-28: Set DSCP Rule



☑ Set DSCP 0 (Hex)

10. Under the screen section 'Logging', check the parameter 'Log Packets Matched by This Rule' to log the first packet from a connection that was matched by this rule.

11. By default, the 'Schedule' rule will always be active. However, you can configure scheduler rules in order to define time segments during which the rule may be active.

12. Click 'OK' to save the settings.

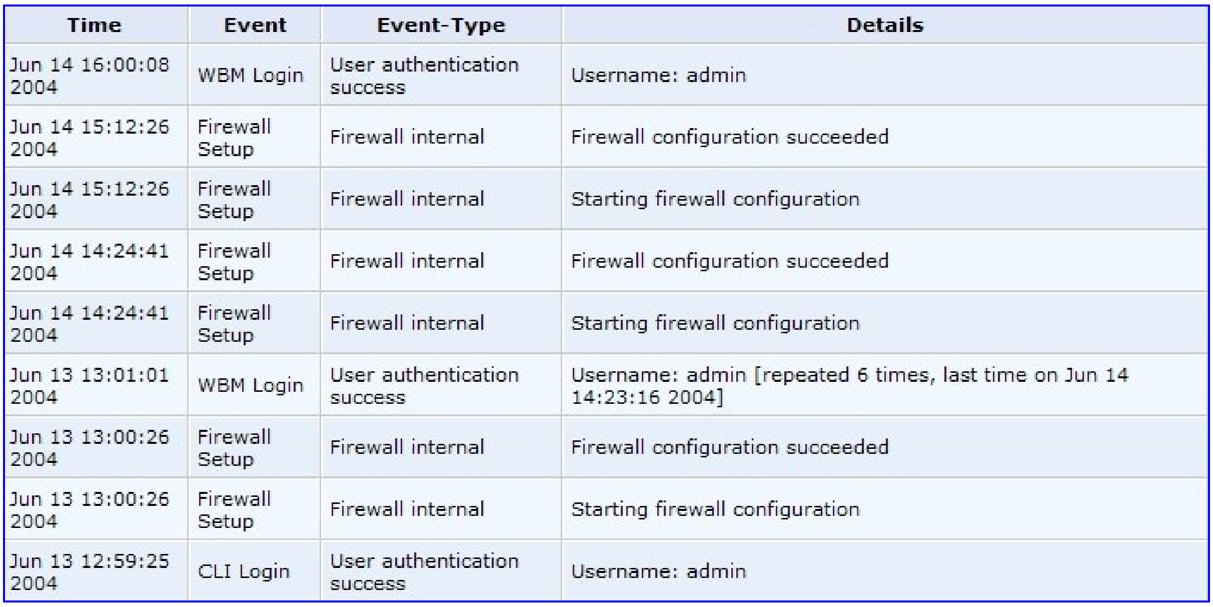
12.8 Security Log

The Security log displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate at an administrative interface (Web-based management or Telnet terminal), firewall configuration and system start-up.

➢ To view the Security Log:

1. Click tab 'Security Log' in the screen 'Security Settings'; the screen 'Security Log' opens.

Figure 12-29: Security Log



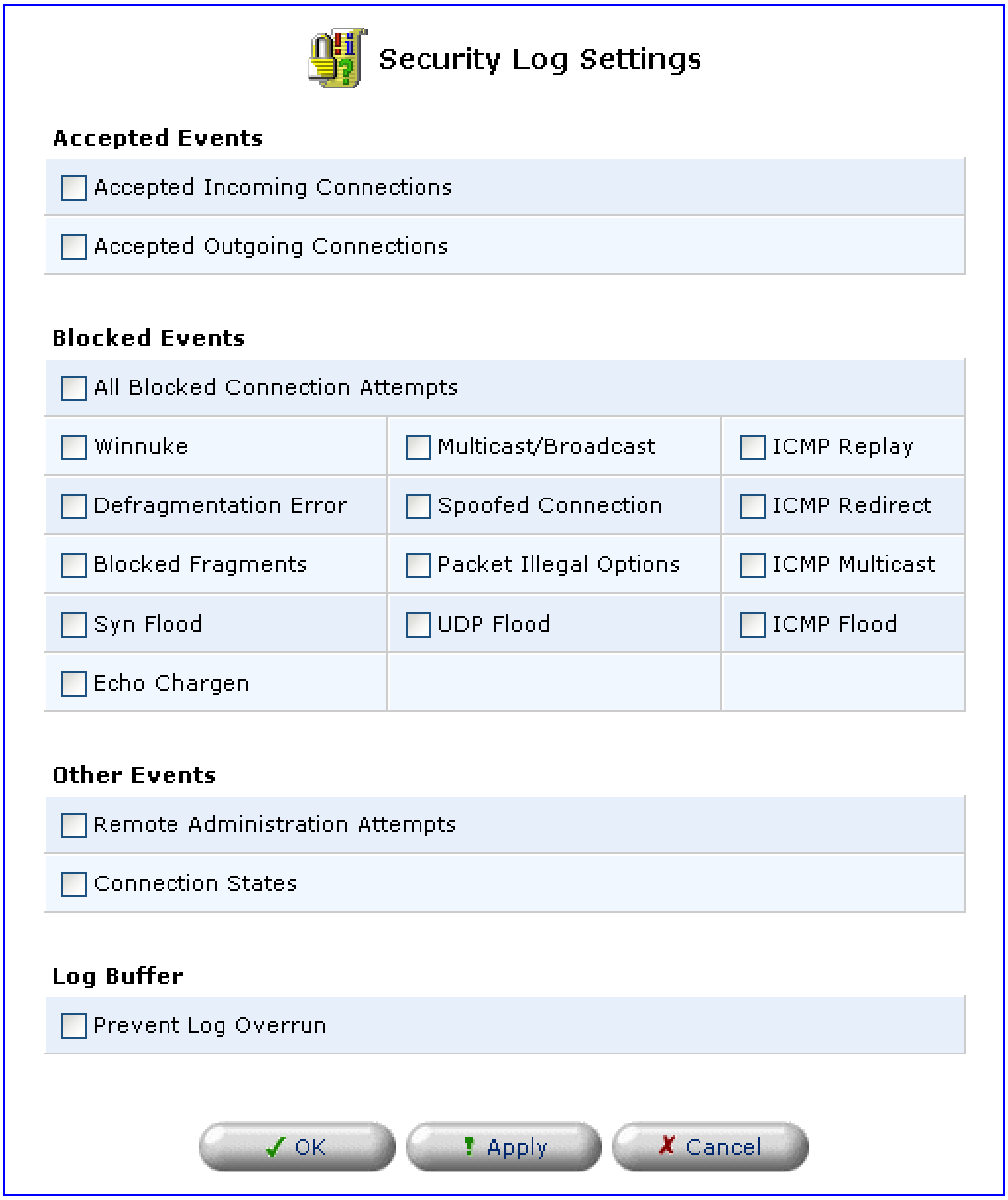
Time	Event	Event-Type	Details
Jun 14 16:00:08 2004	WBM Login	User authentication success	Username: admin
Jun 14 15:12:26 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jun 14 15:12:26 2004	Firewall Setup	Firewall internal	Starting firewall configuration
Jun 14 14:24:41 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jun 14 14:24:41 2004	Firewall Setup	Firewall internal	Starting firewall configuration
Jun 13 13:01:01 2004	WBM Login	User authentication success	Username: admin [repeated 6 times, last time on Jun 14 14:23:16 2004]
Jun 13 13:00:26 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jun 13 13:00:26 2004	Firewall Setup	Firewall internal	Starting firewall configuration
Jun 13 12:59:25 2004	CLI Login	User authentication success	Username: admin

2. View column 'Time' to determine the time the event occurred.
3. View column 'Event' to determine the type of event. There are five types of events:
    - Inbound Traffic: The event is a result of an incoming packet.
    - Outbound Traffic: The event is a result of outgoing packet.
    - Firewall Setup: Configuration message.
    - WBM Login: Indicates that a user has logged in to WBM.
    - CLI Login: Indicates that a user has logged in to CLI (via Telnet).
4. View column 'Event-Type' for a textual description of the event:
    - Blocked: The packet was blocked. The message is color-coded red.
    - Accepted: The packet was accepted. The message is color-coded green.
5. View column 'Details' for details of the packet or the event, such as protocol, IP addresses, ports, etc.

➢ To view or change the security log settings:

1. Click 'Settings' in the 'Firewall Log' screen; the screen 'Security Log Settings' opens (refer to the figure).

Figure 12-30: Security Log Settings



Security Log Settings

Accepted Events

□ Accepted Incoming Connections

□ Accepted Outgoing Connections

Blocked Events

□ All Blocked Connection Attempts

□ Winnuke	□ Multicast/Broadcast	□ ICMP Replay
□ Defragmentation Error	□ Spoofed Connection	□ ICMP Redirect
□ Blocked Fragments	□ Packet Illegal Options	□ ICMP Multicast
□ Syn Flood	□ UDP Flood	□ ICMP Flood
□ Echo Chargen		

Other Events

□ Remote Administration Attempts

□ Connection States

Log Buffer

□ Prevent Log Overrun

2. Select the types of activities for which you would like to have a log message generated.

Accepted Events

- Accepted Incoming Connections - Write a log message for each successful attempt to establish an inbound connection to the home network.
- Accepted Outgoing Connections - Write a log message for each successful attempt to establish an outgoing connection to the public network.

Blocked Events

- All Blocked Connection Attempts - Write a log message for each blocked attempt to establish an inbound connection to the home network or vice versa. You can enable logging of blocked packets of specific types by disabling this option, and enabling some of the more specific options below it.
- Specific Events - Specify the blocked events that should be monitored. Use this to monitor specific event such as SynFlood. A log message will be generated if either the corresponding check-box is checked, or the check-box 'All Blocked Connection Attempts' is checked.

Other Events

- Remote Administration Attempts - Write a log message for each remote-administration connection attempt, whether successful or not.
- Connection States - Provide extra information about every change in a connection opened by the firewall. Use this option to track connection handling by the firewall and Application Level Gateways (ALGs).

Log Buffer

- Prevent Log Overrun - Select this check box in order to stop logging firewall activities when the memory allocated for the log fills up.

3. Click 'OK' to save the settings.

Following are the available event types that can be recorded in the firewall log:

Firewall internal - an accompanying explanation from the firewall internal mechanism will be added in case this event-type is recorded.

Firewall status changed - the firewall changed status from up to down or the other way around, as specified in the event type description.

STP packet - an STP packet has been accepted/rejected.

Illegal packet options - the options field in the packet's header is either illegal or forbidden.

Fragmented packet - a fragment has been rejected.

WinNuke protection - a WinNuke attack has been blocked.

ICMP replay - an ICMP replay message has been blocked.

ICMP redirect protection - an ICMP redirected message has been blocked.

Packet invalid in connection - a packet has been blocked, being on an invalid connection.

ICMP protection - a broadcast ICMP message has been blocked.

Broadcast/Multicast protection - a packet with a broadcast/multicast source IP has been blocked.

Spoofing protection - a packet from the WAN with a source IP of the LAN has been blocked.

DMZ network packet - a packet from a demilitarized zone network has been blocked.

Trusted device - a packet from a trusted device has been accepted.

Default policy - a packet has been accepted/blocked according to the default policy.

Remote administration - a packet designated for OpenRG management has been accepted/blocked.

Access control - a packet has been accepted/blocked according to an access control rule.

Parental control - a packet has been blocked according to a parental control rule.

NAT out failed - NAT failed for this packet.

DHCP request - OpenRG sent a DHCP request (depends on the distribution).

DHCP response - OpenRG received a DHCP response (depends on the distribution).

DHCP relay agent - a DHCP relay packet has been received (depends on the distribution).

IGMP packet - an IGMP packet has been accepted.

Multicast IGMP connection - a multicast packet has been accepted.

RIP packet - a RIP packet has been accepted.

PPTP connection - a packet inquiring whether OpenRG is ready to receive a PPTP connection has been accepted.

Kerberos key management 1293 - security related, for future use.

Kerberos 88 - for future use.

AUTH:113 request - an outbound packet for AUTH protocol has been accepted (for maximum security level).

Packet-Cable - for future use.

IPV6 over IPV4 - an IPv6 over IPv4 packet has been accepted.

ARP - an ARP packet has been accepted.

PPP Discover - a PPP discover packet has been accepted.

PPP Session - a PPP session packet has been accepted.

802.1Q - a 802.1Q (VLAN) packet has been accepted.

Outbound Auth1X - an outbound Auth1X packet has been accepted.

IP Version 6 - an IPv6 packet has been accepted.

OpenRG initiated traffic - all traffic that OpenRG initiates is recorded.

Maximum security enabled service - a packet has been accepted because it belongs to a permitted service in the maximum security level.

SynCookies Protection - a SynCookies packet has been blocked.

ICMP Flood Protection - a packet has been blocked, stopping an ICMP flood.

UDP Flood Protection - a packet has been blocked, stopping a UDP flood.

Service - a packet has been accepted because of a certain service, as specified in the event type.

Advanced Filter Rule - a packet has been accepted/blocked because of an advanced filter rule.

Fragmented packet, header too small - a packet has been blocked because after the defragmentation, the header was too small.

Fragmented packet, header too big - a packet has been blocked because after the defragmentation, the header was too big.

Fragmented packet, drop all - not used.

Fragmented packet, bad align - a packet has been blocked because after the defragmentation, the packet was badly aligned.

Fragmented packet, packet too big - a packet has been blocked because after the defragmentation, the packet was too big.

Fragmented packet, packet exceeds - a packet has been blocked because defragmentation found more fragments than allowed.

Fragmented packet, no memory - a fragmented packet has been blocked because there was no memory for fragments.

Fragmented packet, overlapped - a packet has been blocked because after the defragmentation, there were overlapping fragments.

Defragmentation failed - the fragment has been stored in memory and blocked until all fragments arrived and defragmentation could be performed.

Connection opened - usually a debug message regarding a connection.

Wildcard connection opened - usually a debug message regarding a connection.

Wildcard connection hooked - usually debug message regarding connection.

Connection closed - usually a debug message regarding a connection.

Echo/Chargen/Quote/Snork protection - a packet has been blocked, protecting from Echo/Chargen/Quote/Snork.

First packet in connection is not a SYN packet - a packet has been blocked because of a TCP connection that had started without a SYN packet.

Error: No memory - a message notifying that a new connection has not been established because of lack of memory.

NAT Error : Connection pool is full - a message notifying that a connection has not been created because the connection pool is full.

NAT Error: No free NAT IP - a message notifying that there is no free NAT IP, therefore NAT has failed.

NAT Error: Conflict Mapping already exists - a message notifying that there is a conflict since the NAT mapping already exists, therefore NAT has failed.

Malformed packet: Failed parsing - a packet has been blocked because it is malformed.

Passive attack on ftp-server: Client attempted to open Server ports - a packet has been blocked because of an unauthorized attempt to open a server port.

FTP port request to 3rd party is forbidden (Possible bounce attack) - a packet has been blocked because of an unauthorized FTP port request.

Firewall Rules were changed - the firewall rule set has been modified.

User authentication - a message during login time, including both successful and failed authentication.

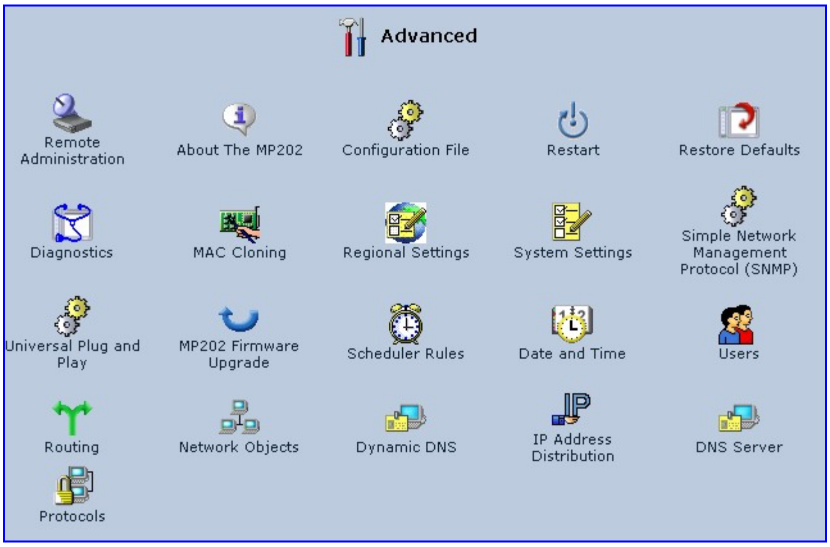
First packet is Invalid - First packet in connection failed to pass firewall or NAT

Reader's Notes

13 Advanced Settings

This section of the Web-based Management is intended primarily for more advanced users. Some changes to settings within this section could adversely affect the operation of the MP-202 and the home network, and should be made with caution.

Figure 13-1: Advanced Settings



From the Advanced screen you can (refer to the table below):

Table 13-1: Action Icons in the Advanced Screen

Icon	What you can do
Remote Administration	Configure remote administration privileges
About the MP-202	View technical information about the gateway, including version number
Configuration File	Load the Configuration File to the MP-202
Restart	Restart the MP-202
Restore Defaults	Restore default factory settings

Icon	What you can do
Diagnostics	Perform networking diagnostics
MAC Cloning	Clone MP-202's MAC address.
Regional Settings	Change the regional settings
System Settings	Modify administrator settings, including the MP-202's hostname
SNMP	Configure the MP-202's SNMP agent
Universal Plug and Play	Configure Universal Plug and Play (UPnP) parameters
MP-202 Firmware Upgrade	Perform a Firmware Upgrade
Scheduler Rules	Define time segments for system rules
Date and Time	Set the local date and time
Users	Configure users
Routing	Manage routing policies
Network Objects	Define groups of LAN devices for system rules
Dynamic DNS	View and modify the DNS Hosts table

Icon	What you can do
IP Address Distribution	Modify the behavior of the DHCP server for each LAN device and view a list of DHCP clients in the local network
DNS Server	Alias a dynamic IP address to a static hostname
Protocols	Manage protocols

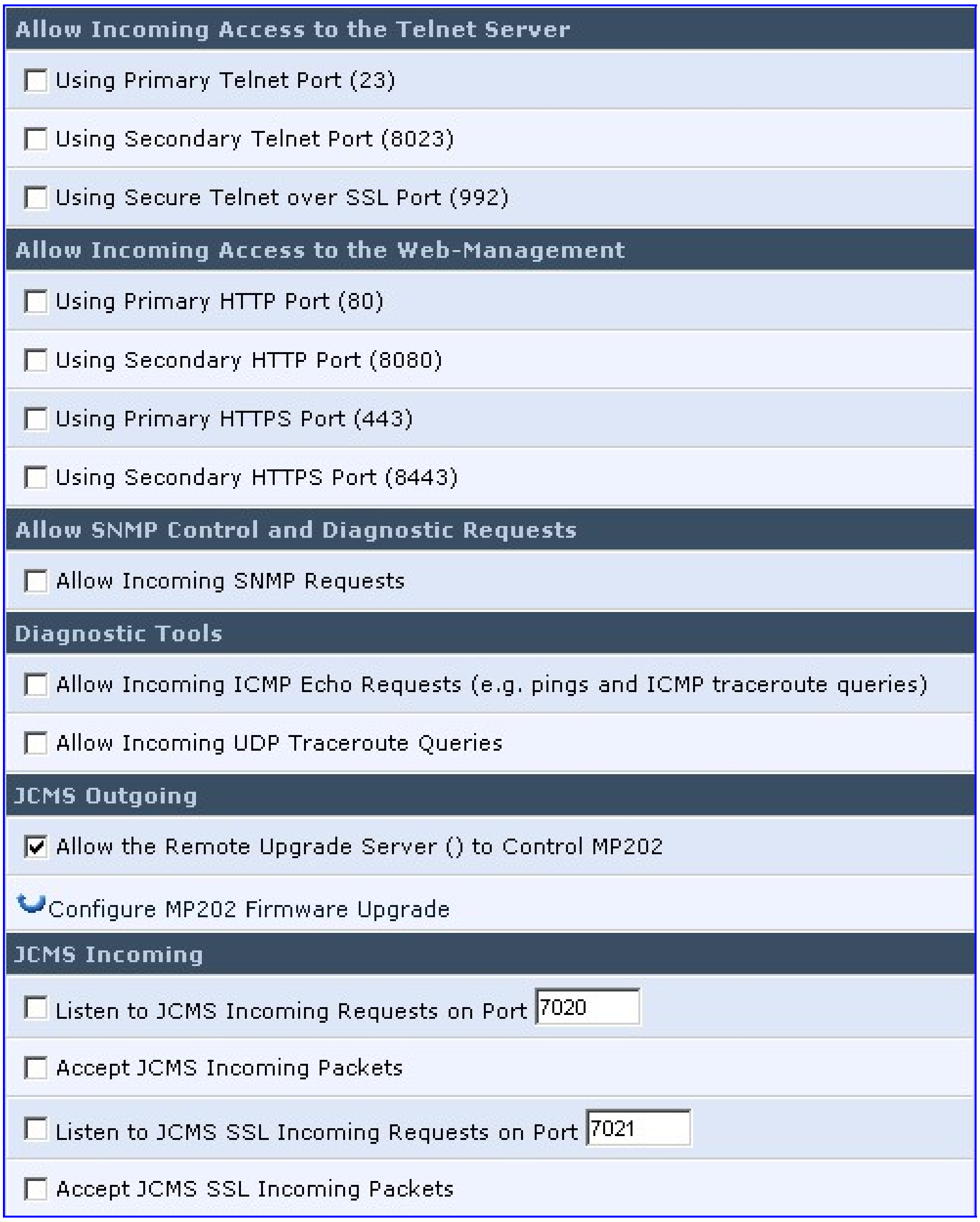
13.1 Remote Administration

It is possible to access and control the MP-202 not only from within the home network, but also from the Internet. This allows you to view or change settings while travelling. It also enables you to allow your ISP to change settings or help you trouble-shoot functionality or communication issues from a remote location.

Remote access to the MP-202 is blocked by default to ensure the security of your home network. However, remote access is supported by the following services, and you may use the 'Remote Access Configuration' screen to selectively enable these services if they are needed.

➢ To view the device's remote administration options:

- Click the icon 'Remote Administration' in the 'Advanced' screen of the Web-based management; the 'Remote Administration' screen appears.



Allow Incoming Access to the Telnet Server

☐ Using Primary Telnet Port (23)

☐ Using Secondary Telnet Port (8023)

☐ Using Secure Telnet over SSL Port (992)

Allow Incoming Access to the Web-Management

☐ Using Primary HTTP Port (80)

☐ Using Secondary HTTP Port (8080)

☐ Using Primary HTTPS Port (443)

☐ Using Secondary HTTPS Port (8443)

Allow SNMP Control and Diagnostic Requests

☐ Allow Incoming SNMP Requests

Diagnostic Tools

☐ Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)

☐ Allow Incoming UDP Traceroute Queries

JCMS Outgoing

☑ Allow the Remote Upgrade Server () to Control MP202

Configure MP202 Firmware Upgrade

JCMS Incoming

☐ Listen to JCMS Incoming Requests on Port 7020

☐ Accept JCMS Incoming Packets

☐ Listen to JCMS SSL Incoming Requests on Port 7021

☐ Accept JCMS SSL Incoming Packets

Note: Telnet and Web-Management can be used to modify the settings of the firewall or to disable it. Users can also change local IP addresses and other settings, making it difficult or impossible to access the Telephone Adapter from the home network. Therefore, remote access to Telnet or HTTP services should be blocked and should only be permitted when absolutely necessary.

➢ To allow remote access to MP-202 services:

1. Click the 'Remote Administration' button. The 'Remote Access Configuration' screen will appear (refer to the figure above).
2. Select the services that you would like to make available to computers on the Internet.
3. Click 'OK' to save your changes and return to the 'Security Settings' screen.

   Encrypted remote administration is done using a secure SSL connection, that requires an SSL certificate. When accessing the MP-202 for the first time using encrypted remote administration, you will be prompted by your browser with a warning regrading certificate authentication. This is due to the fact that the MP-202's SSL certificate is self generated. When encountering this message under these circumstances, ignore it and continue. It should be noted that even though this message appears, the self generated certificate is safe, and provides you with a secure SSL connection.

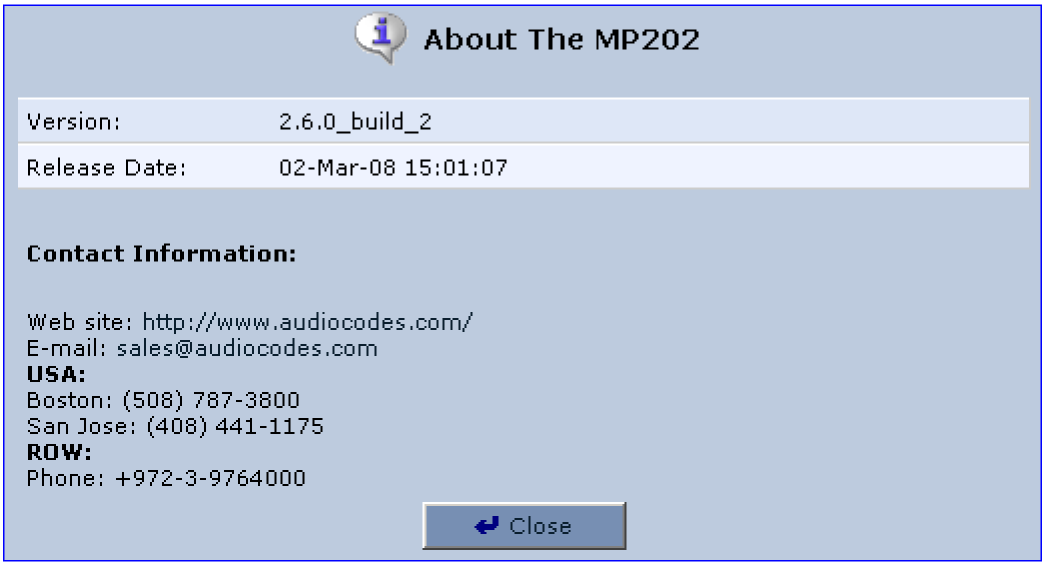
   It is also possible to assign a user-defined certificate to the MP-202.

13.2 About the MP-202

➢ To view technical information regarding the MP-202:

1. Click the icon 'About the MP-202' in the 'Advanced' screen of the Web-based Management; the screen 'About the MP-202' appears showing the version, the release date and the supported features (refer to the figure).

Figure 13-2: Advanced - About the Gateway



About The MP202

Version:	2.6.0_build_2
Release Date:	02-Mar-08 15:01:07

Contact Information:

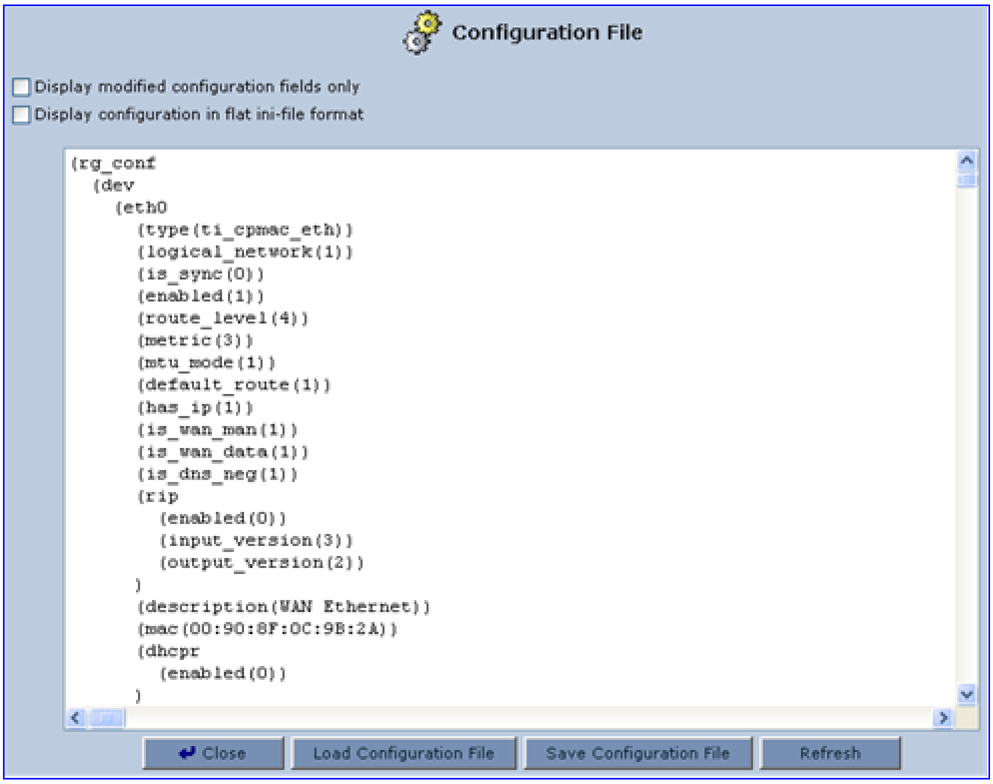
Web site: http://www.audiocodes.com/
E-mail: sales@audiocodes.com
USA:
Boston: (508) 787-3800
San Jose: (408) 441-1175
ROW:
Phone: +972-3-9764000

13.3 Configuration File

Your gateway enables you to view, save and load its configuration file in order to backup and restore your current configuration.

1. Click the icon 'Configuration File' in the 'Advanced' screen of the Web-based management; the 'Configuration File' screen is displayed (refer to the figure) showing the entire contents of the configuration file.

Figure 13-3: Contents of the Configuration File



□ Display modified configuration fields only

□ Display configuration in flat ini-file format

```
(rg_conf
  (dev
    (eth0
      (type(ti_cpmac_eth))
      (logical_network(1))
      (is_sync(0))
      (enabled(1))
      (route_level(4))
      (metric(3))
      (mtu_mode(1))
      (default_route(1))
      (has_ip(1))
      (is_wan_man(1))
      (is_wan_data(1))
      (is_dns_neg(1))
      (rip
        (enabled(0))
        (input_version(3))
        (output_version(2))
      )
      (description(WAN Ethernet))
      (mac(00:90:8F:0C:9B:2A))
      (dhcpr
        (enabled(0))
      )
```

2. You can customize the displayed configuration file, by selecting the following check boxes:

   - 'Display modified configuration fields only': only the configuration parameters that have values other than default values are displayed.
   - 'Display configuration in flat ini-file format': the configuration file is displayed in flat INI-file format.

3. Click the button 'Load Configuration File' to restore your configuration from a file and restart the gateway.

4. Click 'Save Configuration File' to back up your current configuration to a file. Note that the file is generated according to the selected display option (in Step 2).

The saved configuration file can be used as a backup for the specific gateway's configuration, for creating a configuration file for remote configuration update, and also for debugging and diagnostics.

When creating a configuration backup, disable the two display check boxes (i.e. save a full configuration file in the hierarchic conf format). This file can be loaded back to the same gateway, using the procedure described in "Loading From a Computer in the Network" on page 167.

Note: Do not load this file to a different gateway, since it contains the MAC address, which is specific to the gateway from where it was saved.

When creating a file for remote configuration update, it is recommended to enable the 'Display modified configuration fields only'. This ensures that the file includes only parameters that were modified from their default value. You can choose either the conf format or the flat ini-file format. In both cases, it is recommended to review the file and ensure that only the parameters that the user has intended to modify appear. This file can be placed on an FTP or HTTP server for mass configuration update, as described in Remote Configuration Download.

Note: When rebooting, the gateway restores the settings from its configuration file. However, if reboot attempts fail three times consecutively, the gateway resets the configuration file by restoring factory defaults before attempting to reboot.

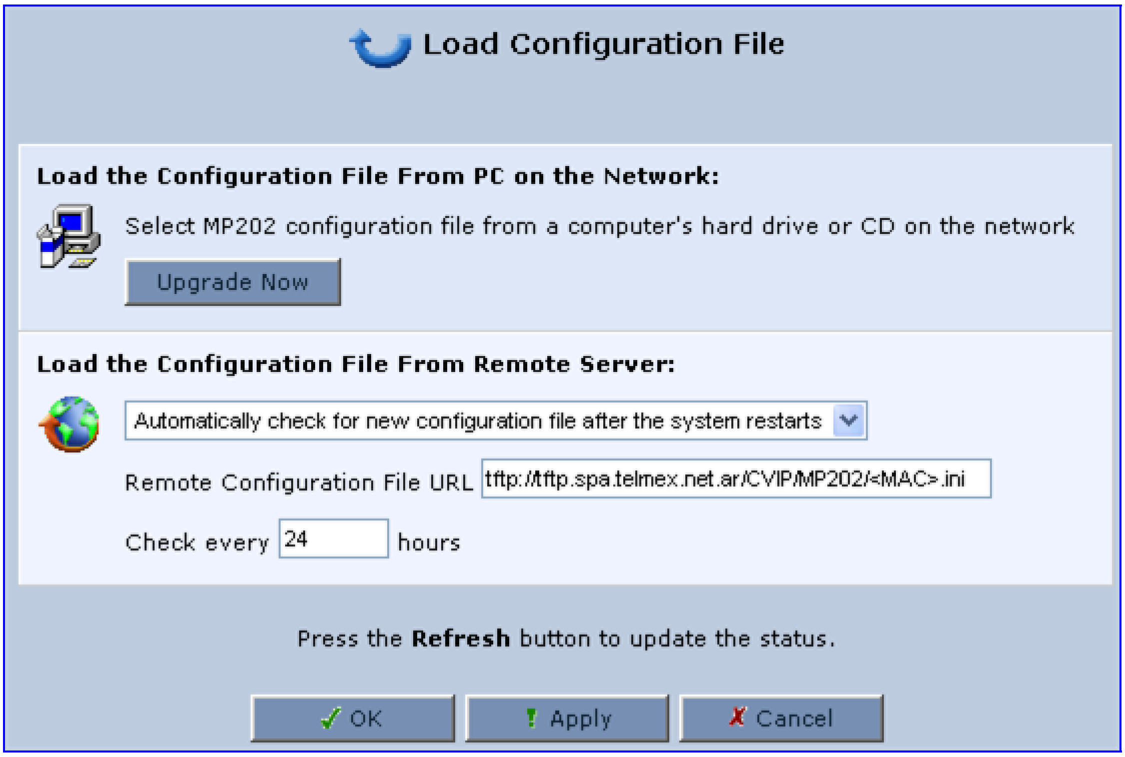
13.3.1 Loading From a Computer in the Network

To load the MP-202's configuration file from a computer in the network:

1. Click the icon 'Configuration File' from the 'Advanced' screen; the 'Configuration File' screen is displayed.

2. Click the button 'Load Configuration File'; the screen 'Load Configuration File' opens (refer to the figure).

Figure 13-4: Load Configuration File



Load Configuration File

Load the Configuration File From PC on the Network:

Select MP202 configuration file from a computer's hard drive or CD on the network

Load the Configuration File From Remote Server:

Automatically check for new configuration file after the system restarts

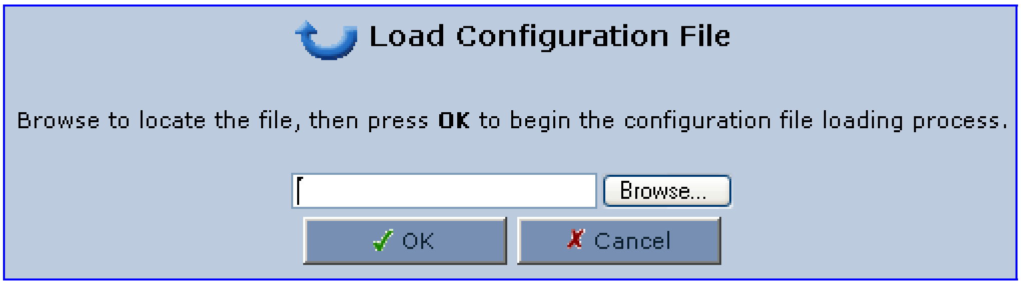
Remote Configuration File URL tftp://tftp.spa.telmex.net.ar/CVIP/MP202/<MAC>.ini

Check every 24 hours

Press the **Refresh** button to update the status.

3. In the screen section 'Load the Configuration File From a PC on the Network', click the button 'Upgrade Now'; the screen 'Load Configuration File' opens (refer to the figure).

Figure 13-5: Advanced - Loading Configuration File from a PC on the Network

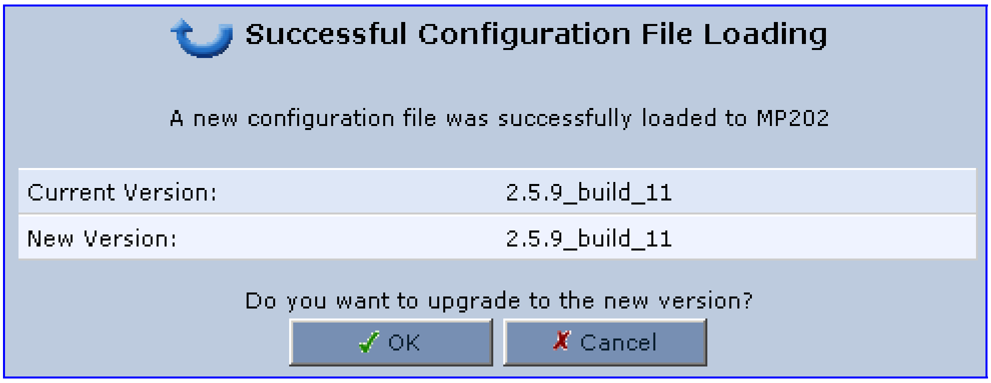


Load Configuration File

Browse to locate the file, then press **OK** to begin the configuration file loading process.

4. Enter the path of the configuration file or click 'Browse' and navigate to the configuration file on your PC. Click 'OK'; the file starts loading from your PC to your gateway. When loading is complete, the screen 'Successful Configuration File Loading' opens (refer to the figure), prompting you to confirm configuration file load.

Figure 13-6: Successful Configuration File Loading



Successful Configuration File Loading

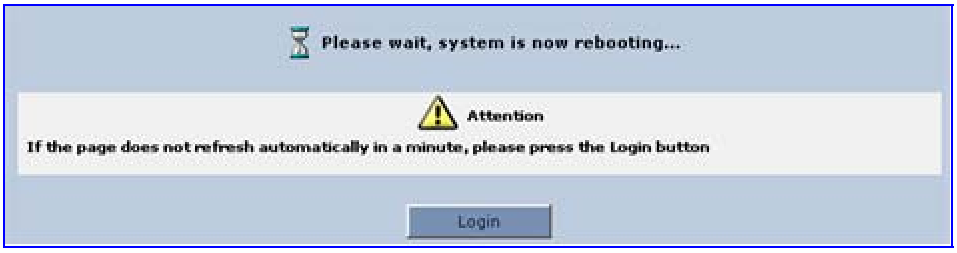
A new configuration file was successfully loaded to MP202

Current Version:	2.5.9_build_11
New Version:	2.5.9_build_11

Do you want to upgrade to the new version?

5. Click 'OK' to confirm; the upgrade process commences and shouldn't take longer than a couple of minutes to complete. At the conclusion of the file load process, the device automatically reboots. The new configuration file is now applied to the gateway.

Figure 13-7: Reboot After Configuration File Load



Please wait, system is now rebooting...

Attention

If the page does not refresh automatically in a minute, please press the Login button

Note: Do not power down the MP-202 or stop the file load process in the middle or else the MP-202 will become inoperable.

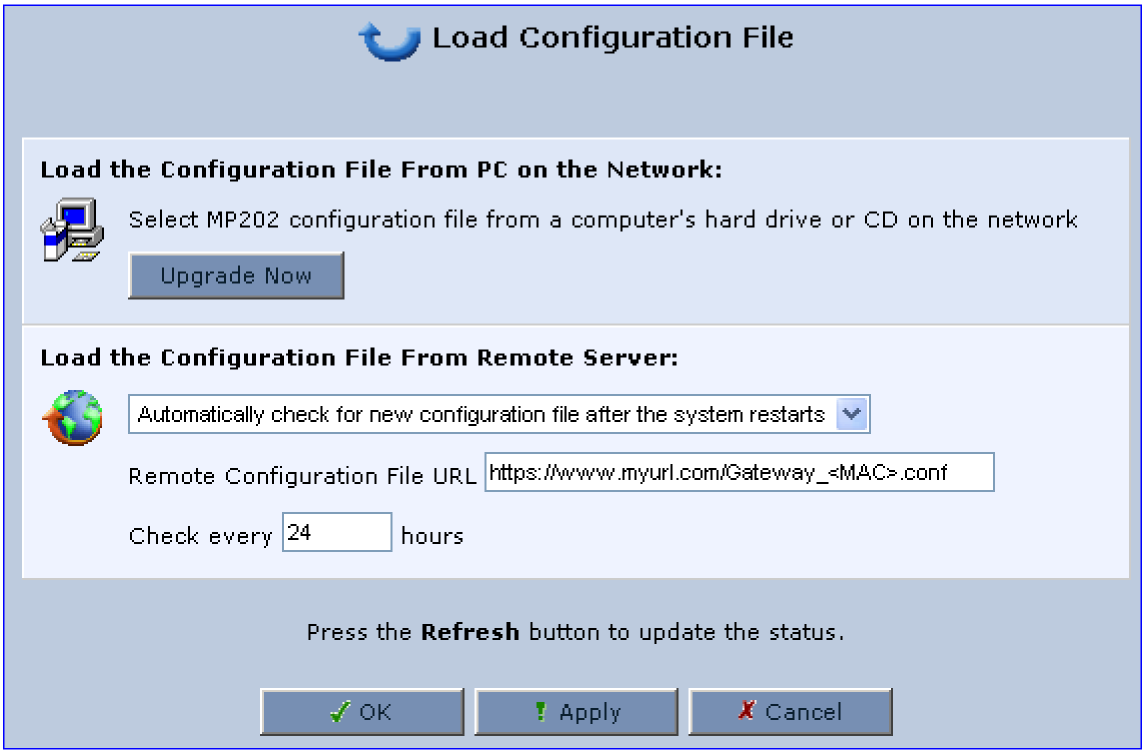
13.3.2 Loading From a Remote Server

The Remote Load mechanism helps you keep your configuration parameters up-to-date, by performing daily checks for a newer configuration file after each time the gateway restarts, as well as letting you perform manual checks.

To load the MP-202's configuration file from a remote server:

1. Click the icon 'Configuration File' from the 'Advanced' screen; the 'Configuration File' screen is displayed.
2. Click the button 'Load Configuration File'; the screen 'Load Configuration File' opens (refer to the figure below).

Figure 13-8: Load Configuration File



Load Configuration File

Load the Configuration File From PC on the Network:

Select MP202 configuration file from a computer's hard drive or CD on the network

Load the Configuration File From Remote Server:

Automatically check for new configuration file after the system restarts

Remote Configuration File URL https://www.myurl.com/Gateway_<MAC>.conf

Check every 24 hours

Press the **Refresh** button to update the status.

3. In the 'Load the Configuration File From Remote Server' section, you can select the utility's checking method and interval:
   - Automatically check for new configuration file after the system restarts:
   - Automatic configuration file check disabled:
4. In the 'Remote Configuration File URL' field, enter the URL address of the remote server where the configuration file is located.
5. In the 'Check every' field, enter the time interval (in hours) for which the gateway periodically checks for a new configuration file. if 0 is defined, the gateway checks only once for a new configuration file, and this occurs after the system restarts.
6. Click the 'OK' button. A download process will begin. When downloading is completed, a confirmation screen will appear, asking you if you want to load the new version.

7. Click 'OK' to confirm. The upgrade process will begin and should take no longer than one minute to complete.

   At the conclusion of the upgrade process, the MP-202 automatically reboots and the new software version runs.

   If a new version is not available, click the 'Check Now' button to perform an immediate check (instead of waiting for the next scheduled one). The screen displays a green "Check in progress..." message.

Notes:

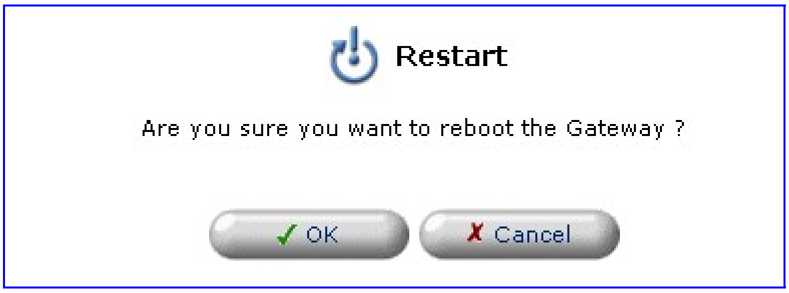
- The configuration file can have one of the following two formats – a hierarchical conf file (indicated by file extension .conf) or a flat ini file (indicated by file extension .ini).
- The parameter '/rmt_config/version' defines the version of the configuration file. The gateway uses the new configuration file only if the version that is defined in this file is later than the current version. By default, the 'version' is set to 0. This means that each time Service Providers' operations personnel require the gateway to download a new configuration file, they need to increment the 'version' parameter in the new file (in the .conf file, the 'version' parameter is under the section 'rmt_config'). To simplify the procedure, it is possible to use the current date in YYYYMMDD format as the version field.
- The remote configuration file must include only a subset of the complete MP202.conf file. A recommended procedure is to start with a gateway restored to its factory settings, modify using the embedded Web server the parameters that should appear in the remote configuration file, and then upload (save) the configuration file. You must save only the modified parameters, as described in "Remote Administration" on page 163.
- The string <MAC> enables the ISP to pre-configure all its deployed gateways with the same URL and file details (under rmt_config/url) and still have each gateway download its unique configuration file. Once the URL is configured with the string <MAC>, the gateway that is trying to update its configuration file automatically replaces <MAC> with its own unique MAC address. For example, if there's a gateway with a WAN MAC address 00:01:02:03:04:05, the ISP can configure the url to http://myserver.com/my_conf_file_<MAC>.conf - and place a file called 'my_conf_file_00_01_02_03_04_05.conf' on the server.
- Downloading a configuration file from a remote server can also be performed from the CLI:
  1) Using Telnet, access the gateway, and then enter the user name and password.
  2) Enter the command **rmt_config**, for example:
  rmt_config –u http://myserver.com/my_conf_file.conf
  3) Enter **rmt_config** without any arguments for more help information.

13.4 Restart

➢ To restart your gateway:

1. Click the icon 'Restart' in the 'Advanced' screen of the Web-based Management; the 'Restart' screen is displayed (refer to the figure below).

Figure 13-9: Advanced - Restart



Restart

Are you sure you want to reboot the Gateway ?

2. Press 'OK' to restart the gateway. This may take up to one minute.

3. To re-enter the Web-based Management after restarting the gateway, click the browser's 'Refresh' button.

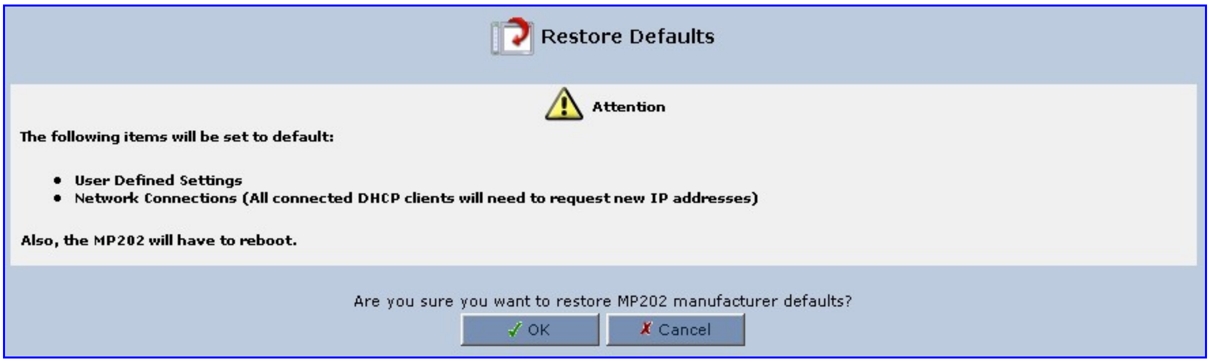
13.5 Restoring Default Settings

You can restore the MP-202's factory default settings when, for example, you're building a new network from the beginning or when you cannot recall changes made to the network and you need to go back to the default configuration).

➢ To restore default settings:

1. Click the 'Restore Defaults' icon in the 'Advanced' screen of the Web-based Management; the 'Restore Defaults' screen is displayed (refer to the figure).

Figure 13-10: Restore Defaults



Restore Defaults

Attention

The following items will be set to default:

- User Defined Settings
- Network Connections (All connected DHCP clients will need to request new IP addresses)

Also, the MP202 will have to reboot.

Are you sure you want to restore MP202 manufacturer defaults?

2. Click 'OK' to restore the MP-202's factory default settings.

Note: If you are accessing the MP-202's Web from the WAN, restoring the factory settings will cause the connection to be lost, since access to the Web from the WAN is blocked by default.

In cases where the Web server cannot be accessed (for example if you've forgotten the password or if the LAN is disabled), it's possible to restore the default settings using a manual procedure.

➢ To restore default settings manually:

1. Disconnect the MP-202 DC power cable.
2. Using a paper clip, press the pushbutton located on the bottom of the MP-202 (a pinhole at one of the corners)
3. While pressing the pushbutton, power up the device. Keep the pushbutton pressed for another 5 seconds.

Note: All Web-based management settings and parameters, not only those in the Advanced section, will be restored to their default values. This includes the administrator password; a user-specified password will no longer be valid.

13.6 Diagnostics

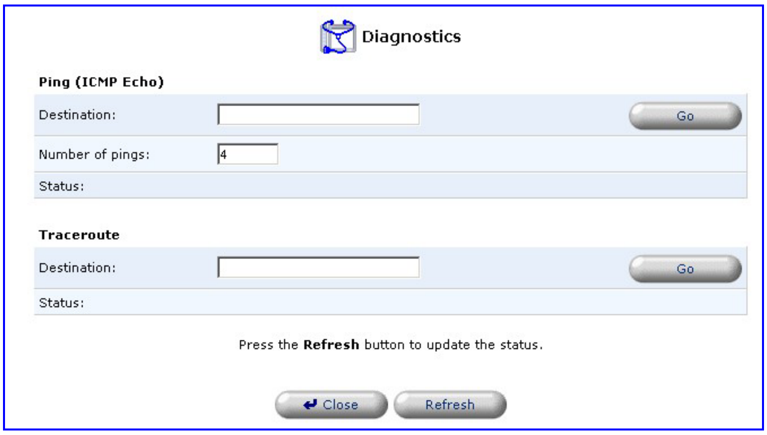
The Diagnostics screen can assist you to test network connectivity and view statistics, such as the number of packets transmitted and received, round-trip time and success status. The test tools are platform-dependent and are not available simultaneously.

13.6.1 Diagnosing Network Connectivity

➢ To diagnose network connectivity:

1. Click the 'Diagnostics' icon from the 'Advanced' screen in the Web-based Management; the 'Diagnostics' screen is displayed.

Figure 13-11: Advanced - Diagnostics



Diagnostics

Ping (ICMP Echo)

Destination:

Number of pings: 4

Status:

Traceroute

Destination:

Status:

Press the **Refresh** button to update the status.

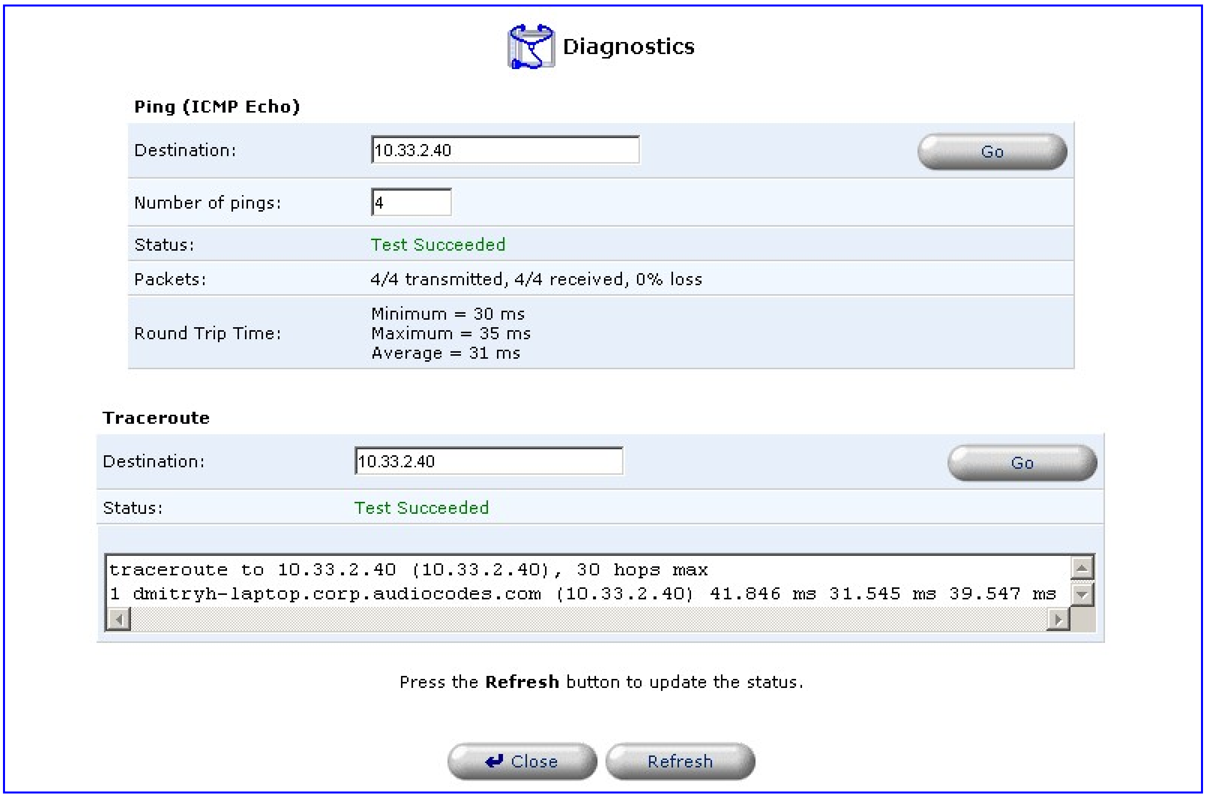
2. Under the screen section 'Ping (ICMP Echo)', enter the IP address or URL to be tested in the 'Destination' field.

3. Enter the number of pings you would like to perform.

4. Press the 'Go' button.

5. In a few seconds, diagnostic statistics are displayed (refer to the figure below). If no new information is displayed, press the 'Refresh' button.

Figure 13-12: Advanced - Diagnostics - Statistics



Diagnostics

Ping (ICMP Echo)

Destination:	10.33.2.40
Number of pings:	4
Status:	Test Succeeded
Packets:	4/4 transmitted, 4/4 received, 0% loss

Round Trip Time:	Minimum = 30 ms
	Maximum = 35 ms
	Average = 31 ms

Traceroute

Destination:	10.33.2.40
Status:	Test Succeeded

```
traceroute to 10.33.2.40 (10.33.2.40), 30 hops max
1 dmitryh-laptop.corp.audiocodes.com (10.33.2.40) 41.846 ms 31.545 ms 39.547 ms
```

Press the **Refresh** button to update the status.

13.6.2 Performing a Traceroute

➢ To perform a traceroute:

1. Click the 'Diagnostics' icon from the 'Advanced' screen in the Web-based Management; the 'Diagnostics' screen is displayed.

2. Under the screen section 'Traceroute', enter the IP address or URL to be tested in the 'Destination' field.

3. Press the button 'Go'; a traceroute commences, constantly refreshing the screen (refer to the figure above).

4. To stop the trace and view the results, press 'Cancel'.

13.7 MAC Cloning

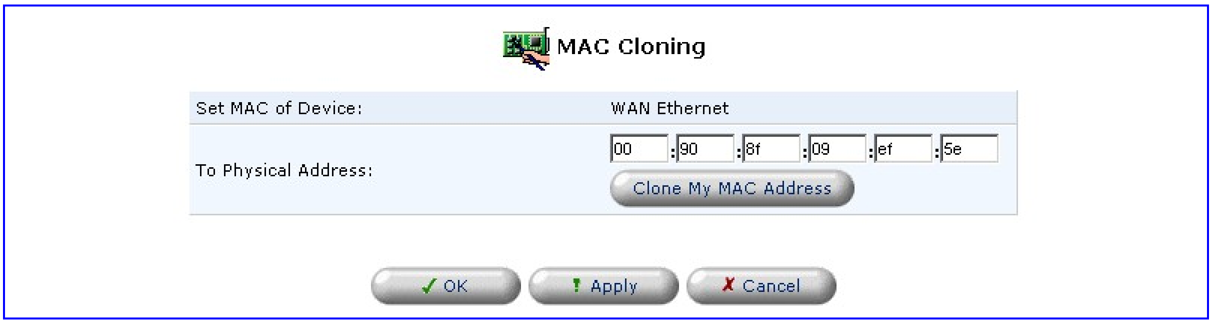
A Media Access Control (MAC) address is the numeric code that identifies a device on a network, such as your external cable/DSL modem or a PC network card. Your Service Provider may ask you to supply the MAC address of your PC, external modem, or both. When replacing an external modem with your gateway, you can simplify the installation process by copying the MAC address of your existing PC to the gateway.

In such a case, you do not need to delay the setup process by informing your Service Provider of newly installed equipment.

➢ To use MAC cloning:

1. Click the 'MAC Cloning' icon in the 'Advanced' screen of the Web-based Management; the MAC Cloning screen appears (refer to the figure).

Figure 13-13: Advanced - MAC Cloning Settings



MAC Cloning

Set MAC of Device:	WAN Ethernet
To Physical Address:	00 : 90 : 8f : 09 : ef : 5e

2. Enter the physical MAC address to be cloned.
3. Press the button 'Clone My MAC Address'.

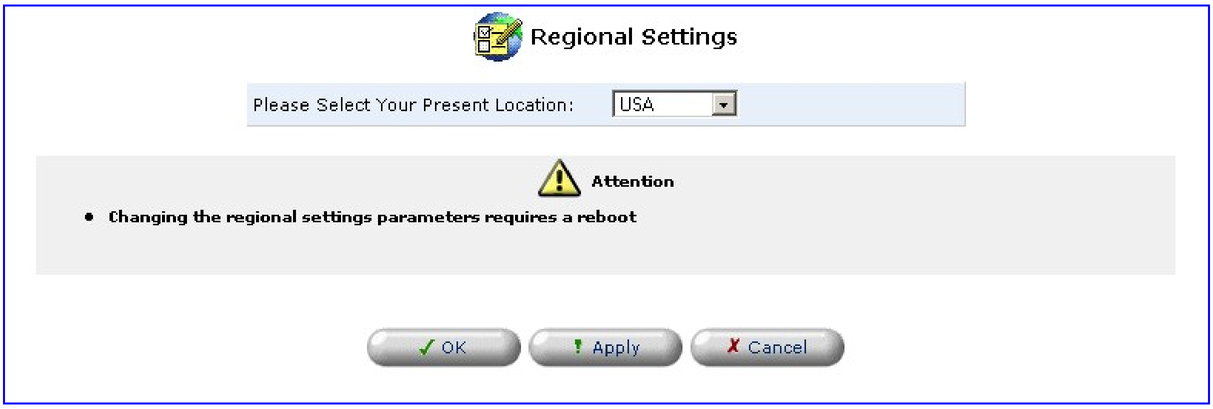
13.8 Regional Settings

The behavior and parameters of analog telephones lines vary between countries. The set of Call Progress Tones, the protocol used for caller ID and the analog line impedance are all location-specific. The MP-202 enables users to select the country they reside in and the MP-202 automatically selects the correct regional settings.

➢ To select your present location:

1. Click the icon 'Regional Settings' in the 'Advanced' screen of the Web-based Management; the 'Regional Settings' screen opens (refer to the figure below).
2. Select the country from the drop-down menu. If your current location is not in the list, contact your Service Provider.

Figure 13-14: Regional Settings



Regional Settings

Please Select Your Present Location: USA

Attention

- Changing the regional settings parameters requires a reboot

13.9 System Settings

The screen 'System Settings' allows you to configure various system and management parameters.

Use the screen section 'System Settings' to configure:

- The Telephone Adapter's host name. The host name is the Telephone Adapter's URL address.
- Your network's local domain.

Use the screen section 'MP-202 Management Console' to configure:

- Automatic Refresh of System Monitoring Web Pages - select this check-box to enable the automatic refresh of system monitoring web pages.
- Warn User Before Network Conguration Changes - select this check-box to activate user warnings before network configuration changes take effect.
- Session Lifetime - the duration of idle time (in seconds) in which the WBM session will remain active. When this duration times out, the user will have to re-login.
- Language - select a different language for the WBM interface.

Use the link 'Remote Administration' to access the MP-202's remote administration screen, from where you can selectively enable services that grant remote access to the MP-202.

Use the screen section 'Management Application Ports' to configure:

- Primary/secondary HTTP ports
- Primary/secondary HTTPS ports
- Primary/secondary Telnet ports
- Secure Telnet over SSL ports

Use the screen section 'System Logging' to configure:

- System Log buffer size
- Remote system notify level
    - None
    - Error
    - Warning
    - Information

Use the screen section 'Security Logging' to configure:

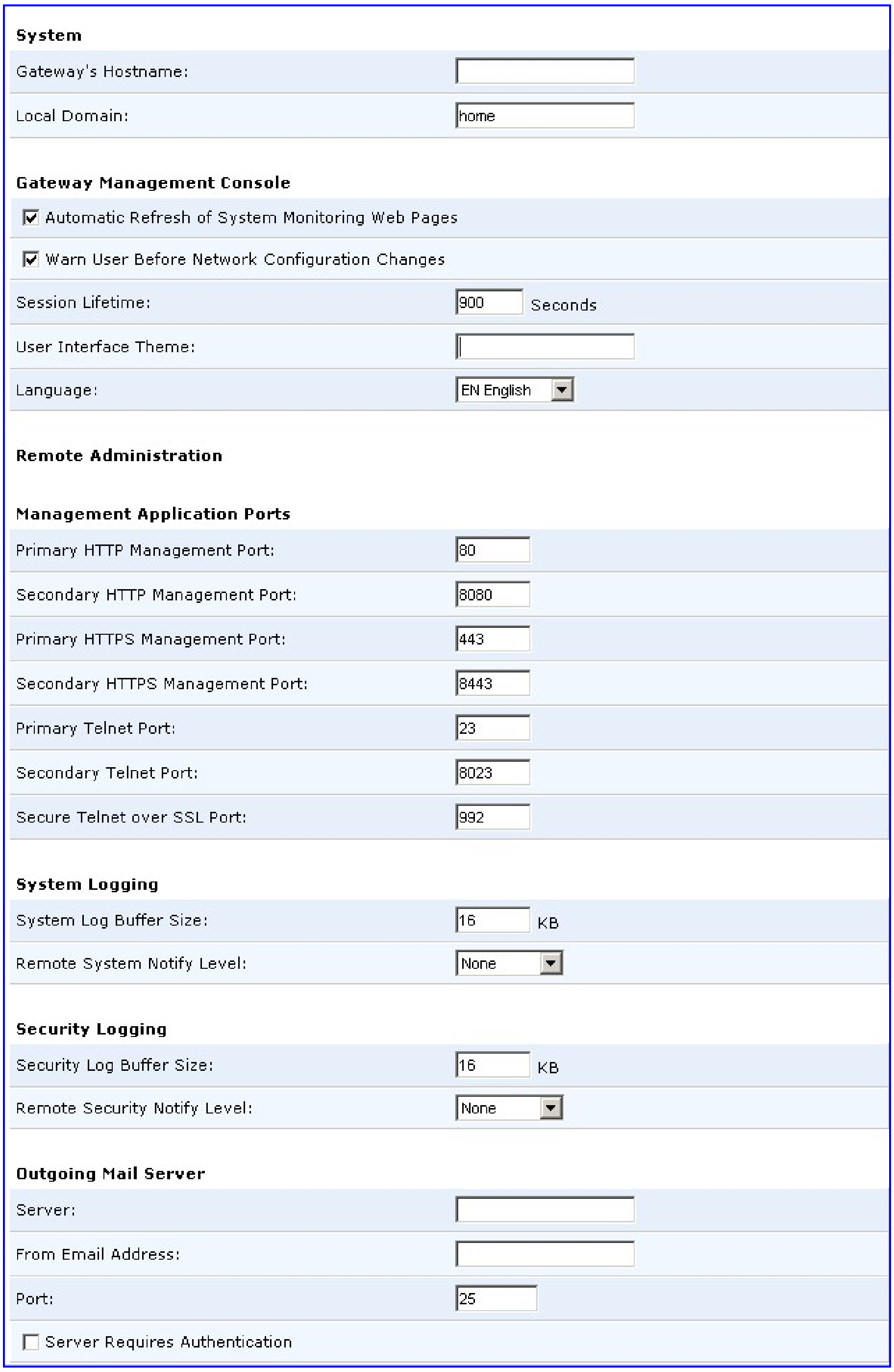
- Security Log buffer size
- Remote system notify level
    - None
    - Error
    - Warning
    - Information

Use the screen section 'Outgoing Mail Server':

- Enter the hostname of your outgoing (SMTP) server in the 'Server' field.
- Each email requires a 'from' address and some outgoing servers refuse to forward mail without a valid 'from' address for anti-spam considerations. Enter a 'from' email address in the 'From Email Address' field.
- If your outgoing mail server requires authentication check the 'Server Requires Authentication' check-box and enter your user name and password in the 'User Name' and 'Password' fields respectively.

- Enter the port that is used by your outgoing mail server.

Figure 13-15: System Settings



System

Gateway's Hostname:	
Local Domain:	home

Gateway Management Console

☑ Automatic Refresh of System Monitoring Web Pages

☑ Warn User Before Network Configuration Changes

Session Lifetime:	900 Seconds
User Interface Theme:	
Language:	EN English

Remote Administration

Management Application Ports

Primary HTTP Management Port:	80
Secondary HTTP Management Port:	8080
Primary HTTPS Management Port:	443
Secondary HTTPS Management Port:	8443
Primary Telnet Port:	23
Secondary Telnet Port:	8023
Secure Telnet over SSL Port:	992

System Logging

System Log Buffer Size:	16 KB
Remote System Notify Level:	None

Security Logging

Security Log Buffer Size:	16 KB
Remote Security Notify Level:	None

Outgoing Mail Server

Server:	
From Email Address:	
Port:	25

☐ Server Requires Authentication

13.10 SNMP

Simple Network Management Protocol (SNMP) enables Network Management Systems (NMSs) to remotely configure and monitor your gateway. Your Internet Service Provider (ISP) may use SNMP to identify and resolve technical problems.

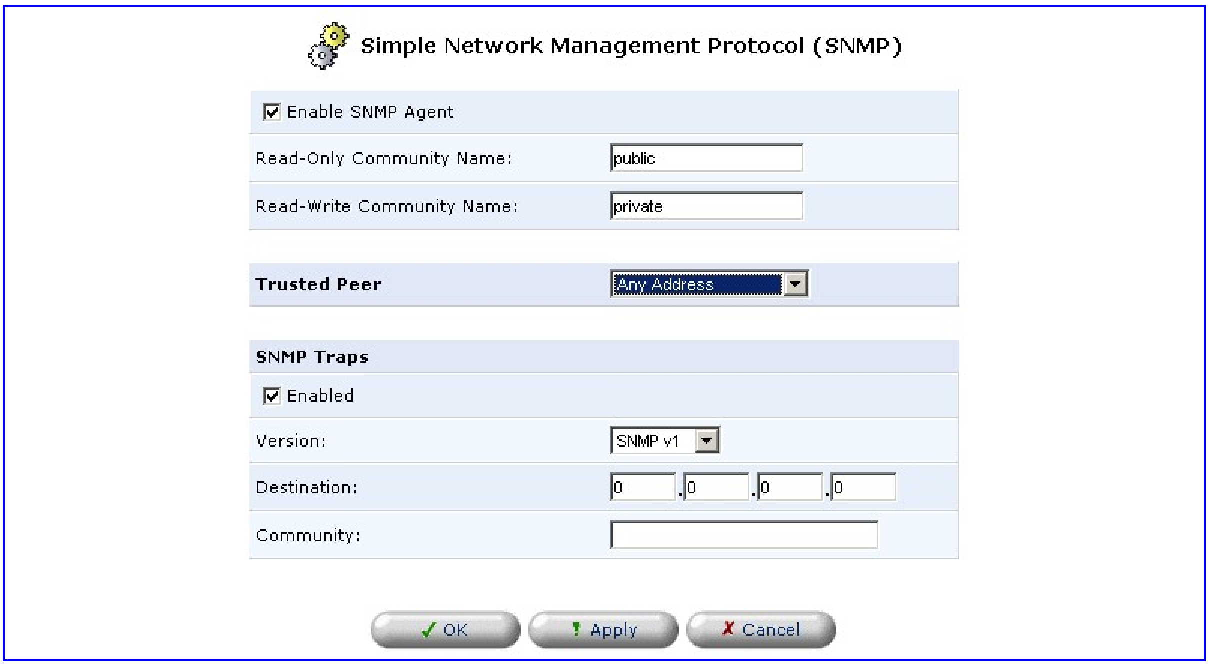
13.10.1 Configuring Your Gateway's SNMP Agent

Technical information regarding the properties of the gateway's SNMP agent should be provided by your ISP.

➢ To configure the gateway's SNMP agent:

1. Click the icon 'Simple Network Management Protocol (SNMP)' in the 'Advanced' screen of the Web-based Management; the SNMP screen appears (refer to the figure).

Figure 13-16: Advanced - SNMP



Simple Network Management Protocol (SNMP)

☑ Enable SNMP Agent

Read-Only Community Name: public

Read-Write Community Name: private

Trusted Peer: Any Address

SNMP Traps

☑ Enabled

Version: SNMP v1

Destination: 0 . 0 . 0 . 0

Community:

2. Define the SNMP parameters according to the instructions of the ISP:

Read-only/Write Community Names — SNMP community strings are passwords used in SNMP messages between the management system and the gateway. A read-only community allows the manager to monitor the gateway. A read-write community allows the manager to both monitor and configure the gateway.

SNMP Trusted Peer — The IP address, or subnet of addresses, that identify which remote management stations are allowed to perform SNMP operations on the gateway.

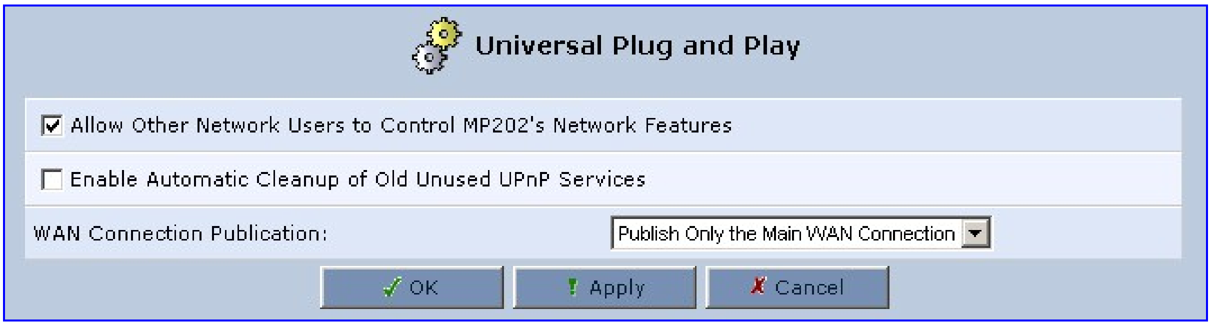
SNMP Traps — Messages sent by the gateway to a remote management station, in order to notify the manager about the occurrence of important events or serious conditions. The gateway supports both SNMP version 1 and SNMP version 2c traps.

13.11 Universal Plug and Play

➢ To configure UPnP:

- Click the icon 'Universal Plug and Play' in the 'Advanced' screen of the Web-based Management; the 'Universal Plug and Play' screen appears (refer to the figure).

Figure 13-17: Advanced - Universal Plug n Play



Universal Plug and Play

☑ Allow Other Network Users to Control MP202's Network Features

□ Enable Automatic Cleanup of Old Unused UPnP Services

WAN Connection Publication: Publish Only the Main WAN Connection

Universal Plug-and-Play is a networking architecture that provides compatibility among networking equipment, software and peripherals. UPnP-enabled products can seamlessly connect and communicate with other Universal Plug-and-Play enabled devices, without the need for user configuration, centralized servers, or product-specific device drivers. This technology leverages existing standards and technologies, including TCP/IP, HTTP 1.1 and XML, facilitating the incorporation of Universal Plug-and-Play capabilities into a wide range of networked products for the home.

Universal Plug-and-Play technologies are rapidly adopted and integrated into widely-used consumer products such as Windows XP. Therefore it is critical that today's Residential Gateways be UPnP-compliant. Your gateway is at the forefront of this development, offering a complete software platform for UPnP devices. This means that any UPnP-enabled control point (client) can dynamically join the network, obtain an IP address and exchange information about its capabilities and those of other computers on the network. They can subsequently communicate with each other directly, thereby further enabling peer-to-peer networking. And this all happens automatically, providing a truly zero-configuration network.

13.12 Firmware Upgrade

The MP-202 offers a built-in mechanism for upgrading its software image. There are two methods for upgrading the software image:

Upgrading from a Computer on the Network - use a software image file pre-downloaded to your PC's disk drive or located on the accompanying CD.

Upgrading from the Internet - also referred to as 'Remote Update', use this method to upgrade your firmware by remotely downloading an updated software image file.

Go to: "Upgrading from a Computer on the Network" on page 180

Go to: "Upgrading from the Internet" on page 181

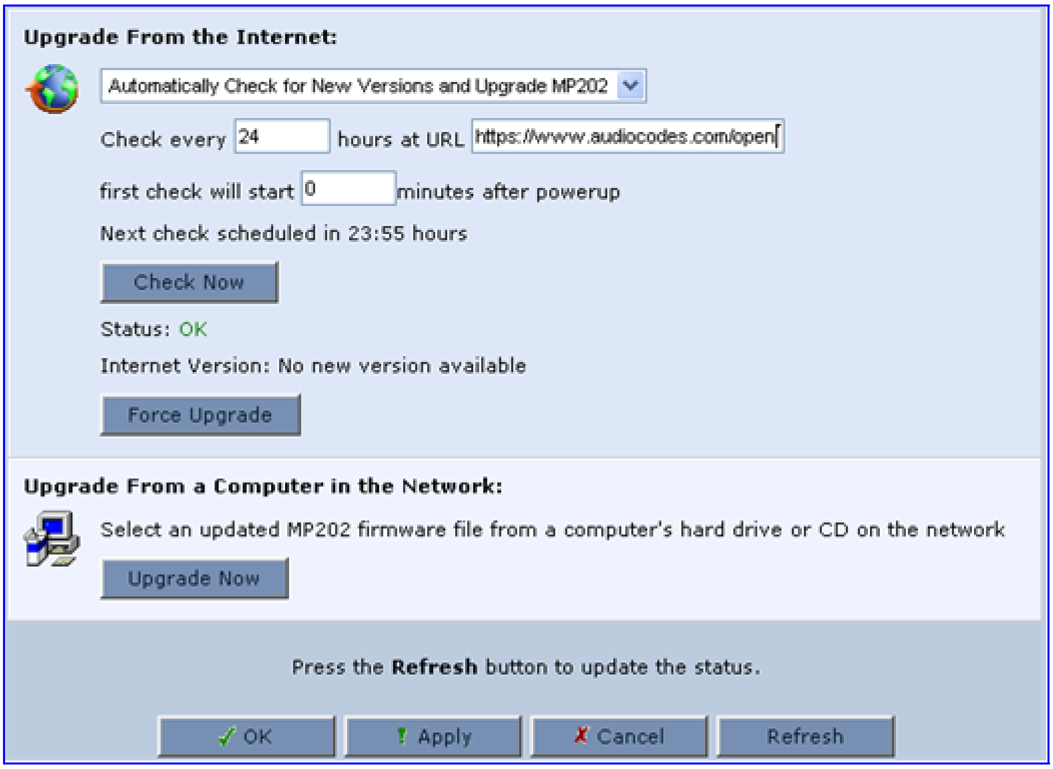
13.12.1 Upgrading From a Computer in the Network

➢ **To upgrade the MP-202's software image using a locally available .rmt file:**

> **Note:** You can only use files with an *rmt* extension when performing the firmware upgrade procedure.

1. Click the icon 'MP-202 Firmware Upgrade' from the 'Advanced' screen; the screen 'MP-202 Firmware Upgrade' opens (refer to the figure).

Figure 13-18: Advanced - Firmware and Configuration Upgrade



Upgrade From the Internet:

Automatically Check for New Versions and Upgrade MP202

Check every 24 hours at URL https://www.audiocodes.com/open

first check will start 0 minutes after powerup

Next check scheduled in 23:55 hours

Status: OK

Internet Version: No new version available

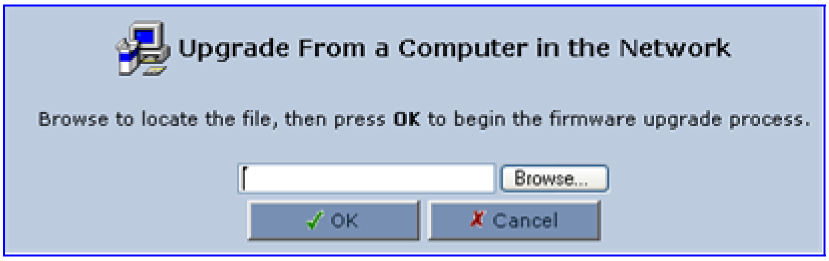
Upgrade From a Computer in the Network:

Select an updated MP202 firmware file from a computer's hard drive or CD on the network

Press the **Refresh** button to update the status.

2. In the screen section 'Upgrade From a Computer in the Network', click the button 'Upgrade Now'; the screen 'Upgrade From a Computer in the Network' opens (refer to the figure).

Figure 13-19: Advanced - Upgrading from a Computer in the Network



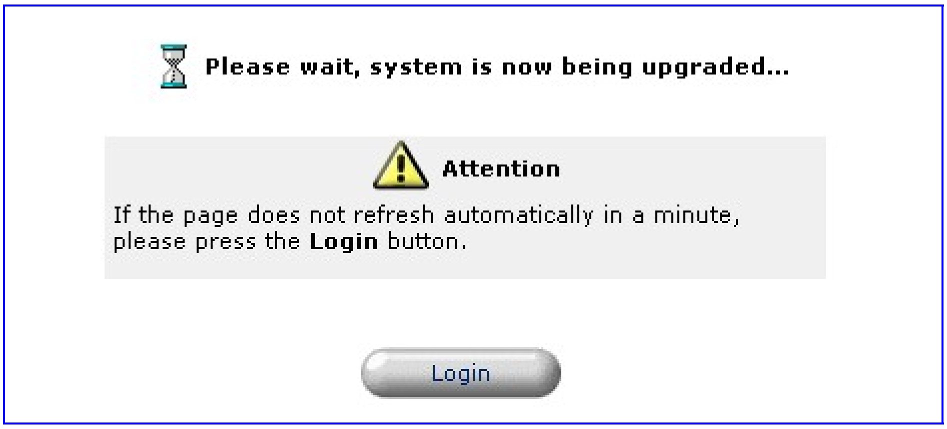
Upgrade From a Computer in the Network

Browse to locate the file, then press **OK** to begin the firmware upgrade process.

3. Enter the path of the software image file or click 'Browse' and navigate to the *rmt* file on your PC. Click 'OK'; the file starts loading from your PC to your gateway. When loading is complete, a confirmation screen prompts you if you want to upgrade to the new version.

4. Click 'OK' to confirm; the upgrade process commences and shouldn't take longer than a couple of minutes to complete.

Figure 13-20: Upgrade in Progress



Please wait, system is now being upgraded...

Attention

If the page does not refresh automatically in a minute, please press the **Login** button.

5. At the conclusion of the upgrade process, the device automatically reboots. The new software version runs, maintaining your custom configurations and settings.

Note: Do not power down the MP-202 or stop the upgrade process in the middle or else the MP-202 will become inoperable.

13.12.2 Upgrading From the Internet

The Remote Update mechanism helps you keep your software image up-to-date, by performing routine daily checks for newer software versions, as well as letting you perform manual checks.

To view the automatic check utility's settings and last check result, click the 'MP-202 Firmware Upgrade' icon from the 'Advanced' screen. The 'MP-202 Firmware Upgrade' screen will appear.

In the 'Upgrade From the Internet' section, you can select the utility's checking method and interval. The result of the last performed check is displayed by the line between the 'Check Now' and 'Force Upgrade' buttons, indicating whether a new version is available or not.

- If a new version is available:

  a. Click the 'Force Upgrade' button. A download process begins. When downloading is completed, a confirmation screen will appear, asking you if you want to upgrade to the new version.

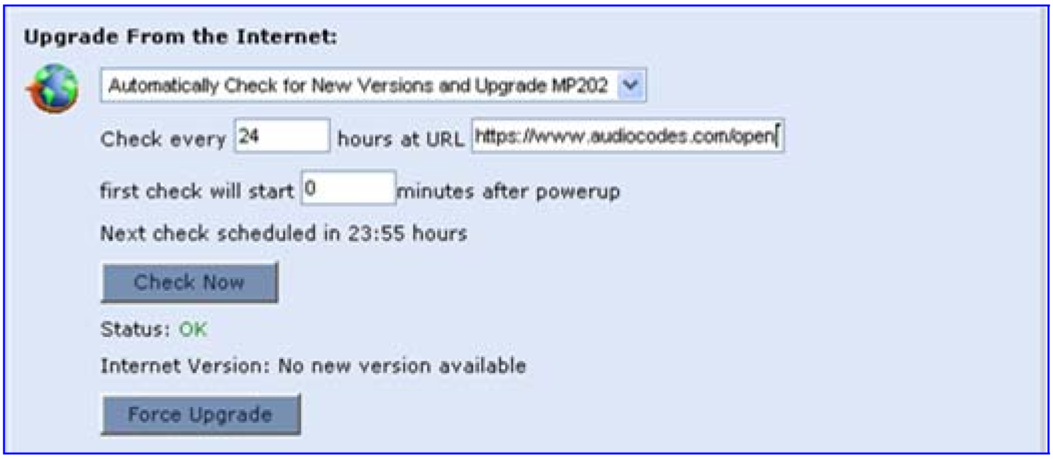
  b. Click 'OK' to confirm. The upgrade process will begin and should take no longer than one minute to complete.

  At the conclusion of the upgrade process, the MP-202 will automatically reboot. The new software version will run.

- If a new version is not available:

  a. Click the 'Check Now' button to perform an immediate check (instead of waiting for the next scheduled one). The screen will display a green "Check in progress..." message.

Figure 13-21: Remote Update Check



Upgrade From the Internet:

Automatically Check for New Versions and Upgrade MP202

Check every 24 hours at URL https://www.audiocodes.com/open

first check will start 0 minutes after powerup

Next check scheduled in 23:55 hours

Status: OK

Internet Version: No new version available

  b. Click the 'Refresh' button until the check is completed and the result is displayed.

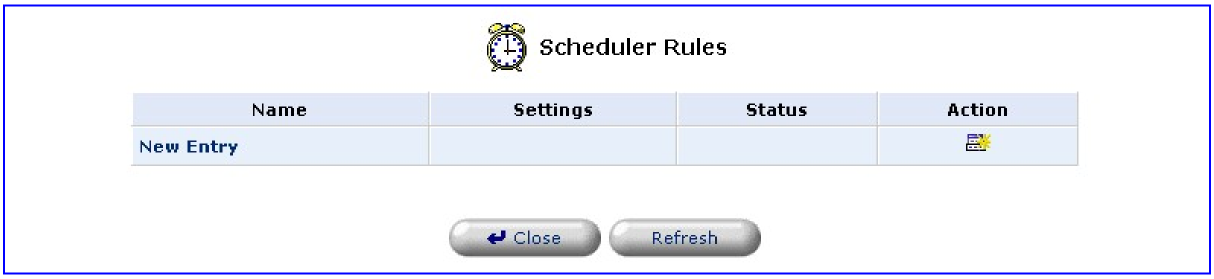
13.13 Scheduler Rules

Scheduler rules are used for limiting the activation of Firewall rules to specific time periods, specified in days of the week, and hours.

➢ To define a Rule:

1. Click the icon 'Scheduler Rules' in the 'Advanced' screen of the Web-based Management; the 'Scheduler Rules' screen appears (refer to the figure).

Figure 13-22: Advanced - Scheduler Rules

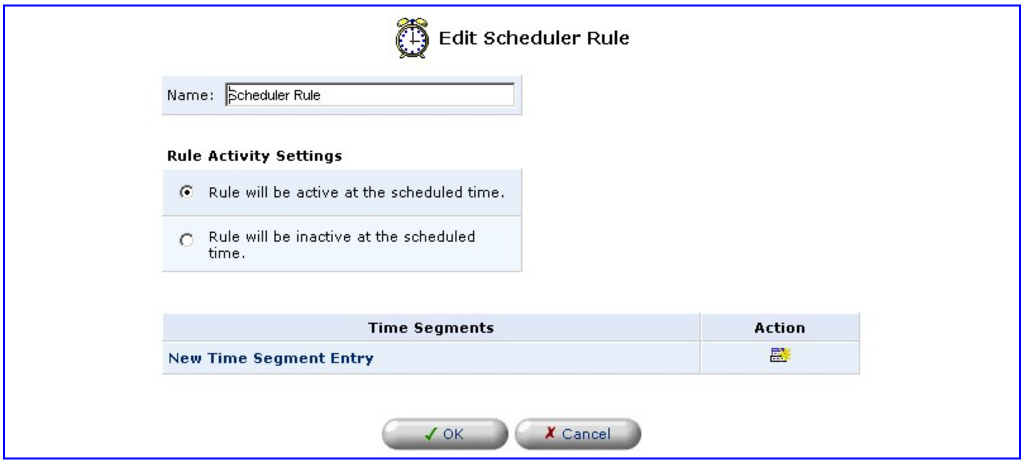


Scheduler Rules

Name	Settings	Status	Action
New Entry			

2. Click the link 'New Scheduler Entry'; the 'Scheduler Rule Edit' screen appears (refer to the figure).

Figure 13-23: Advanced - Scheduler Rules - Edit Scheduler Rule



Edit Scheduler Rule

Name: Scheduler Rule

Rule Activity Settings

● Rule will be active at the scheduled time.

○ Rule will be inactive at the scheduled time.

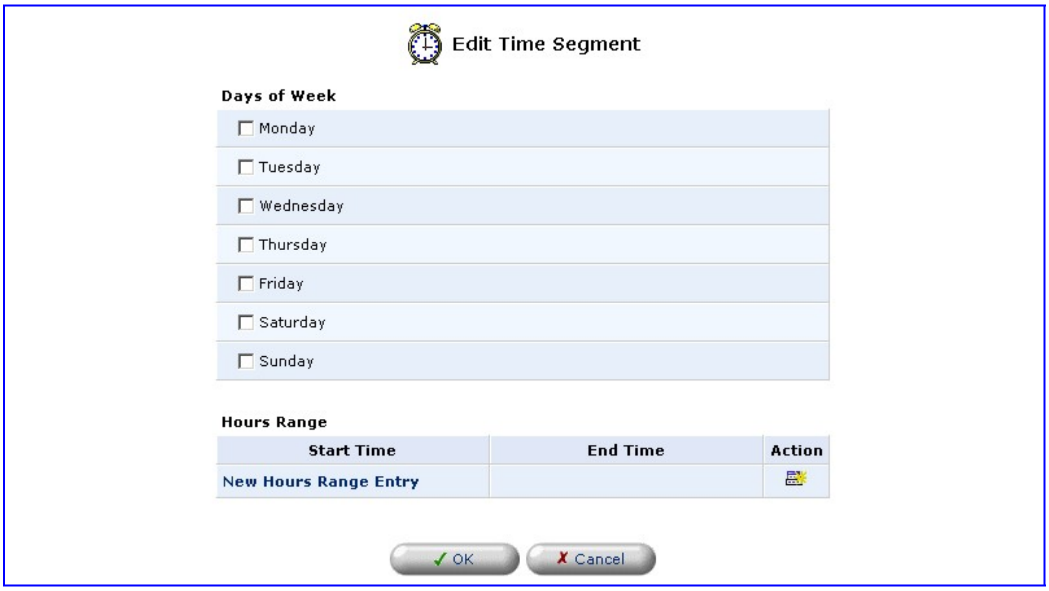
Time Segments	Action
New Time Segment Entry	✎

3. Specify a name for the rule in the 'Name' field.

4. Specify if the rule will be active/inactive during the designated time period, by selecting the appropriate 'Rule Activity Settings' check-box.

5. Click the link 'New Time Segment Entry' to define the time segment to which the rule will apply; the 'Time Segment Edit' screen appears (refer to the figure).

Figure 13-24: Advanced - Scheduler Rules - Time Segment Edit



Edit Time Segment

Days of Week

□ Monday

□ Tuesday

□ Wednesday

□ Thursday

□ Friday

□ Saturday

□ Sunday

Hours Range

Start Time	End Time	Action
New Hours Range Entry		✎

   a. Select active/inactive days of the week.

   b. Click the 'New Time Segment Entry' to define an active/inactive hourly range.

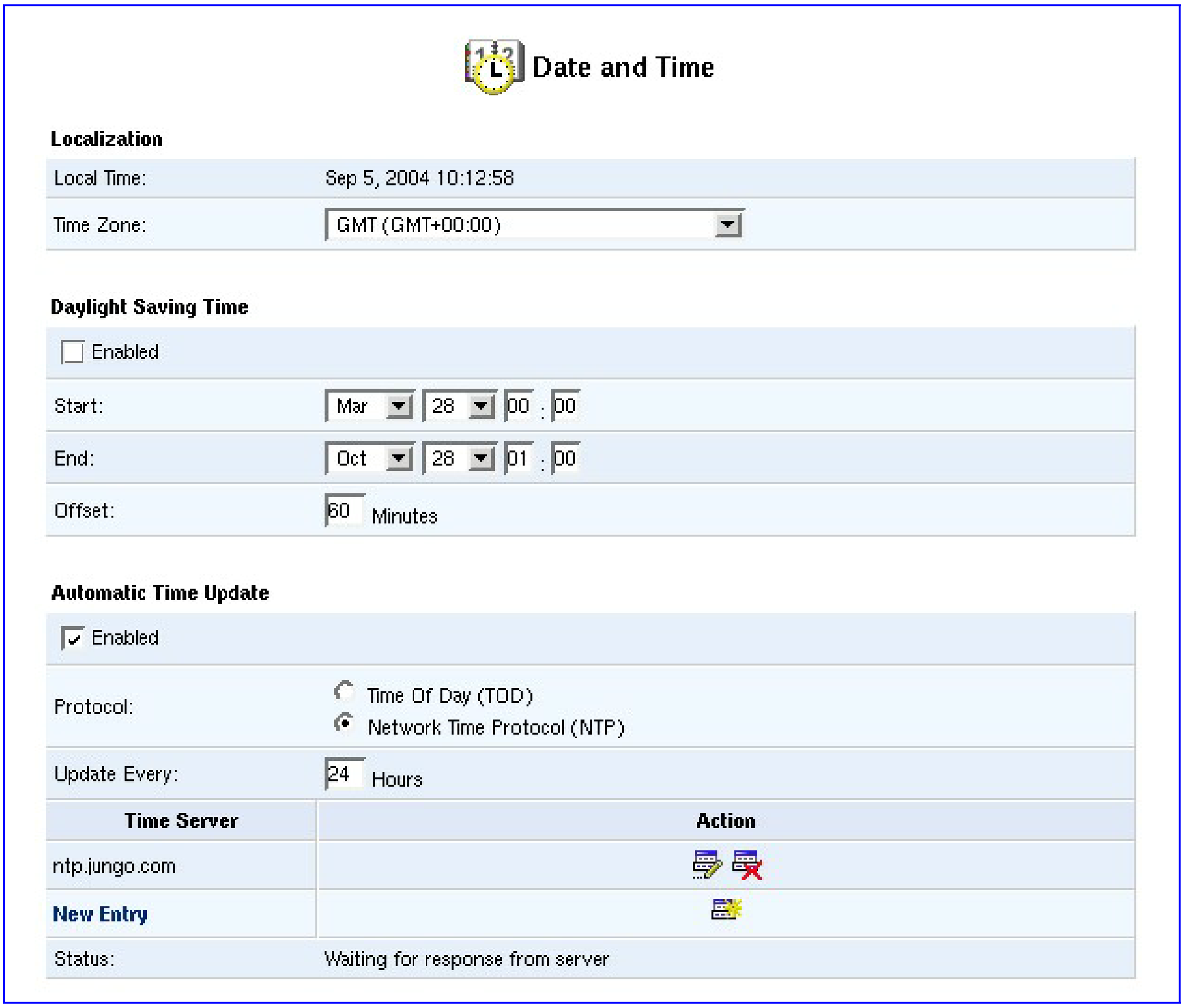
6. Click 'OK' to save the settings.

13.14 Date & Time

➢ To configure date, time and daylight savings time settings:

1. Click the 'Date and Time' icon in the 'Advanced' screen of the Web-based Management. The 'Date & Time' settings screen will be displayed.

Figure 13-25: Date & Time Settings



Date and Time

Localization

Local Time:	Sep 5, 2004 10:12:58
Time Zone:	GMT (GMT+00:00)

Daylight Saving Time

□ Enabled

Start:	Mar 28 00 : 00
End:	Oct 28 01 : 00
Offset:	60 Minutes

Automatic Time Update

☑ Enabled

Protocol: ○ Time Of Day (TOD) ● Network Time Protocol (NTP)

Update Every: 24 Hours

Time Server	Action
ntp.jungo.com	
New Entry	

Status: Waiting for response from server

2. Select the local time zone from the pull-down menu. The MP-202 can automatically detect daylight saving setting for selected time zones. If the daylight saving settings for your time zone are not automatically detected, the following fields will be displayed:

Enabled	Select this check box to enable daylight saving time.
Start	Date and time when daylight saving starts.
End	Date and time when daylight saving ends.
Offest	Daylight saving time offset.

➢ For the Telephone Adapter to perform an automatic time update:

- Select the 'Enabled' checkbox under the 'Automatic Time Update' section.
- Select the protocol to be used to perform the time update by selecting wither the 'Time of Day' or 'Network Time Protocol' radio button.
- Specify how often to perform the update in the 'Update Every' field.
- You can define time server addresses by pressing the 'New Entry' link on the bottom of the 'Automatic Time Update' section.

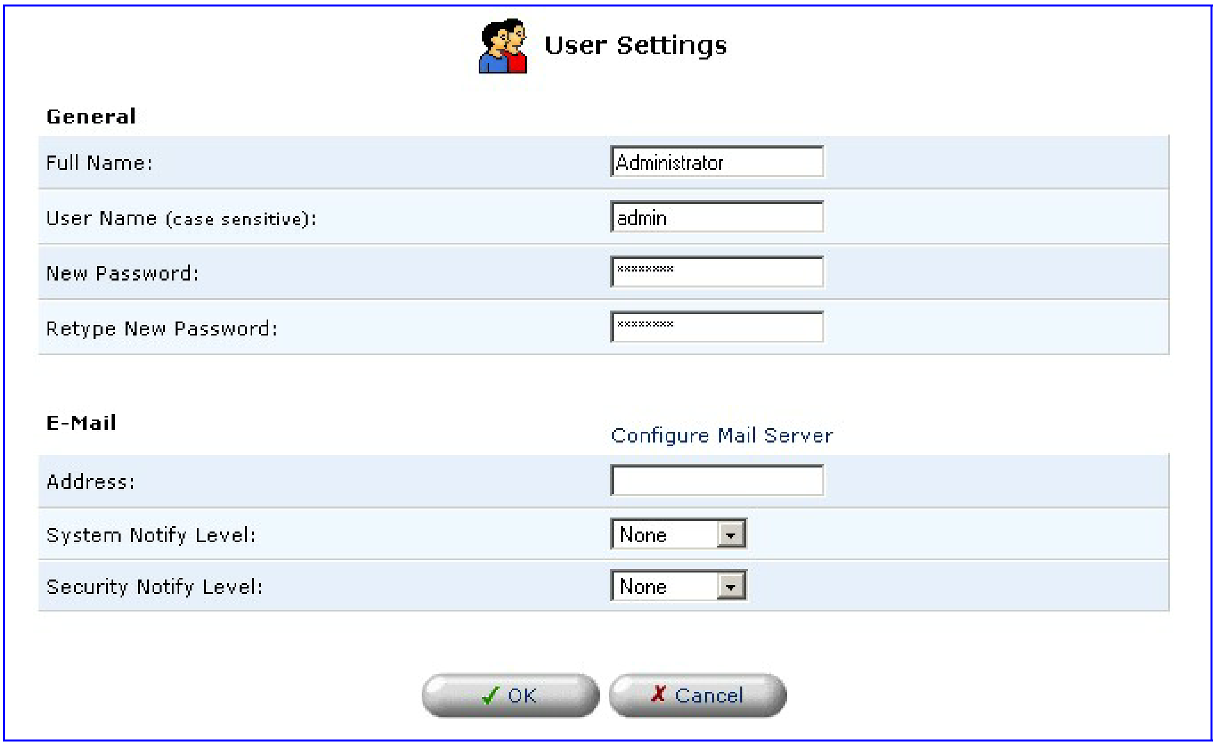
13.15 Configuring Users

You can add, edit and delete users. When adding a user, you need to specify the following parameters:

Table 13-2: Managing Users

Parameter	Description
Full Name	The remote user's full name.
User Name	The name a remote user will use to access your home network.
New Password	Type a new password for the remote user. If you do not want to change the remote user's password leave this field empty.
Retype New Password	If a new password was assigned, type it again to verify correctness.

Figure 13-26: Managing Users



User Settings

General

Full Name:	Administrator
User Name (case sensitive):	admin
New Password:	********
Retype New Password:	********

E-Mail

Configure Mail Server

Address:	
System Notify Level:	None
Security Notify Level:	None

Note that changing any of the user parameters will prompt the connection associated with the user to terminate. For changes to take effect you should activate the connection manually after modifying user parameters.

13.15.1 Email Notification

You can use email notification to receive indications of system events for a predefined severity classification. The available types of events are 'System' or 'Security' events. The available severity of events are 'Error', 'Warning' and 'Information'. If the 'Information' level is selected the user will receive notification of 'Information', 'Warning' and 'Error' events. If the 'Warning' level is selected the user will receive notification of 'Warning' and 'Error' events etc.

➢ To configure email notification for a specific user:

1. Make sure you have configured an outgoing mail server in 'System Settings'. A click on the 'Configure Mail Server' link will display the 'System Settings' page were you can configure the outgoing mail server.

2. Enter the user's email address in the 'Address' field in the 'Email' section.

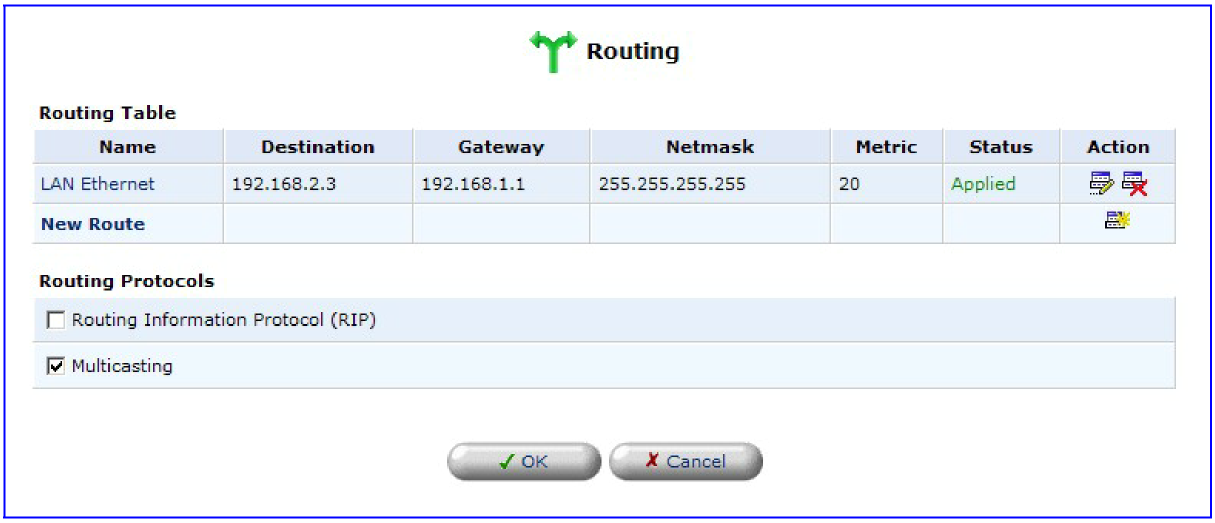
3. Select the 'System' and 'Security' notification levels in the 'System Notify Level' and 'Security Notify Level' combo boxes respectively.

13.16 Routing

13.16.1 Managing Routing Table Rules

You can access the routing table rules by clicking the 'Routing' icon from the 'Advanced' screen. The 'Routing' screen will appear.

Figure 13-27: Routing Rules



Routing

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Ethernet	192.168.2.3	192.168.1.1	255.255.255.255	20	Applied	
New Route						

Routing Protocols

☐ Routing Information Protocol (RIP)

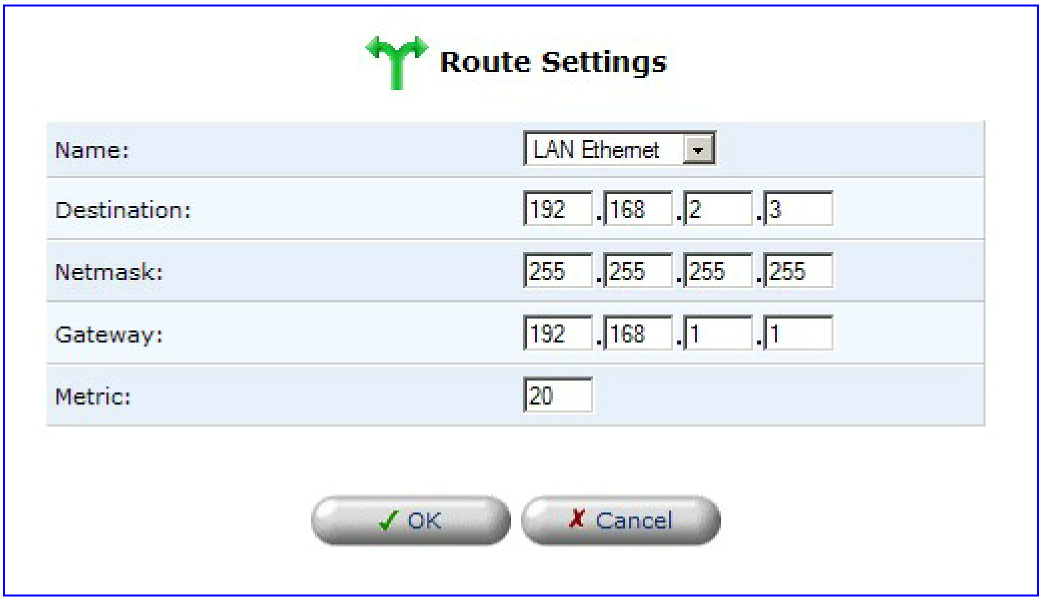
☑ Multicasting

When adding a routing rule, you need to specify:

Table 13-3: Adding a Routing Rule - Parameter Descriptions

Parameter	Description
Device	Select the network device.
Destination	The destination is the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.
Netmask	The network mask is used in conjunction with the destination to determine when a route is used.
Gateway	Enter the Telephone Adapter's IP address.
Metric	A measurement of the preference of a route. Typically, the lowest metric is the most preferred route. If multiple routes exist to a given destination network, the route with the lowest metric is used.

Figure 13-28: Routing Rule Settings



Route Settings

Name:	LAN Ethernet
Destination:	192 . 168 . 2 . 3
Netmask:	255 . 255 . 255 . 255
Gateway:	192 . 168 . 1 . 1
Metric:	20

13.16.2 Multicasting

The MP-202 provides support for IGMP multicasting, which allows hosts connected to a network to be updated whenever an important change occurs in the network. A multicast is simply a message that is sent simultaneously to a pre-defined group of recipients. When you join a multicast group you will receive all messages addressed to the group, much like what happens when an e-mail message is sent to a mailing list.

IGMP multicasting enables UPnP capabilities over wireless networks and may also be useful when connected to the Internet through a router. When an application running on a computer in the home network sends out a request to join a multicast group the MP-202 intercepts and processes the request. If the MP-202 is set to 'Minimum Security' no further action is required. However, if the MP-202 is set to 'Typical Security' or 'Maximum Security' you must add the group's IP address to the MP-202's 'Multicast Groups' screen. This will allow incoming messages addressed to the group to pass through the Firewall and on to the correct LAN computer.

1. Click the 'Routing' icon in the 'Advanced' screen.
2. Select the 'Multicast Groups Management' check-box.
3. Press the 'OK' button.

13.17 Network Objects

Network Objects is a method used to abstractly define a set of LAN hosts, according to one or more MAC address, IP address, and host name. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring the gateway's security filtering settings such as IP address filtering, host name filtering or MAC address filtering.

You can use network objects in order to apply security rules based on host names instead of IP addresses. This may be useful, since IP addresses change from time to time. Moreover, it is possible to define network objects according to MAC addresses, making rule application more persistent against network configuration settings.

➢ To define a network object:

1. Click the icon 'Network Objects' in the 'Advanced' screen of the Web-based Management; the 'Network Objects' screen appears (refer to the figure).

Network Objects

2. Click the link 'New Entry', the 'Edit Network Object' screen appears (refer to the figure).

Edit Network Object

3. Name the network object in the Description field, and click New Entry to actually create it; the 'Edit Item' screen appears (refer to the figure).
4. The source address can be entered in one of the following methods:
   - IP Address
   - IP Subnet
   - IP Range
   - MAC Address
   - Host Name
5. When selecting a method from the combo box, the screen refreshes, presenting the respective fields by which to enter the relevant information.

Edit Item

6. Select a method and enter the source address accordingly.
7. Click 'OK' to save the settings.

13.18 Dynamic DNS

The Dynamic DNS (DDNS) service enables you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessible from various locations on the Internet. Typically, when you connect to the Internet, your service provider assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of a specific connection. Dynamically assigning addresses extends the usable pool of available IP addresses, whilst maintaining a constant domain name.

When using the DDNS service, each time the IP address provided by your ISP changes, the DNS database will change accordingly to reflect the change. In this way, even though your IP address will change often, your domain name will remain constant and accessible.

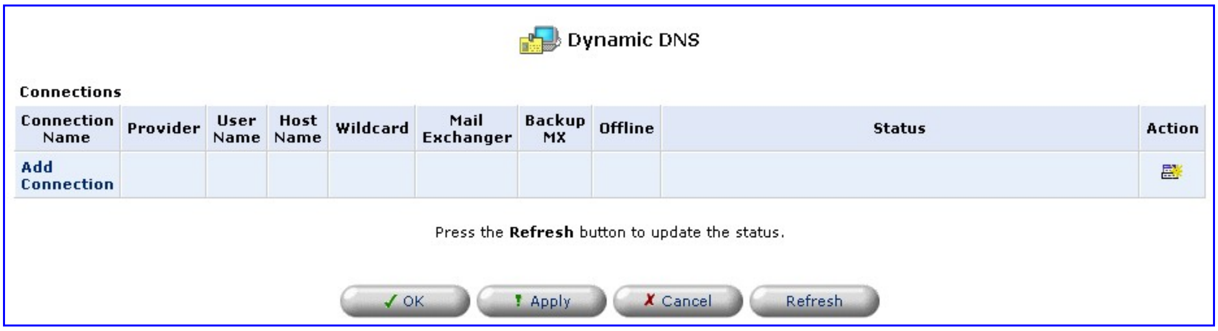
13.18.1 Opening a Dynamic DNS Account

To be able to use the DDNS feature, you must first open a free DDNS account at http://www.dyndns.org/account/create.html.
When applying for an account, you will need to specify a user name and password. Have them readily available when customizing the MP-202's DDNS support. For detailed information on DDNS, refer to http://www.dyndns.org.

➢ To open a dynamic DNS account:

- Click the icon 'Dynamic DNS' in the 'Advanced' screen of the Management Console; the 'Dynamic DNS' connections screen opens (refer to the figure) displaying a table showing the different connections and their DDNS aliases.

Figure 13-29: Advanced - Dynamic DNS



Dynamic DNS

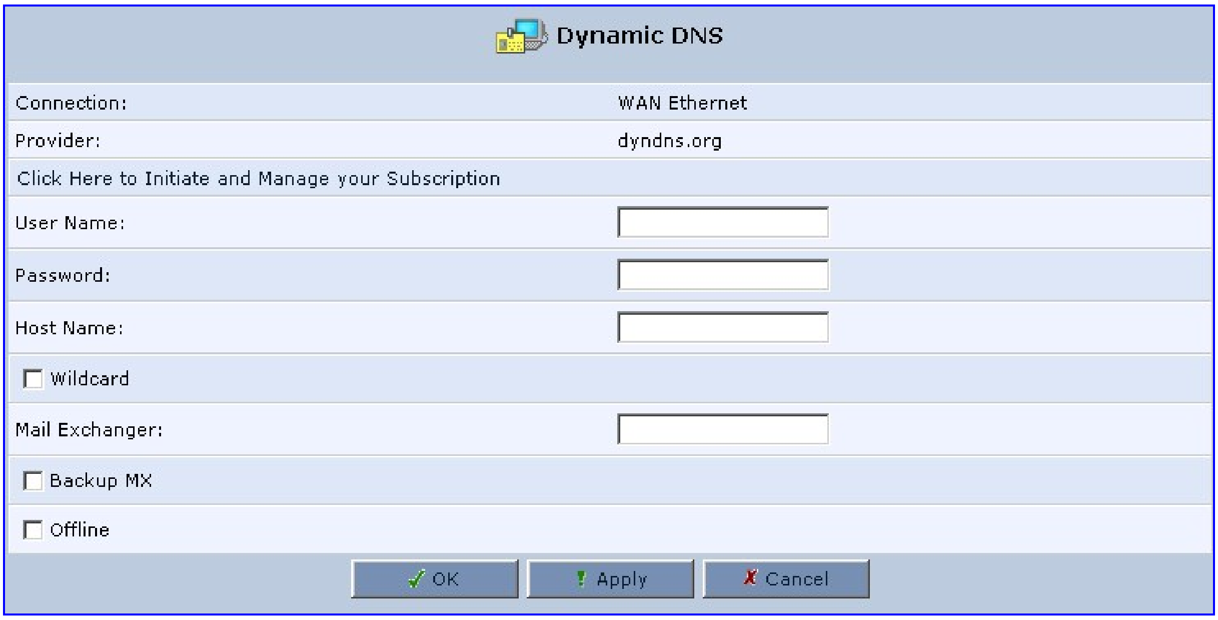
Connections

Connection Name	Provider	User Name	Host Name	Wildcard	Mail Exchanger	Backup MX	Offline	Status	Action
Add Connection									

Press the **Refresh** button to update the status.

- Click the link 'Add Connection' to add a new connection; alternatively, click the icon under 'Action'; the 'Dynamic DNS' screen appears (refer to the figure).

Figure 13-30: Advanced - Dynamic DNS



Dynamic DNS

Connection:	WAN Ethernet
Provider:	dyndns.org
Click Here to Initiate and Manage your Subscription	
User Name:	
Password:	
Host Name:	
□ Wildcard	
Mail Exchanger:	
□ Backup MX	
□ Offline	

- Configure the DDNS parameters. Use the table below as a reference.

Table 13-4: Dynamic DNS Parameter Descriptions

Dynamic DNS Parameter	Description
Connection	In a single WAN scenario, the connection parameter appears as static text (non-configurable). However, if you have multiple WAN devices, a combo-box appears (refer to the figure), enabling you to select the connection to which you would like to couple the DDNS service. The DDNS service only uses the chosen device, unless fail-over is enabled. In this case, the failed-to device will be used instead (assuming its route rules consent), until the chosen device is up again.
Provider	Select your DDNS service provider. Currently, only dyndns.org is supported. Click Here to Initiate and Manage your Subscription Clicking this link opens a new browser page in http://www.dyndns.com/account/.
User Name	Enter your DDNS user name.
Password	Enter your DDNS password.
Host Name	Enter your full DDNS domain name.
Wildcard	Select this check-box to enable use of special links such as www.<yourhost>.dyndns.org.
Mail Exchanger	Enter your mail exchange server address, to redirect all e-mails arriving at your DDNS address to your mail server.
Backup MX	Select this check-box to designate the mail exchange server to be a backup server.
Offliine	To temporarily take your site offliine (prevent traffic from reaching your DDNS domain name), check this box to enable redirection of DNS requests to an alternative, predefined URL. The availability of this feature depends on your DDNS account's level of service. The redirection URL must be configured through the account as well.

13.19 IP Address Distribution

Your gateway's Dynamic Host Configuration Protocol (DHCP) server makes it possible to easily add computers that are configured as DHCP clients to the home network. It provides a mechanism for allocating IP addresses and delivering network configuration parameters to such hosts. The gateway's default DHCP server is the LAN bridge.

A client (host) sends out a broadcast message on the LAN requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as `taken'. At this point the host is configured with an IP address for the duration of the lease.

The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease then it will also receive current information about network services, as it did with the original lease, allowing it to update its network configurations to reject any changes that may have occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration it can send a release message to the DHCP server, which will then make the IP address available for use by others.

Your gateway's DHCP server:

- Displays a list of all DHCP host devices connected to the gateway
- Defines the range of IP addresses that can be allocated in the LAN
- Defines the length of time for which dynamic IP addresses are allocated
- Provides the above configurations for each LAN device and can be configured and enabled/disabled separately for each LAN device
- Can assign a static lease to a LAN PC so that it receives the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computers
- Provides the DNS server with the host name and IP address of each PC that is connected to the LAN

Additionally, the gateway can act as a DHCP relay, escalating DHCP responsibilities to a WAN DHCP server. In this case, the gateway will act merely as a router, while its LAN hosts will receive their IP addresses from a DHCP server on the WAN.

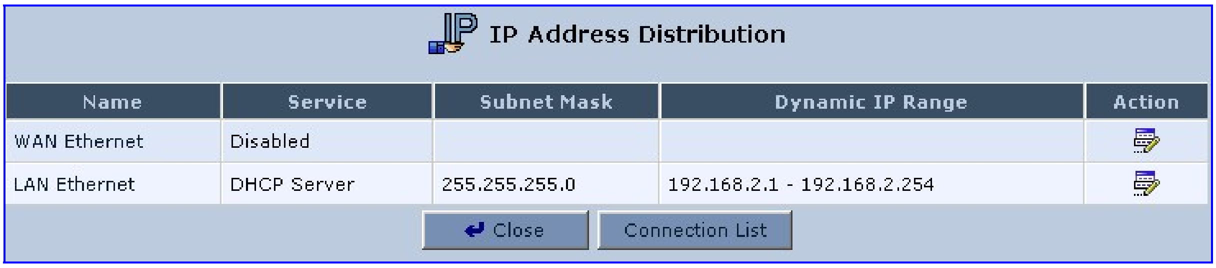
With the gateway's optional Zero Configuration Technology feature, the IP Auto Detection method detects statically-defined IP addresses in addition to the gateway's DHCP clients. It learns all the IP addresses on the LAN, and integrates the collected information with the database of the DHCP server. This allows the DHCP server to issue valid leases, thus avoiding conflicting IP addresses used by other computers in the network.

13.19.1 DHCP Server Parameters

➢ To view a summary of the services currently being provided by the DHCP server:

- Click the icon 'IP Address Distribution' in the 'Advanced' screen; the 'IP Address Distribution' screen opens.

Figure 13-31: DHCP Server Summary



IP Address Distribution

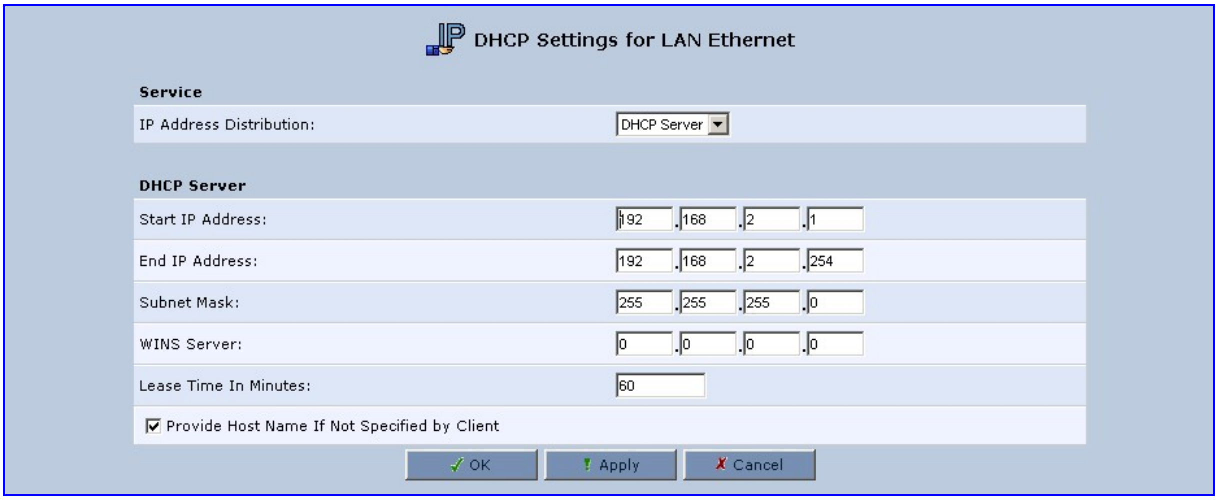
Name	Service	Subnet Mask	Dynamic IP Range	Action
WAN Ethernet	Disabled			✎
LAN Ethernet	DHCP Server	255.255.255.0	192.168.2.1 - 192.168.2.254	✎

Note: If In the column 'Service' of the 'IP Address Distribution' screen, if a gateway is indicated 'Disabled', then DHCP services are not being provided to hosts connected to the network through that gateway. This means that the gateway will not assign IP addresses to these computers, which is useful if you wish to work with static IP addresses only.

➢ To edit the DHCP server settings for a device:

1. Under the column 'Action', click the icon 'Edit'; the DHCP Server settings for this device are displayed (refer to the figure).

Figure 13-32: Advanced - IP Address Distribution - DHCP Server



DHCP Settings for LAN Ethernet

Service

IP Address Distribution: DHCP Server

DHCP Server

Start IP Address: 192 . 168 . 2 . 1

End IP Address: 192 . 168 . 2 . 254

Subnet Mask: 255 . 255 . 255 . 0

WINS Server: 0 . 0 . 0 . 0

Lease Time In Minutes: 60

☑ Provide Host Name If Not Specified by Client

2. From the 'IP Address Distribution' drop-down list, select whether to enable or disable the DHCP server.

3. From the 'IP Address Distribution' drop-down list, select whether the gateway will function as a DHCP server or as DHCP relay. Choose 'DHCP Server'; the screen section 'DHCP Server' is displayed, showing the parameters described in the table below.

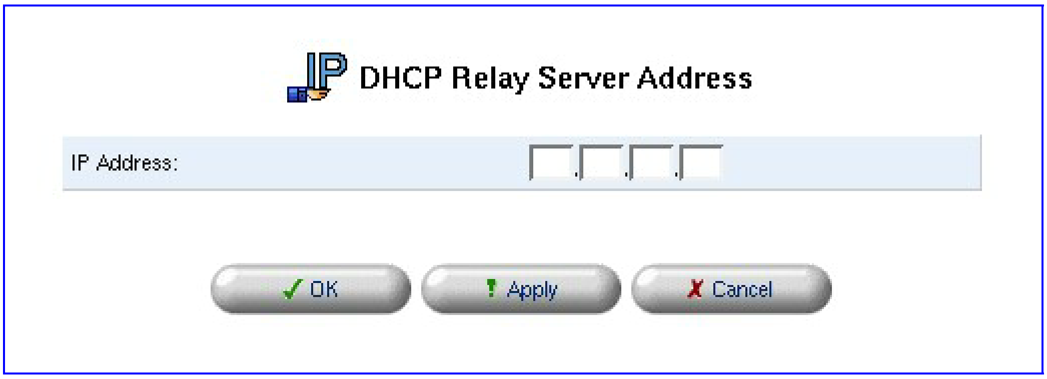
Table 13-5: DHCP Server Parameter Descriptions

Parameter	Description
IP Address Range (Start and End)	Determines the number of hosts that may be connected to the network in this subnet. `Start' specifies the first IP address that may be assigned in this subnet and `End' specifies the last IP address in the range.
Subnet Mask	A mask used to determine what subnet an IP address belongs to. An example of a subnet mask value is 255.255.0.0.
Lease Time	Each device will be assigned an IP address by the DHCP server for a limited time (`Lease Time') when it connects to the network. When the lease expires the server will determine if the computer has disconnected from the network. If it has, then the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use will become available for other computers on the network.
Provide host name if not specified by client	If the DHCP client does not have a host name, the Telephone Adapter will assign the client a default name.

➢ To configure a DHCP relay server:

1. From the 'IP Address Distribution' drop-down list, select 'DHCP Relay'; the screen 'DHCP Relay Server Address' opens (refer to the figure below). Use this screen to configure your DHCP server's IP address.

Figure 13-33: DHCP Server Relay



DHCP Relay Server Address

IP Address: ___ . ___ . ___ . ___

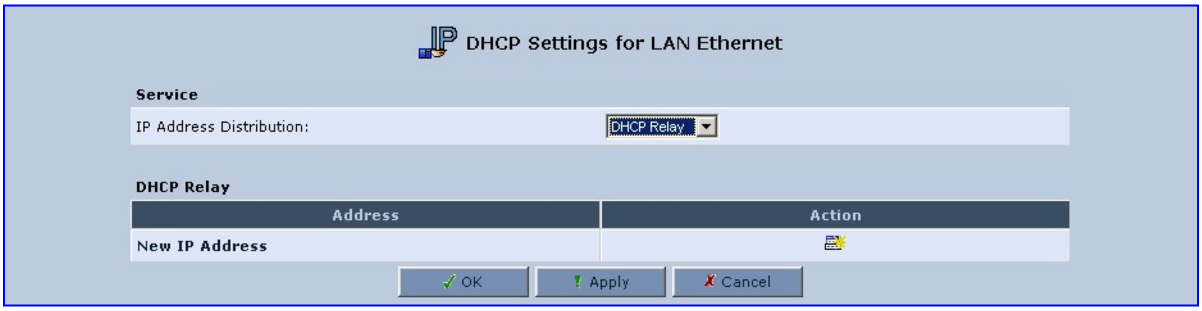
2. Click 'OK' to save your changes.

13.19.2 DHCP Relay Parameters

To configure a device as a DHCP relay, perform the following steps:

1. Select the 'DHCP Relay' option in the 'IP Address Distribution' drop-down list under the screen section 'Service' (refer to the figure).

Figure 13-34: Advanced - IP Address Distribution - DHCP Relay



DHCP Settings for LAN Ethernet

Service

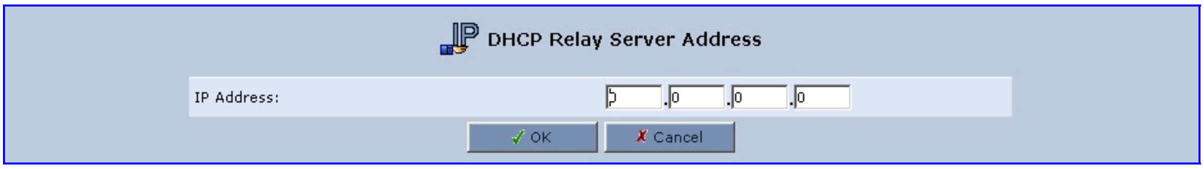
IP Address Distribution: DHCP Relay

DHCP Relay

Address	Action
New IP Address	

2. Click the link 'New IP Address'; the 'DHCP Relay Server Address' screen opens (refer to the figure).

Figure 13-35: Advanced - IP Address Distribution - DHCP Relay - New IP Address



DHCP Relay Server Address

IP Address: 0 .0 .0 .0

3. Specify the IP address of the DHCP server.

4. Click 'OK' to save the settings.

5. Click 'OK' once more in the 'DHCP Settings' screen.

6. Click the icon 'Network Connections' on the sidebar of the main screen; the screen 'Network Connections' opens.

7. Click the link 'WAN Ethernet'; the 'WAN Ethernet Properties' screen opens.

8. Press the button 'Settings'; the screen 'Configure WAN Ethernet' opens.

9. In the screen section 'Routing', select 'Advanced' from the drop-down list; the screen refreshes.

10. In the 'Routing Mode' drop-down list, select 'Route'; this changes the gateway's WAN to work in routing mode, which is necessary in order for DHCP relaying to function correctly.

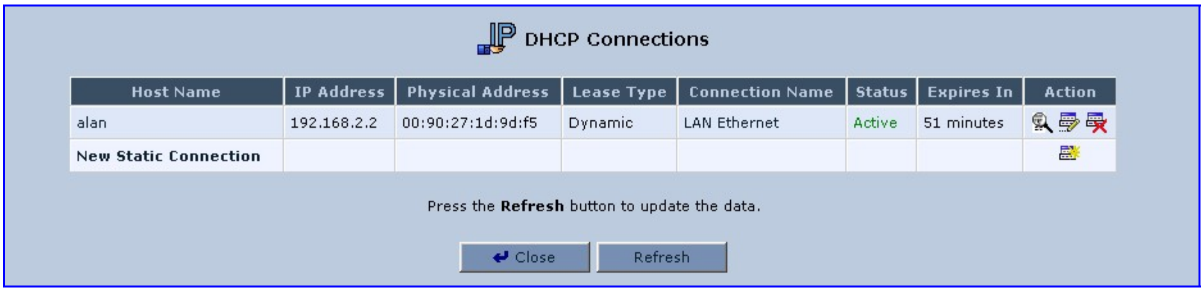
11. Click 'OK' to save the settings.

13.19.3 DHCP Connections

➢ To view a list of computers currently recognized by the DHCP server:

1. Open the screen 'IP Address Distribution' and click button 'Connection List' (refer to the figure); the 'IP Address Distribution' screen opens.

Figure 13-36: Advanced - IP Address Distribution - Connection List



DHCP Connections

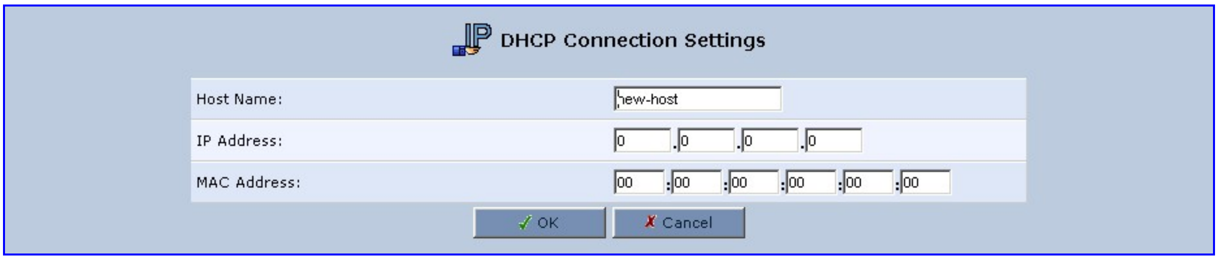
Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expires In	Action
alan	192.168.2.2	00:90:27:1d:9d:f5	Dynamic	LAN Ethernet	Active	51 minutes	
New Static Connection							

Press the **Refresh** button to update the data.

➢ To define a new connection with a fixed IP address:

1. Click the link 'New Static Connection'; the screen 'DHCP Connection Settings' opens (refer to the figure).

Figure 13-37: Advanced - IP Address Distribution - Connection List - New Static Connection



DHCP Connection Settings

Host Name:	new-host
IP Address:	0 . 0 . 0 . 0
MAC Address:	00 : 00 : 00 : 00 : 00 : 00

2. Enter a host name for this connection.
3. Enter the fixed IP address to be assigned to the computer.
4. Enter the MAC address of the computer's network card.

> **Note:** A device's fixed IP address is actually assigned to the specific network card's (NIC) MAC address installed on the LAN computer. If you replace this network card then you must update the device's entry in the DHCP Connections list with the new network card's MAC address.

- Click 'OK' to save the settings; the 'DHCP Connections' screen reappears displaying the defined static connection. This connection can be edited or deleted using the standard 'Action' icon.

13.20 DNS Server

Domain Name System (DNS) provides a service that translates domain names into IP addresses and vice versa. The Telephone Adapter's DNS server is an auto-learning DNS, which means that when a new computer is connected to the network the DNS server learns its name and automatically adds it to the DNS table. Other network users may immediately communicate with this computer using either its name or its IP address.

In addition your Telephone Adapter's DNS:

- Shares a common database of domain names and IP addresses with the DHCP server.
- Supports multiple subnets within the LAN simultaneously.
- Automatically appends a domain name to unqualified names.
- Allows new domain names to be added to the database using the MP-202's Web-based Management.
- Permits a computer to have multiple host names.
- Permits a host name to have multiple IPs (needed if a host has multiple network cards).

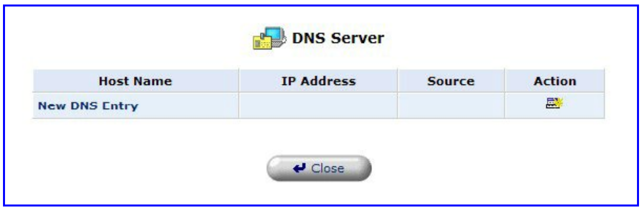
The DNS server does not require configuration. However, you may wish to view the list of computers known by the DNS, edit the host name or IP address of a computer on the list, or manually add a new computer to the list.

13.20.1 Viewing and Modifying the DNS Table

➢ To view the list of computers stored in the DNS table:

- Click the icon 'DNS Server' in the 'Advanced' screen of the Web-based Management; the DNS table is displayed (refer to the figure).

Figure 13-38: DNS Server



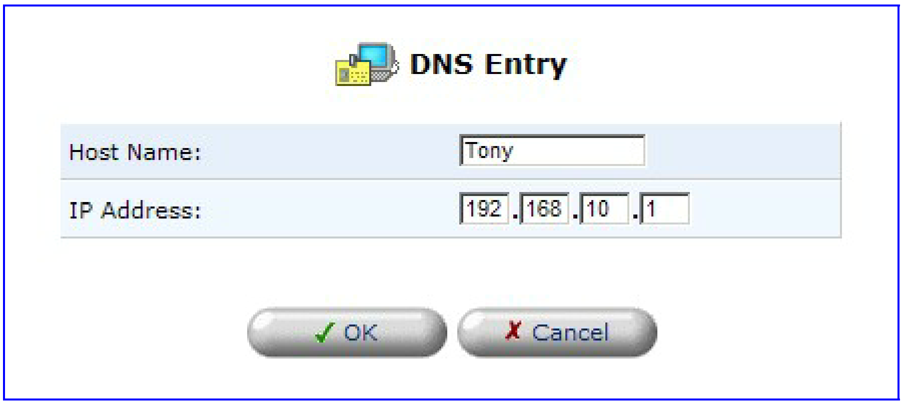
DNS Server

Host Name	IP Address	Source	Action
New DNS Entry			

➢ To add a new entry to the list:

1. Click the link 'New DNS Entry'; the 'DNS Entry' screen opens (refer to the figure).

Figure 13-39: DNS Entry



DNS Entry

Host Name:	Tony
IP Address:	192 . 168 . 10 . 1

2. Enter the computer's host name and IP address.
3. Click 'OK' to save your changes.

➢ To edit the host name or IP address of an entry:

1. Click the 'Edit' button under column 'Action'; the 'DNS Entry' screen opens.
2. If the host was manually added to the DNS Table, you can modify its host name and/or IP address. If it wasn't, you can only modify its host name.
3. Click 'OK' to save your changes.

➢ To remove a host from the DNS table:

- Click 'Delete' under column 'Action'; the entry is removed from the table.

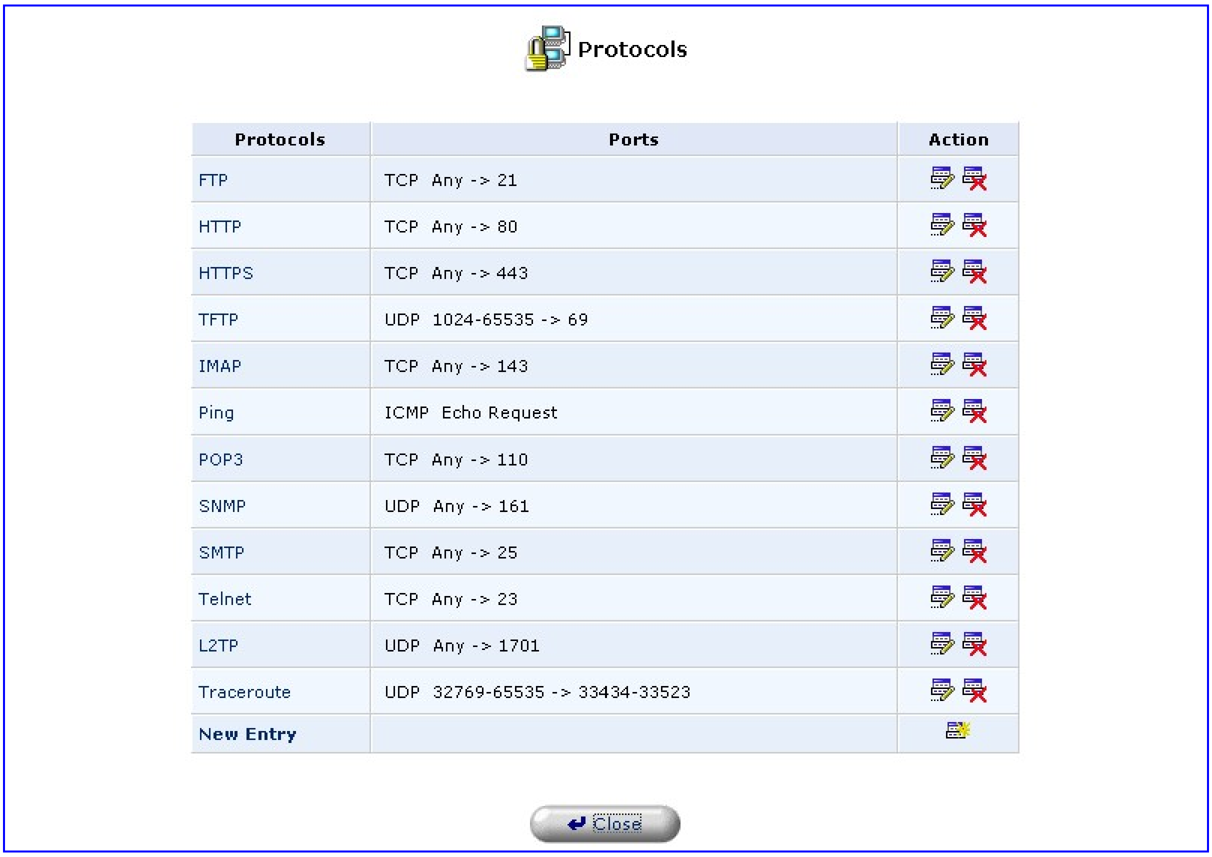
13.21 Protocols

The Protocols feature incorporates a list of preset and user-defined applications and common port settings. You can use protocols in various security features such as Access Control and Port Forwarding. You may add new protocols to support new applications or edit existing ones according to your needs.

➢ To define a protocol:

1. Click the Advanced icon on the side-bar.
2. Click the icon 'Protocols', the 'Protocols' screen appears (refer to the figure).

Figure 13-40: Advanced - Protocols

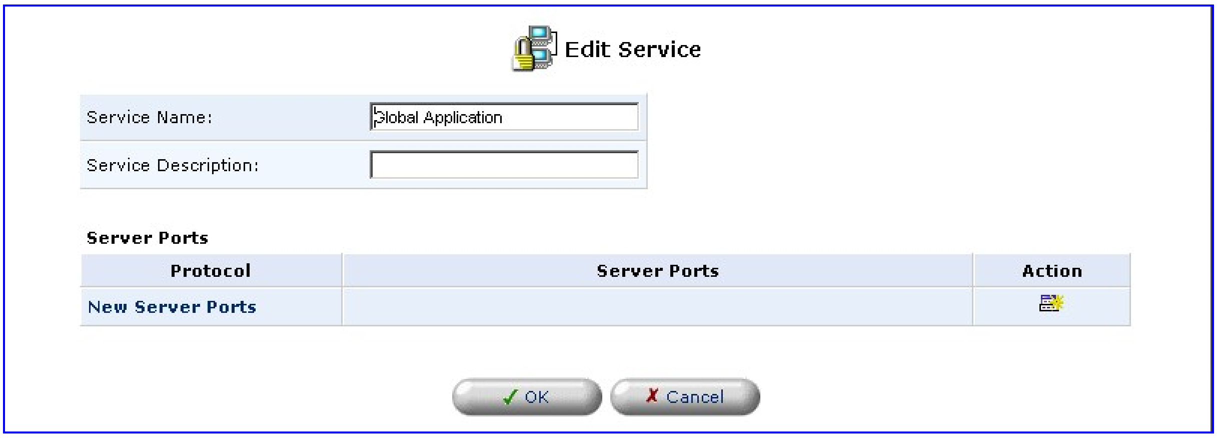


Protocols

Protocols	Ports	Action
FTP	TCP Any -> 21	
HTTP	TCP Any -> 80	
HTTPS	TCP Any -> 443	
TFTP	UDP 1024-65535 -> 69	
IMAP	TCP Any -> 143	
Ping	ICMP Echo Request	
POP3	TCP Any -> 110	
SNMP	UDP Any -> 161	
SMTP	TCP Any -> 25	
Telnet	TCP Any -> 23	
L2TP	UDP Any -> 1701	
Traceroute	UDP 32769-65535 -> 33434-33523	
New Entry		

3. Click the link 'New Entry'; the 'Edit Service' screen appears (refer to the figure).

Figure 13-41: Advanced - Protocols - Edit Service



Edit Service

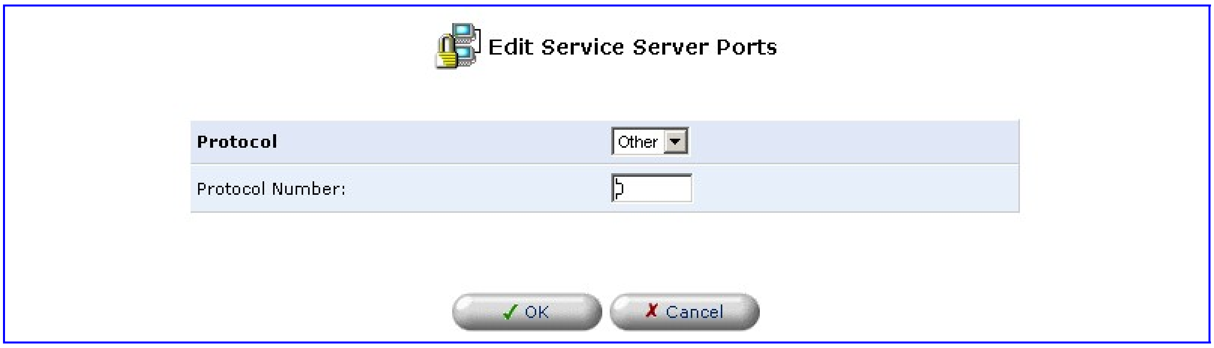
Service Name:	Global Application
Service Description:	

Server Ports

Protocol	Server Ports	Action
New Server Ports		

4. Name the service in the parameter 'Service Name' and click the link 'New Service Ports'; the 'Edit Service Server Ports' screen appears (refer to the figure).

Figure 13-42: Advanced - Protocols - Edit Service - Server Ports



Edit Service Server Ports

Protocol	Other
Protocol Number:	0

5. You may choose any of the protocols available in the combo box, or add a new one by selecting 'Other'. When selecting a protocol from the combo box, the screen refreshes, presenting the respective fields by which to enter the relevant information.

6. Select a protocol and enter the relevant information.

7. Click OK to save the settings.

Reader's Notes

14 System Monitoring

The System Monitoring screen displays important system information, including:

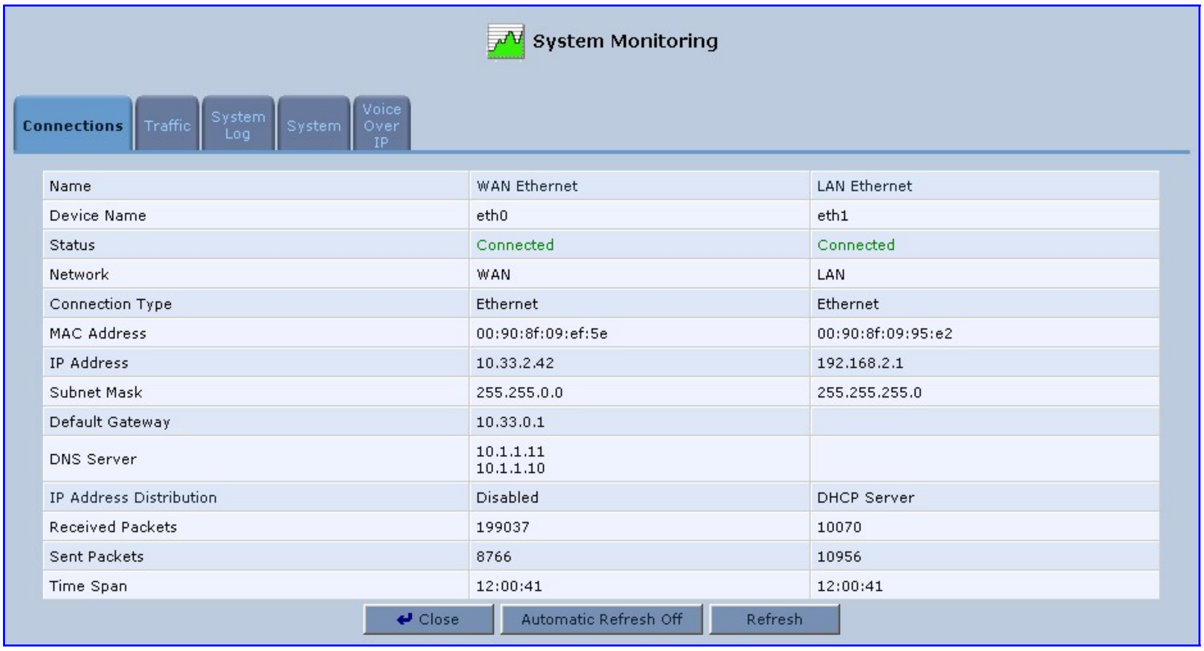
- Key network device parameters
- Network traffic statistics
- The system log
- The length of time that has transpired since the system was last started
- Voice over IP

14.1 Connections

➢ To monitor connections:

1. Click the menu 'System Monitoring' in the left sidebar; the 'System Monitoring' screen, tab 'Connections', is displayed, showing a read-only summary (with the exception of linked parameter 'IP Address Distribution') of the monitored connection data (refer to the figure).

Figure 14-1: System Monitoring - Connections



Name	WAN Ethernet	LAN Ethernet
Device Name	eth0	eth1
Status	Connected	Connected
Network	WAN	LAN
Connection Type	Ethernet	Ethernet
MAC Address	00:90:8f:09:ef:5e	00:90:8f:09:95:e2
IP Address	10.33.2.42	192.168.2.1
Subnet Mask	255.255.0.0	255.255.255.0
Default Gateway	10.33.0.1	
DNS Server	10.1.1.11 10.1.1.10	
IP Address Distribution	Disabled	DHCP Server
Received Packets	199037	10070
Sent Packets	8766	10956
Time Span	12:00:41	12:00:41

2. Click the 'Refresh' button to update the display, or press the 'Automatic Refresh On' button to constantly update the displayed parameters.

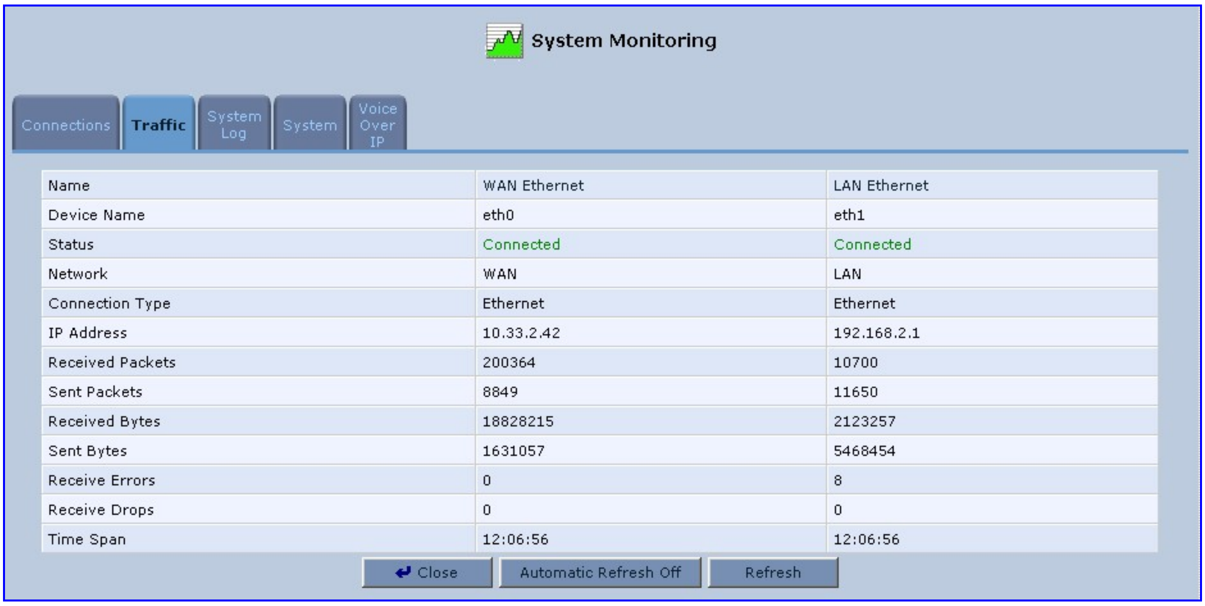
14.2 Traffic

The gateway is constantly monitoring traffic within the local network and between the local network and the Internet. You can view up-to-the-second statistical information about data received from and transmitted to the Internet (WAN) and about data received from and transmitted to computers in the local network (LAN).

➢ To view traffic statistics:

- Click tab 'Traffic'; the 'System Monitoring - Traffic' screen opens.

Figure 14-2: System Monitoring - Traffic



Name	WAN Ethernet	LAN Ethernet
Device Name	eth0	eth1
Status	Connected	Connected
Network	WAN	LAN
Connection Type	Ethernet	Ethernet
IP Address	10.33.2.42	192.168.2.1
Received Packets	200364	10700
Sent Packets	8849	11650
Received Bytes	18828215	2123257
Sent Bytes	1631057	5468454
Receive Errors	0	8
Receive Drops	0	0
Time Span	12:06:56	12:06:56

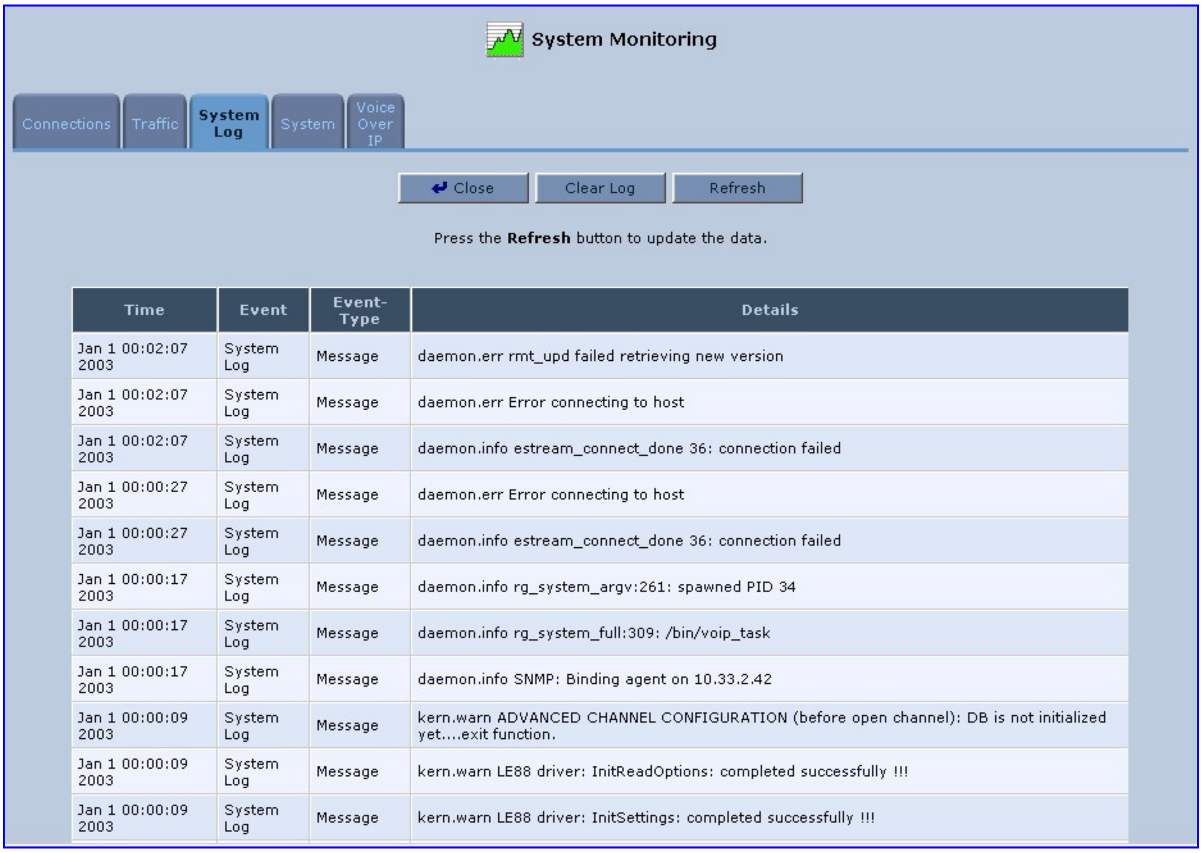
14.3 System Log

The System Log displays a list of the most recent activity that has taken place on the gateway.

➢ To open the system log:

- Click tab 'System Log'; the 'System Monitoring - System Log' screen opens.

Figure 14-3: System Monitoring - System Log



Press the **Refresh** button to update the data.

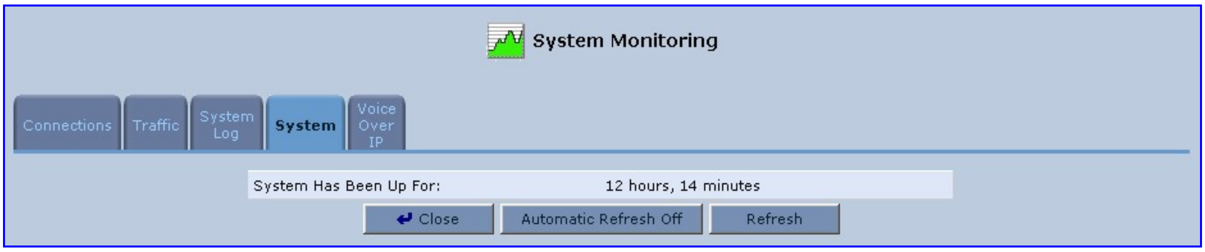
Time	Event	Event-Type	Details
Jan 1 00:02:07 2003	System Log	Message	daemon.err rmt_upd failed retrieving new version
Jan 1 00:02:07 2003	System Log	Message	daemon.err Error connecting to host
Jan 1 00:02:07 2003	System Log	Message	daemon.info estream_connect_done 36: connection failed
Jan 1 00:00:27 2003	System Log	Message	daemon.err Error connecting to host
Jan 1 00:00:27 2003	System Log	Message	daemon.info estream_connect_done 36: connection failed
Jan 1 00:00:17 2003	System Log	Message	daemon.info rg_system_argv:261: spawned PID 34
Jan 1 00:00:17 2003	System Log	Message	daemon.info rg_system_full:309: /bin/voip_task
Jan 1 00:00:17 2003	System Log	Message	daemon.info SNMP: Binding agent on 10.33.2.42
Jan 1 00:00:09 2003	System Log	Message	kern.warn ADVANCED CHANNEL CONFIGURATION (before open channel): DB is not initialized yet....exit function.
Jan 1 00:00:09 2003	System Log	Message	kern.warn LE88 driver: InitReadOptions: completed successfully !!!
Jan 1 00:00:09 2003	System Log	Message	kern.warn LE88 driver: InitSettings: completed successfully !!!

14.4 System Up Time

➢ To display the system up time:

- Press tab 'System' to display the length of time that has passed since the system was last started.

Figure 14-4: System Monitoring - System Up Time



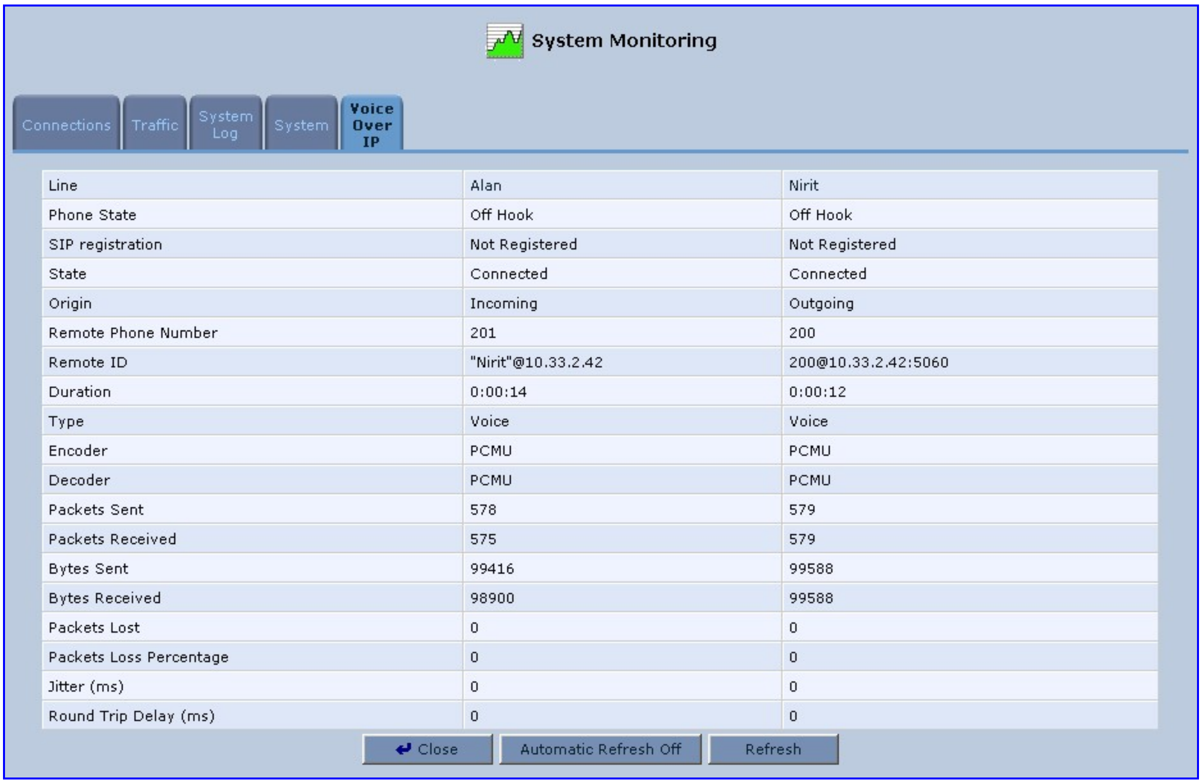
System Has Been Up For: 12 hours, 14 minutes

14.5 Voice over IP

➢ To monitor VoIP:

- Click tab 'Voice over IP'; the 'System Monitoring - Voice over IP' screen opens showing read-only VoIP call related parameters.

Figure 14-5: Advanced - System Monitoring - VoIP



Line	Alan	Nirit
Phone State	Off Hook	Off Hook
SIP registration	Not Registered	Not Registered
State	Connected	Connected
Origin	Incoming	Outgoing
Remote Phone Number	201	200
Remote ID	"Nirit"@10.33.2.42	200@10.33.2.42:5060
Duration	0:00:14	0:00:12
Type	Voice	Voice
Encoder	PCMU	PCMU
Decoder	PCMU	PCMU
Packets Sent	578	579
Packets Received	575	579
Bytes Sent	99416	99588
Bytes Received	98900	99588
Packets Lost	0	0
Packets Loss Percentage	0	0
Jitter (ms)	0	0
Round Trip Delay (ms)	0	0

15 Software and Hardware Specifications

Note: For the list of features available in the current software version, refer to the latest Release Notes.

Table 15-1: MP-202 Telephone Adapter Software Specifications

Feature	Details
VoIP Signaling Protocols	▪ SIP - RFC 3261, RFC 2327 (SDP)
Data Protocols	▪ IPv4, TCP, UDP, ICMP, ARP,TLS (SIP Over TLS) ▪ PPPoE (RFC 2516) ▪ L2TP (RFC 2661) ▪ PPTP (RFC 2637) ▪ DNS, Dynamic DNS ▪ WAN to LAN Layer 3 routing with: ✓ DHCP Client/Server (RFC 2132) ✓ NAT: RFC 3022, Application Layer Gateway (ALG) ✓ Stateful Packet Inspection Firewall ✓ QoS: Priority queues, VLAN 802.1p,Q tagging, traffic shaping or ▪ Layer 2 switching (currently not supported) ▪ STUN (RFC 3489)
Media Processing	▪ Voice Coders: G.711, G.723.1, G.729A/B, G.726 Optional - iLBC, AMR (separate software image) ▪ Echo Cancelation: G.168-2004 compliant, 64 msec tail length ▪ Silence Compression ▪ Adaptive Jitter Buffer 300 msec ▪ Fax bypass, Voice-Band Data and T.38 fax relay ▪ Automatic Gain Control
Telephony Features	▪ Call Hold and Transfer ▪ Call Waiting ▪ 3-Way Conferencing ▪ Message Waiting Indication ▪ Call Forward
Configuration/ Management	▪ Embedded Web Server for configuration and management ▪ TR-069 and TR-104 for remote configuration and management ▪ Remote firmware upgrade and configuration by HTTP ▪ SIP-triggered remote firmware and configuration upgrade ▪ Command-Line Interface (CLI) over Telnet
Packetization	▪ RTP/RTCP Packetization (RFC 3550, RFC 3551) ▪ DTMF Relay (RFC 2833)

Feature	Details
Security	▪ HTTPs for Web-based configuration ▪ Password protected Web pages (MD5)
Telephony Signaling	▪ In-band: ✓ DTMF: Detection and Generation, TIA464B ✓ Caller ID: Telcordia, ETSI, NTT - Type I, Telcordia Type II ✓ Call Progress Tones ▪ Out-of-band: ✓ FXS Loop-start ✓ On/Off Hook, Flash Hook ✓ Polarity reversal

Table 15-2: MP-202 Telephone Adapter Hardware Specifications

Power	+12VDC
Interfaces	RJ-45 - 10/100 Base-T for LAN RJ-45 - 10/100 Base-T for WAN 2xRJ-11 - 2 FXS lines for telephones (POTS)
LED Indications	LAN activity on Ethernet Port Power on Phone 1 and Phone 2 - Registered, In Use, Alert
SLIC characteristics	Maximum Ringer Load (REN) - 5 Short Haul Ringer Voltage - up to 65Vrms Configurable Terminating Impedance