AudioCodes CPE & Access Gateway Products

MP-20x series

MediaPack™ Series Telephone Adapters with Integrated Router

User's Manual

MP-20x Telephone Adapter

Version 3.0.1

Document #: LTRT-50609

AudioCodes

Contents

List of Figures

List of Tables

Reader’s Notes

Trademarks

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-20x Telephone Adapter.

Regulatory Information

The Regulatory Information can be viewed at http://www.audiocodes.com/downloads.

Related Documentation

Document Name
MP-20x Telephone Adapter Release Notes
MP-202C Broadband VoIP Gateway & Wireless Router Quick Guide
MP-20x FXS-FXO Telephone Adapter Quick Installation Guide
MP-20x FXS Telephone Adapter Quick Installation Guide
MP-202 Advanced Configuration and Management Features Application Note
MP-20x Debugging and Diagnostic Tools Application Note
MP-20x FXO Interface Application Note
MP-20x Redundant Proxy Application Note
MP-20x Recommended Network Topologies Application Note
MP-20x Web Access Protection Application Note
MP-20x Remote Management Application Note

Note: Open source software may have been added and/or amended for this product. For further information please visit our website at: http://audiocodes.com/support or contact your AudioCodes sales representative.

For Customers in Canada

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

The County Code Selection feature is disabled for products marketed in the US/Canada.

IC Radiation Exposure Statement

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

1 Introducing AudioCodes' MP-20x Telephone Adapter

AudioCodes MP-20x series of analog Telephone Adapters are cost-effective, feature-rich gateways, allowing the connection of ordinary POTS analog telephones or fax machines to a Voice-over-Broadband (VoBB) service provider.

The MP-20x series is designed for the rapidly growing residential and Small Office/Home Office (SOHO) voice-over-IP (VoIP) market. The MP-20x series typically connects to an existing Broadband Internet device (Cable, ADSL modem, or WiMAX wireless - depending on model), and establishes a communications path with the service provider network through its IP uplink connection. Supporting a rich set of subscriber calling features such as caller ID, call forwarding, and call waiting, the MP-20x series maintains a uniform user experience when migrating to VoIP services. In addition, the MP-20x series serves as a router with capabilities such as DHCP, NAT, Firewall, PPPoE, PPTP and L2TP, supporting connectivity of home PC networks.

The MP-20x VoIP Gateway is an all-in-one unit featuring (depending on model) a VoIP adapter, FXS lines, FXO interfaces, Ethernet LAN interfaces (with an internal Layer-2 switch), Ethernet WAN interface, and/or 802.11b/g Wireless LAN.

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 cutting-edge features for end users, such as T.38 Fax Relay and G.168-2004 compliant Echo Cancellation. Low bit rate vocoders (voice coders) can be used simultaneously on all the telephony ports to save valuable bandwidth.

The MP-20x is available in the following models:

Table 1-1: MP-20x Models

Model	FXS	FXO	WAN	LAN	WiFi
MP-201B/1FXS/SIP	1	-	1	1	-
MP-202B/2FXS/SIP	2	-	1	1	-
MP-203B/2FXS/1FXO/SIP[1]	2	1	1	1	**-**
MP-204B/4FXS/SIP	4	-	1	1	-
MP-202C-A	2	-	1	1	-
MP-202C-R	2	-	1	4	-
MP-202C-W	2	-	1	4	802.11b/g

[1] This model is currently not supported in this release.

Figure 1-1: Rear Panel of MP-20xB Models

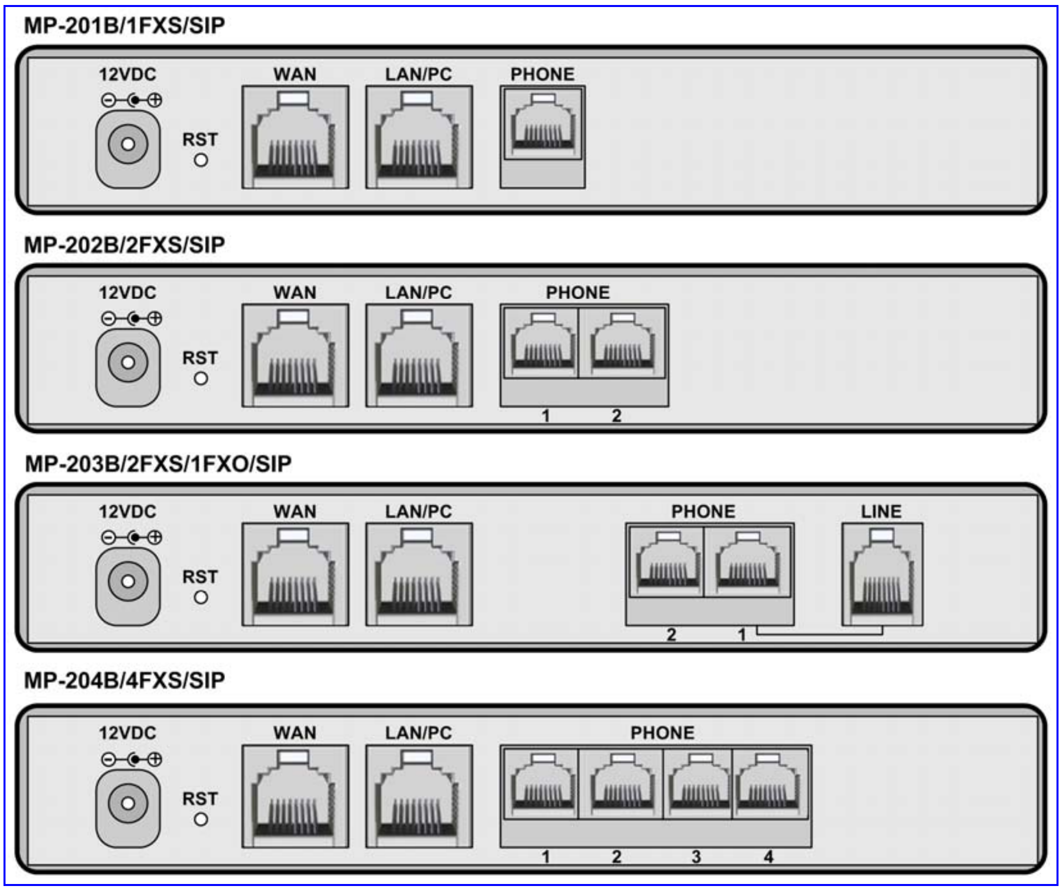
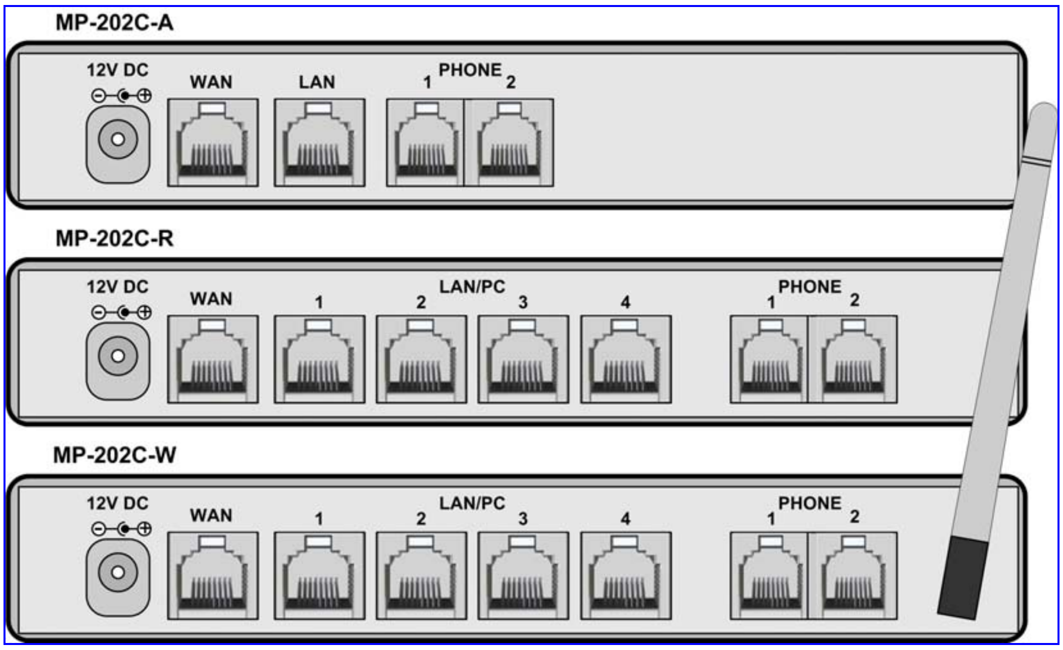


Figure 1-2: Rear Panel of MP-202C Models

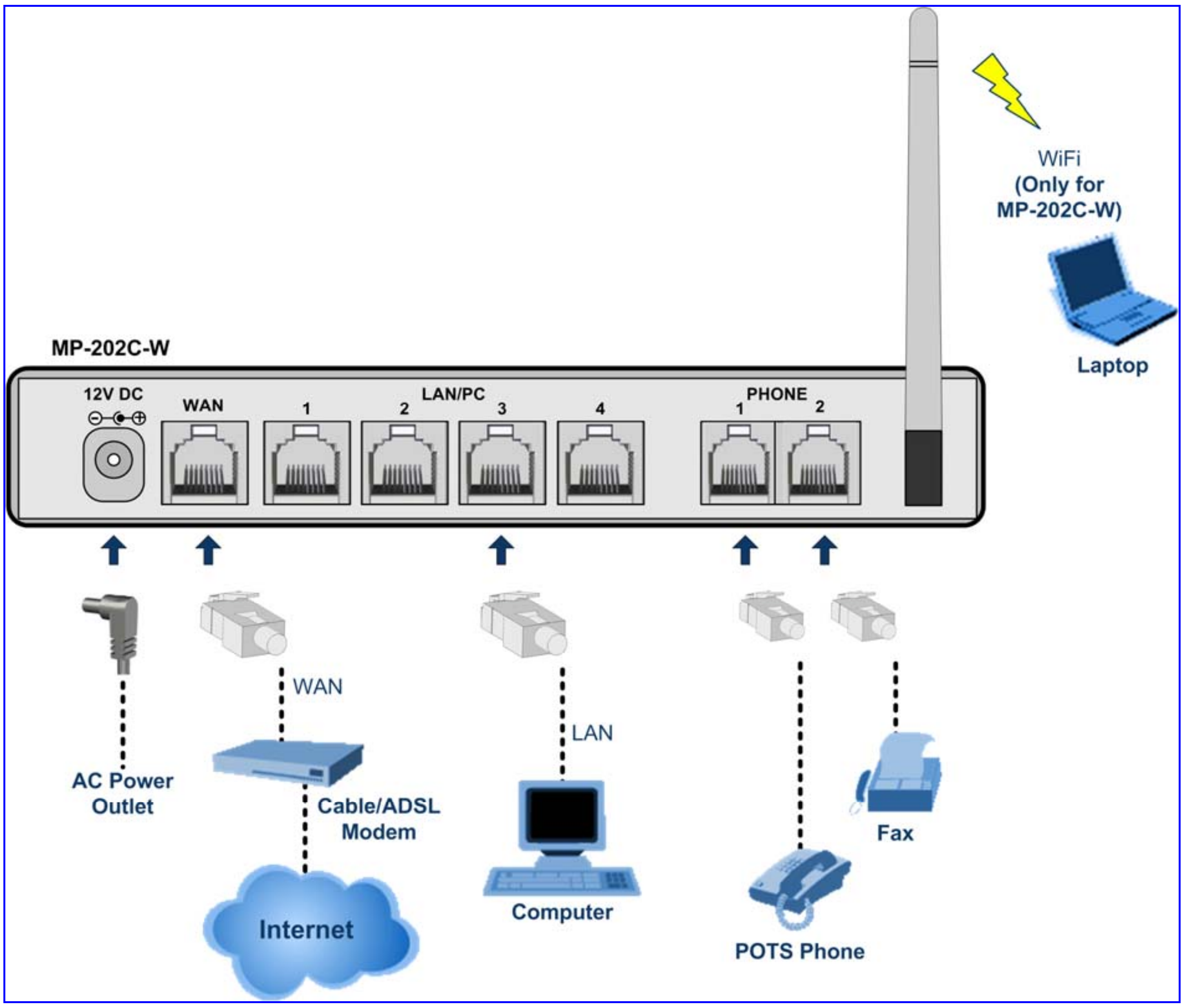


2 Cabling the MP-20x Telephone Adapter

➢ **To cable the MP-20x:**

1. Connect the MP-20x'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-20x's Ethernet 10/100 Base-T RJ-45 connector labeled **LAN/PC** to a computer.
3. Optionally, you can connect the MP-20x's connector labeled **LAN/PC** to a switch / hub and connect multiple PCs to the latter.
4. Connect the MP-20x's RJ-11 ports labeled **PHONE 1**, **PHONE 2** and so on (number of ports depends on model) to analog telephones.
5. Connect the power cable to the electrical outlet using the AC/DC power adapter; the **POWER** LED is lit (green) and when initialization completes (~ 1 minute), the **STATUS** LED changes from red to green.

Figure 2-1: Cabling the Device (Example using MP-202C-W)



MP-20x provides LEDs on the front panel for indicating various operating status, as described in the table below:

Table 2-1: MP-20x LEDs Description

LED	Color	State	Description
POWER	**Green**	On	Power received by MP-20x
	-	Off	MP-20x has been powered off
STATUS	**Green**	On	System start-up successful
	Red	On	Reboot (automatic, by default)
WAN	**Green**	On	WAN port is successfully connected
		Blinking	Data is being sent and received
	-	Off	Ethernet cable is not connected
LAN	**Green**	On	LAN port is in use
		Blinking	LAN port is sending or receiving data
	-	Off	Ethernet cable is not connected
WiFi	**Green**	On	WiFi is enabled and active
	-	Off	No WiFi activity **Note:** This LED is applicable only to MP-202C-W.
PHONE	**Green**	Type 1 Blinking	Idle Proxy register ok
		On	Off-hook
		Type 2 Blinking	Phone ringing
		Type 3 Blinking	Upgrade in process (all LEDs including STATUS LED)
	Red	On	Idle Proxy register failed
	-	Off	On-hook and not ringing, not using Proxy
LINE	**Green**	On	FXO line is in off-hook state
		Type 2 Blinking	FXO Line is ringing
	-	Off	FXO line in idle state

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 21)
2. Configure MP-20x's network connection (refer to 'Configuring the MP-20x's Network Connection' on page 24)

3.1 Defining Your PC's Network Connection

Refer to MP-20x Telephone Adapter Quick Installation Guide for instructions relating to installation on a Windows™ operating system.

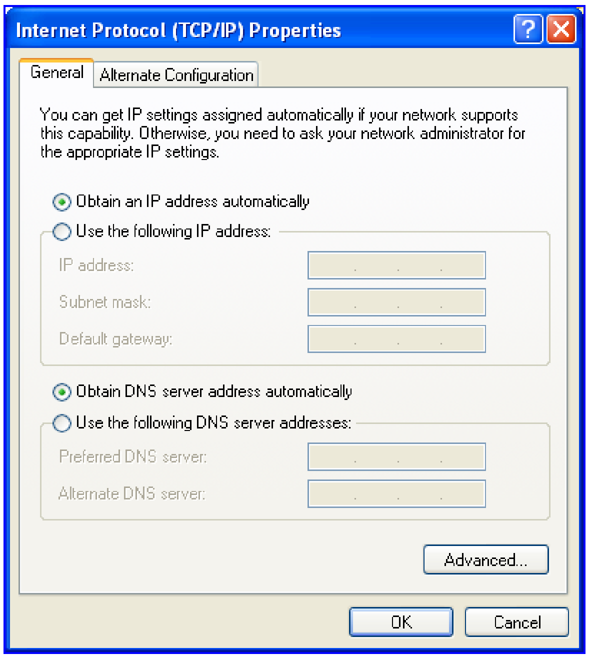
Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or should be instructed to automatically obtain an IP address using the Network DHCP server. MP-20x provides a DHCP server on its LAN and it is recommended to configure your PC to obtain 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 22
- Refer to 'Linux' on page 22

For connecting your PC to the MP-20x's wireless network, refer to 'Wireless LAN Connection' on page 22.

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

General | Alternate Configuration

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

➢ **To configure your PC running Windows XP for dynamic IP addressing:**

1. Access 'Network Connections' from the Control Panel.
2. Right-click the **Ethernet connection** icon, and select 'Properties'.
3. Under the **General** tab, select the 'Internet Protocol (TCP/IP)' component, and click the **Properties** button.
4. The 'Internet Protocol (TCP/IP)' properties window is 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

➢ **To configure your PC running Linux for dynamic IP addressing:**

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>.

3.1.3 Wireless LAN Connection

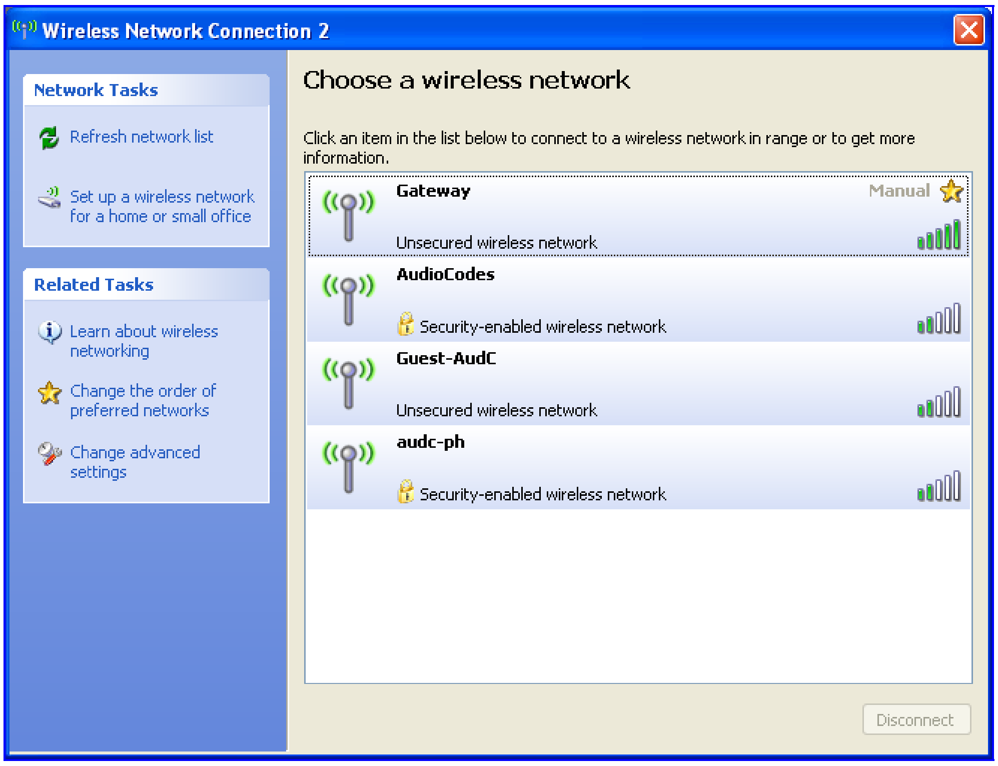
If your PC has wireless capabilities, Windows automatically recognizes this and creates a wireless connection for you. You can view this connection in the 'Network Connections' window.

Note: This section is based on PC's running Microsoft Windows XP Professional.

➢ To configure your PC for connecting to MP-20x's wireless connection:

1. From your Windows **Start** menu, point to **Settings**, **Control Panel**, **Network Connections**, and then choose **Wireless Connection**; Windows starts enabling the wireless connection.
2. On the Windows Taskbar, right-click the **Wireless Network Connection** icon, and then choose **View Available Wireless Connections**;

Figure 3-2: Available Wireless Networks


Wireless Network Connection 2
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Disconnect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Gateway — Manual — Unsecured wireless network

AudioCodes — Security-enabled wireless network

Guest-AudC — Unsecured wireless network

audc-ph — Security-enabled wireless network

3. Double-click MP-20x's wireless network name ("Gateway"); your computer establishes a connection with MP-20x, indicated by the display of "Connected". The Windows Taskbar displays the wireless connection.

3.2 Configuring the MP-20x's Network Connection

The Web-based management interface of MP-20x allows you to control the device's system parameters. The interface is accessed through a Web browser. For detailed information on MP-20x's Web-management interface, refer to 'Using the MP-20x's Web Interface' on page 33.

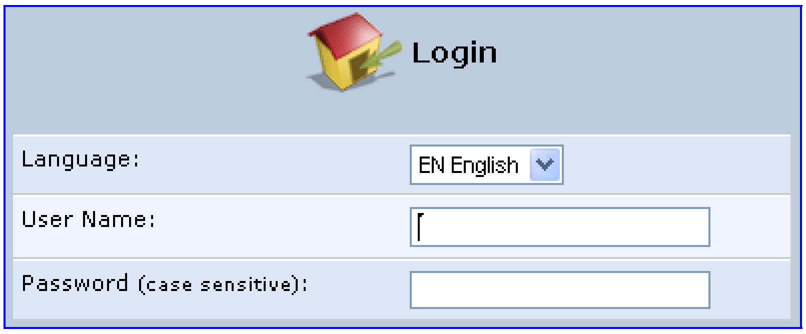
3.2.1 Logging in to MP-20x Web Interface

The procedure below describes how to login to MP-20x’s embedded Web interface.

➢ **To log in:**

1. Launch a Web browser on your PC.
2. With your PC connected directly to MP-20x, use URL *http*://mp20x.*home* to access the Web-based management interface; the ‘Login’ screen appears.

Figure 3-3: Logging In



Login

Language:	EN English
User Name:	
Password (case sensitive):	

3. In the 'User Name' field, enter your user name.
4. In the 'Password' field, enter your case-sensitive password.
5. Click **OK**; the 'Quick Setup' screen opens.

Notes:

- The default user name and password is "admin" (case-sensitive). However, it is recommended to define a new password after your first login session (refer to 'Configuring Users' on page 255).
- If there’s inactivity after logging in, a new login becomes necessary after a lapse of 15 minutes.

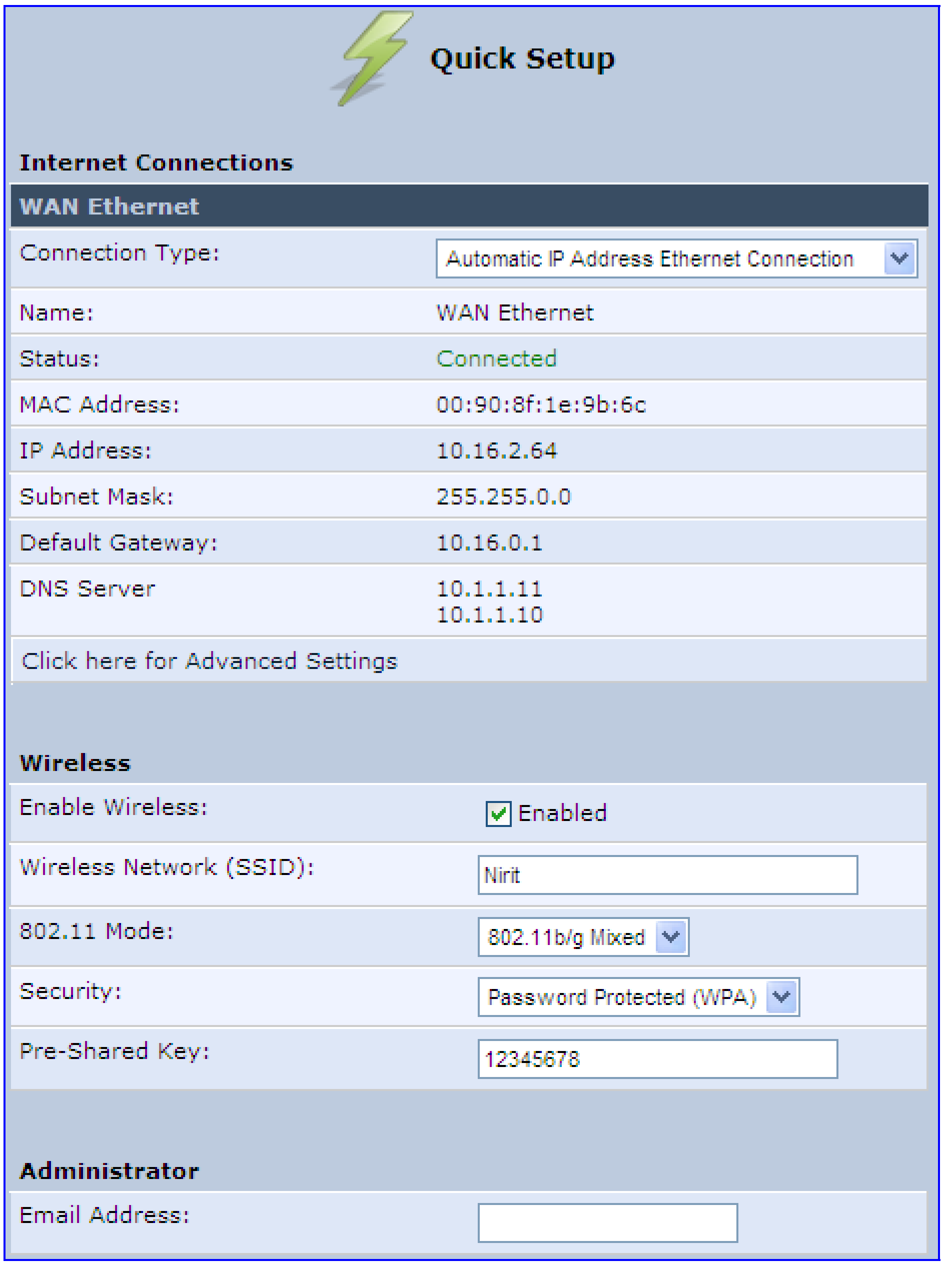
3.2.2 Configuring 'Quick Setup' Screen Parameters

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

➢ To access the 'Quick Setup' screen:

1. From the sidebar menu, click the **Quick Setup** menu; the 'Quick Setup' screen appear.

Figure 3-4: Quick Setup Screen



Quick Setup

Internet Connections

WAN Ethernet

Connection Type:	Automatic IP Address Ethernet Connection
Name:	WAN Ethernet
Status:	Connected
MAC Address:	00:90:8f:1e:9b:6c
IP Address:	10.16.2.64
Subnet Mask:	255.255.0.0
Default Gateway:	10.16.0.1
DNS Server	10.1.1.11 10.1.1.10

Click here for Advanced Settings

Wireless

Enable Wireless:	✓ Enabled
Wireless Network (SSID):	Nirit
802.11 Mode:	802.11b/g Mixed
Security:	Password Protected (WPA)
Pre-Shared Key:	12345678

Administrator

Email Address:	

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

In the 'Administrator' section of the 'Quick Setup' screen, specify the administrator's e-mail in the 'E-mail Address' field. System alerts and notifications are sent to this address.

3.2.2.1 Configuring Your Internet Connection

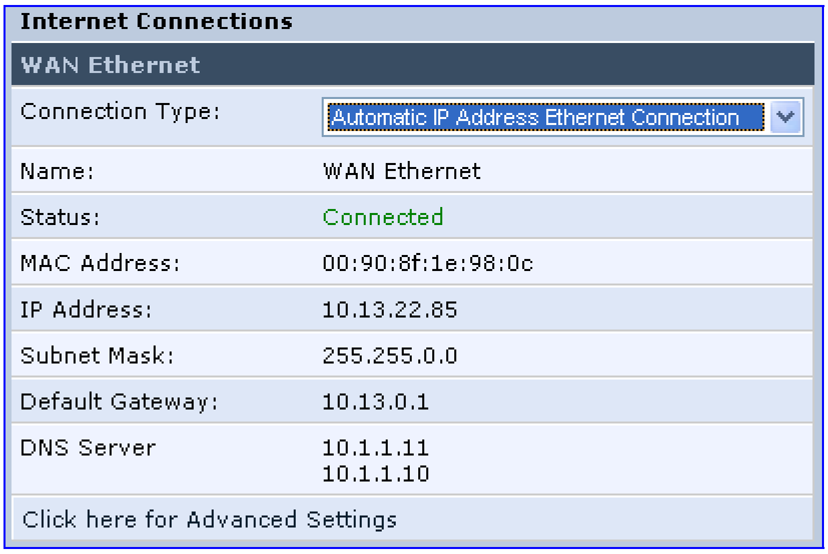
When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Technical information regarding the properties of your Internet connection should be provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether 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.

Note: MP-20x supports automatic detection of the user's Internet dialer type and allows you to ignore the settings in this subsection. For a detailed description of this feature, refer to “Configuring Automatic Internet Dialer Detection” on page 31.

3.2.2.1.1 Automatic IP Address Ethernet Connection

'Automatic IP Address Ethernet Connection' is the default connection type in the 'Connection Type' drop-down list.

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



Internet Connections

WAN Ethernet

Connection Type:	Automatic IP Address Ethernet Connection
Name:	WAN Ethernet
Status:	Connected
MAC Address:	00:90:8f:1e:98:0c
IP Address:	10.13.22.85
Subnet Mask:	255.255.0.0
Default Gateway:	10.13.0.1
DNS Server	10.1.1.11 10.1.1.10

Click here for Advanced Settings

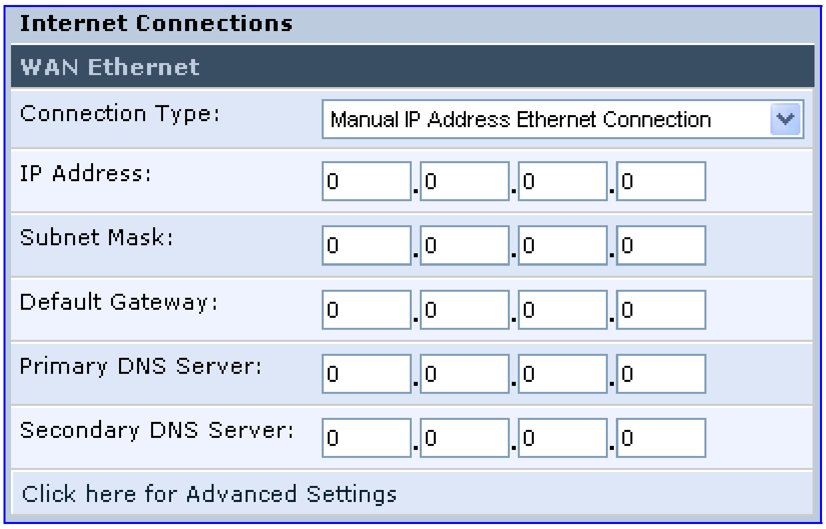
If left at the default, MP-20x obtains the WAN IP and DNS IP addresses from a DHCP server on the WAN.

3.2.2.1.2 Manual IP Address Ethernet Connection

➢ To configure manual IP address connection:

1. From the 'Connection Type' drop-down list, select 'Manual IP Address Ethernet Connection'.

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

Click here for Advanced Settings

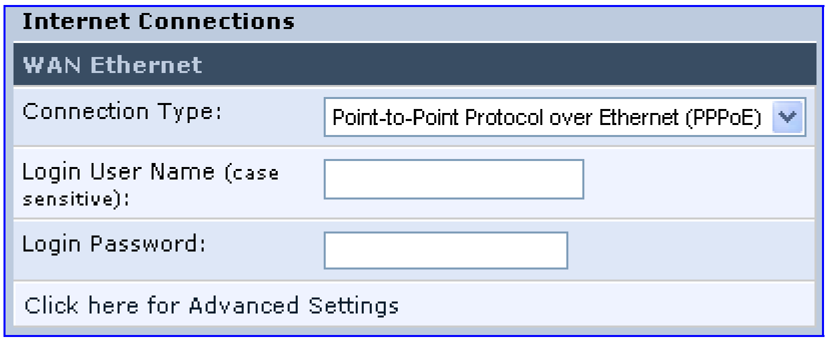
2. According to your ISP's instructions, specify the following parameters:
   - IP address
   - Subnet mask
   - Default device
   - Primary DNS server
   - Secondary DNS server

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

➢ **To configure PPPoE connection:**

1. From the 'Connection Type' drop-down list, select 'Point-to-point protocol over Ethernet (PPPoE)'.

Figure 3-7: Internet Connection - PPPoE


Internet Connections

WAN Ethernet

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

Click here for Advanced Settings

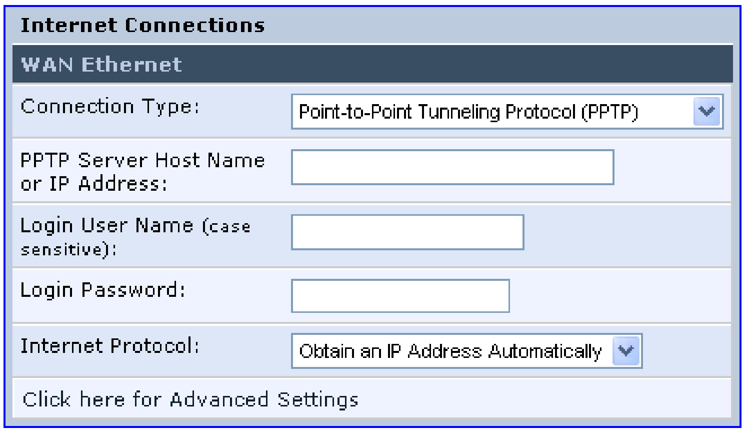
2. Your ISP should provide you with the following information:
   - Login user name
   - Login password

3.2.2.1.4 Point-to-Point Tunneling Protocol (PPTP)

➢ **To configure PPTP connection:**

1. From the 'Connection Type' drop-down list, select 'Point-to-Point Tunneling Protocol (PPTP)'.

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


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

Click here for Advanced Settings

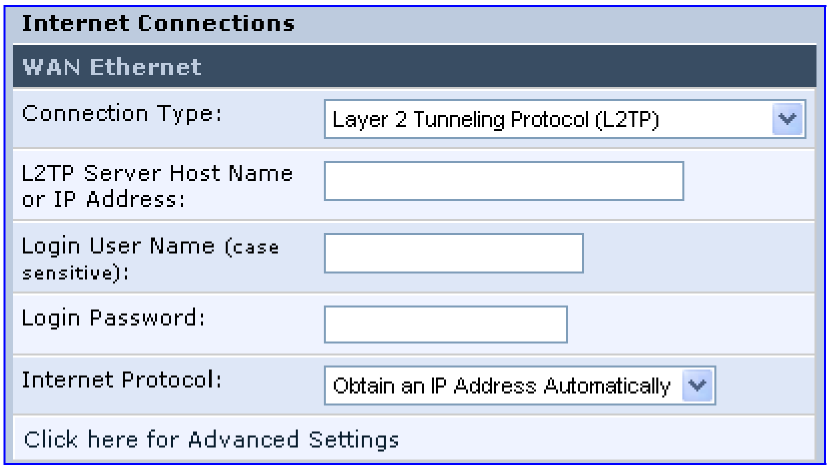
2. Your ISP should provide you with the following information:
   - PPTP Server Host Name or IP Address
   - Login user name
   - Login password

3.2.2.1.5 Layer 2 Tunneling Protocol (L2TP)

➢ **To configure L2TP connection:**

1. From the 'Connection Type' drop-down list, select 'Layer 2 Tunneling Protocol (L2TP)'.

Figure 3-9: Layer 2 Tunneling Protocol



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

Click here for Advanced Settings

2. Your ISP should provide you with the following information:
   - L2TP Server Host Name or IP Address
   - Login user name
   - Login password

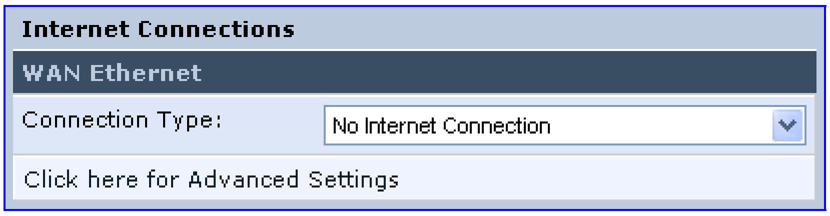
3.2.2.1.6 No Internet Connection

This option is if you do not have an Internet connection, or if you want to disable all existing connections.

➢ **To configure no Internet connection:**

- From the 'Connection Type' drop-down list, select 'No Internet Connection'.

Figure 3-10: Internet Connection - No Internet Connection



Internet Connections

WAN Ethernet

Connection Type:	No Internet Connection

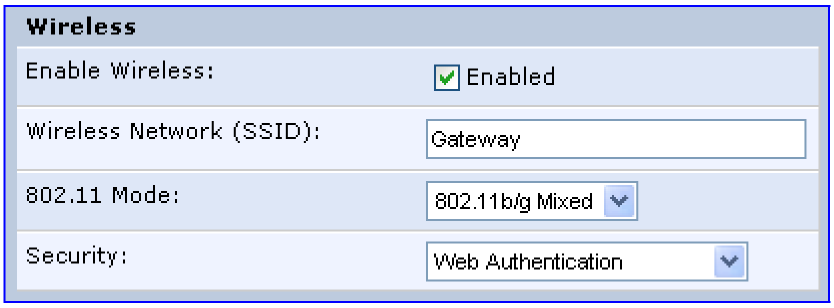
Click here for Advanced Settings

3.2.2.2 Enabling Wireless LAN Connection

The 'Quick Setup' screen allows you to quickly setup a LAN wireless connection.

➢ **To setup your wireless connection:**

1. From the sidebar menu, click the **Quick Setup** menu; the 'Quick Setup' screen appears.



Wireless

Enable Wireless:	✓ Enabled
Wireless Network (SSID):	Gateway
802.11 Mode:	802.11b/g Mixed
Security:	Web Authentication

2. Under the 'Wireless' section, perform the following:
   a. Select the 'Enable Wireless' check box to enable the LAN wireless connection.
   b. In the 'Wireless Network (SSID)' field, specify the wireless network's ID. The default SSID is 'Gateway'.

For a full description on configuring MP-20x's LAN wireless interface, refer to 'LAN Wireless Connection' on page 87.

3.2.3 Configuring Automatic Internet Dialer Detection

MP-20x supports the automatic detection of the user's Internet dialer type. This allows you to ignore the Internet connection settings required in Configuring Your Internet Connection. This support is customer ordered and pre-defined in the MP-20x factory settings. These factory settings are according to the ISP's Internet connection requirements (e.g., PPPoE user name and password), provided by the ISP for the parameters listed below.

Notes:

- Detection of the dialer type occurs only at initial power up (or after restoring to defaults).
- If the Automatic Dialer Detection feature is enabled, the remote configuration file mechanism only starts (immediately) once the automatic detection process is performed successfully.

The parameters and their values required (from the ISP) for the Automatic Internet Dialer Detection feature are shown below:

```
auto dialer detect/enabled=0
; where 0 = disabled and 1=enabled
auto dialer detect/done=1
; process completed successfully (1 = success and -1 = failed)
auto dialer detect/connection type/0 /Type= PPPOE
auto dialer detect/connection type/0/enabled=1
auto dialer detect/connection type/0/user name=xxx
; where xxx is the PPPoE username
auto dialer detect/connection type/0/password=xxx
; where xxx is the PPPoE password
auto dialer detect/connection type/1/type=L2TP
auto dialer detect/connection type/1/enabled=1
auto dialer detect/connection type/1/server ip=xxx.xxx.xxx.xxx
; where xxx.xxx.xxx.xxx is the L2TP IP address
auto dialer detect/connection type/1/username=xxx
; where xxx is the L2TP username
auto dialer detect/connection type/1/password=xxx
; where xxx is the L2TP password
auto dialer detect/connection type/2/type=DHCP
auto dialer detect/connection type/2/enabled=1
auto dialer detect/auto detect retries=x
; number of retires for the detection feature
auto dialer detect/ping retries=x
; number of pings to send for Internet connectivity check
auto dialer detect/ping retries timeout=x
; seconds to wait for ping response
auto dialer detect/max dialer conn time=x
; seconds to wait for a dialer to connect
```

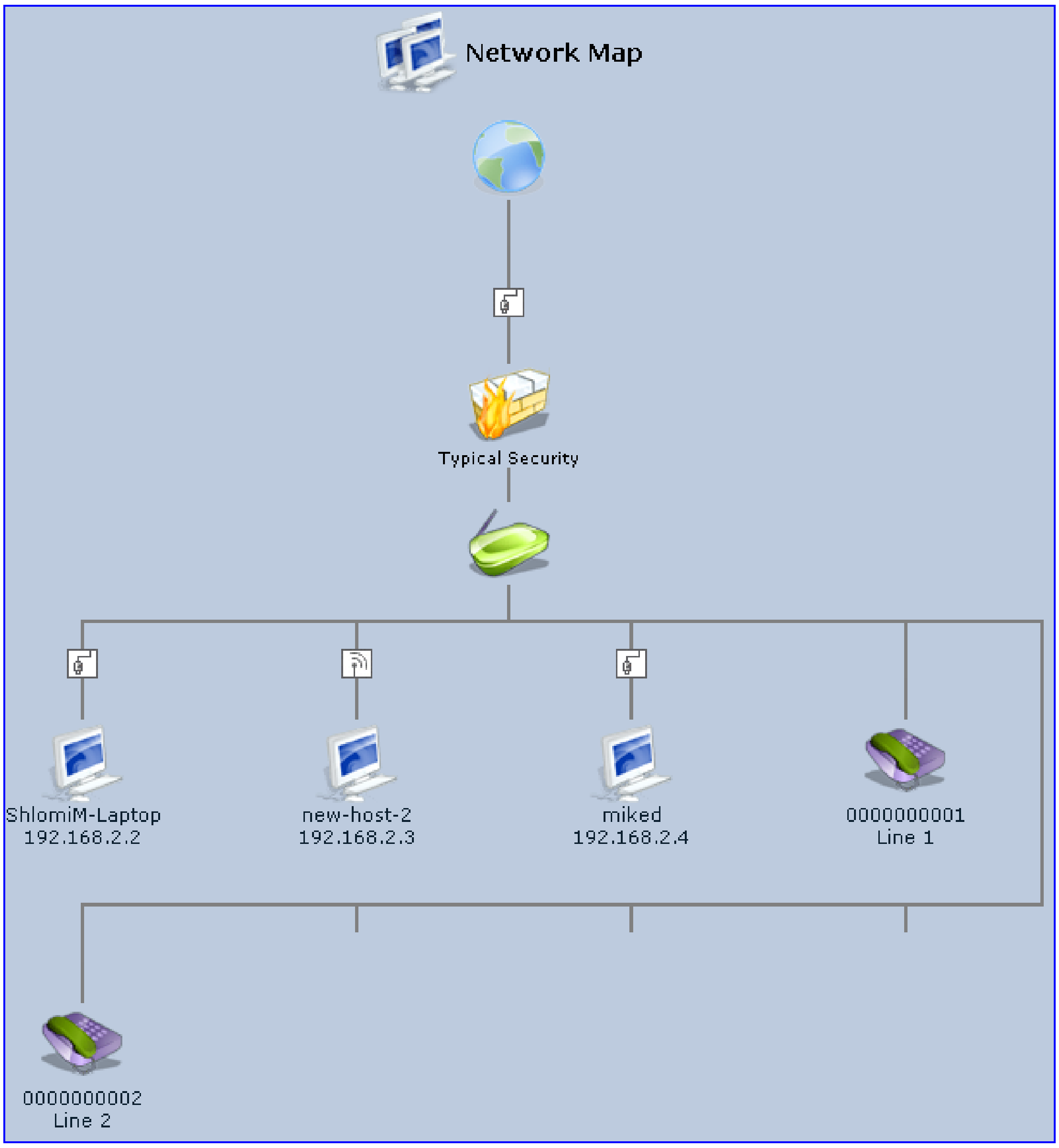
Reader’s Notes

4 Using the MP-20x's Web Interface

4.1 Your Home Network Map

After you log in to the Web-based management, the Network Map is displayed, as shown below.

Figure 4-1: Network Map



Note: The maximum number of displayed telephone lines depends on the MP-20x model (refer to 'Introducing AudioCodes' MP-20x Telephone Adapter' on page 17).

The network map depicts various network elements, from top to bottom:

1. External network interface (WAN Internet connection)
2. Firewall
3. MP-20x
4. Telephones, LAN network computers, and peripherals connected to MP-20x

The table below describes the different network map icons:

Table 4-1: Network Map Icons

Icon	Description
🌐	Represents the Internet. Clicking this icon redirects you to the 'Quick Setup' screen.
🔌	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 (yellow "bricks") corresponds to the security level currently selected: Minimum, Typical or Maximum. Click this icon to configure security settings.
📟	Represents the Telephone Adapter's model and displays the software version currently running on the device. Click this icon to access the 'Quick Setup' screen for performing basic device configuration.
☎	Represents an analog telephone connected to the device. Click this icon to configure the line settings.
🖥	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.
📶	Represents a Wi-Fi connection to connect to a LAN device (PC). Click this icon to configure the LAN wireless access properties for the device.
🔌	Represents an Ethernet Local Area Network (LAN) connection to a LAN device. Click this icon to configure network parameters for the Ethernet LAN device. If there is no connection to a connected PC, an "X" appears on the connecting line.
🔌	Represents a bridge connected in the home network. Click this icon to view the bridge's underlying devices.

4.2 Web Interface Menus

The Web-based management screens have been grouped into several subject areas and can be accessed by clicking the appropriate menu listed in the left sidebar.

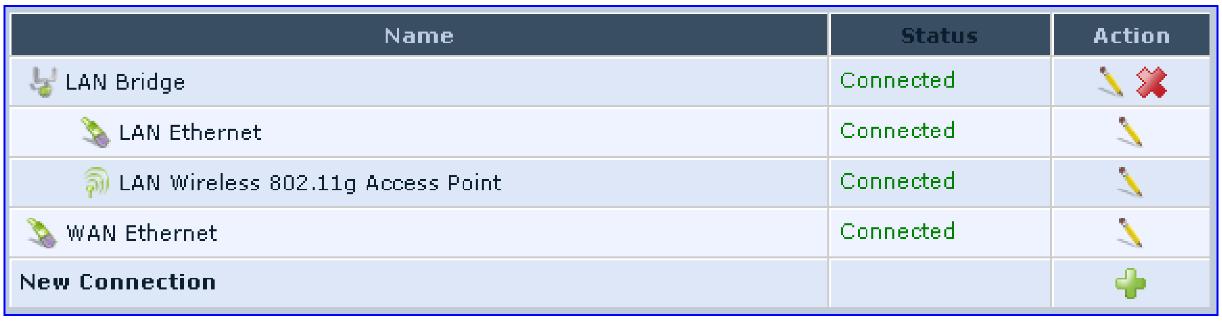
Table 4-2: Sidebar Menu Description

Menu	Description
Home	Displays the Network Map.
Quick Setup	Displays the 'Quick Setup' screen for quickly configuring your MP-20x.
Network Connections	Displays the 'Network Connections' screen for adding and configuring network connections.
Security	Displays the 'Security' screen for configuring MP-20x's Firewall and regulates communication between the Internet and the home network.
Voice over IP	Displays the 'Voice Over IP' screen for configuring the VoIP parameters to use MP-20x's VoIP to place and receive calls over the Internet using a standard telephone set.
QoS	Displays the 'Quality Of Service' screen for configuring Quality of Service (QoS) parameters for MP-20x.
Advanced	Displays the 'Advanced' screen for configuring system parameters (e.g., DHCP server and DNS) and performs administrative functions, including changing password, setting date and time and upgrading the system.
System Monitoring	Displays the 'System Monitoring' screen for viewing various status such as network status, traffic statistics, the system log and the VoIP status.
Logout	Logs off from MP-20x.

4.3 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 4-2: Typical Table Structure



Name	Status	Action
LAN Bridge	Connected	✎ ✖
LAN Ethernet	Connected	✎
LAN Wireless 802.11g Access Point	Connected	✎
WAN Ethernet	Connected	✎
New Connection		✚

The figure illustrates a typical table. Each row denotes an entry in the table. The table also provides 'Action' icons for performing various tasks, as described in the table below.

Table 4-3: Table Action Icons Description

Action Icon	Name	Description
✚	**Add**	Adds a row to the table.
✎	**Edit**	Edits a row in the table.
✖	**Delete**	Removes a row from the table.
💾	**Download**	Downloads a file to a folder on your computer.

5 Configuring VoIP Parameters

The VoIP parameters are configured in the 'Voice over IP' screen. This screen is opened by clicking the 'Voice over IP' link on the menu bar to the left; the Voice over IP' screen opens showing the tabs that allow:

- 'Configuring Signaling Protocol Parameters' on page 37
- 'Configuring Dialing Parameters' on page 43
- 'Configuring Media Streaming Parameters' on page 47
- 'Configuring Voice and Fax Parameters' on page 50
- 'Configuring Services Parameters' on page 54
- 'Configuring Line Settings' on page 56
- 'Configuring Speed Dial Settings' on page 59
- 'Configuring Telephone Interfaces' on page 62

Note: Clicking the button **Advanced** in the 'Voice Over IP' screens displays additional VoIP parameters for advanced configuration.

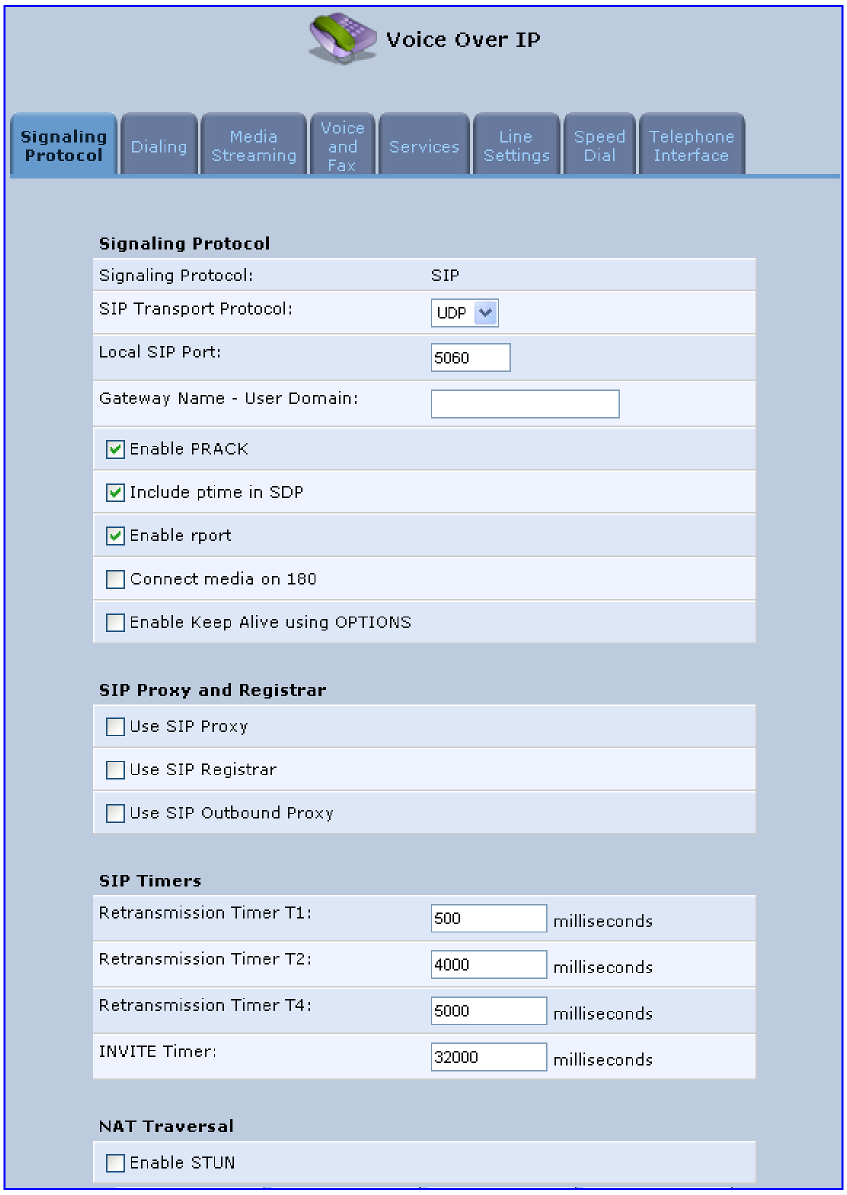
5.1 Configuring Signaling Protocol Parameters

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

➢ To configure signaling protocol parameters:

1. From the left sidebar, click the **Voice Over IP** menu; the 'Signaling Protocol' tab screen appears (by default).

Figure 5-1: VoIP - Signaling Protocol



Signaling Protocol

Signaling Protocol:	SIP
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

2. Configure the desired parameters according to the table below, and then click **OK**.

Table 5-1: Signaling Protocol Tab Parameters Description

Parameter	Description
Signaling Protocol	
Signaling Protocol	Signaling protocol running on the device. In the current version release, only SIP (Session Initiation Protocol) is supported.
SIP Transport Protocol	Choose either UDP (default) or TCP. **Note:** This parameter appears only in 'Advanced' mode.
Local SIP Port	The UDP/TCP port (default = 5060) on which the Stack listens. **Note:** This parameter appears only in 'Advanced' mode.
Gateway Name-User Domain	This domain name is sent in the From header of outgoing Invite messages. **Note:** This parameter appears only in 'Advanced' mode.
Enable PRACK	When enabled, MP-20x replies with a PRACK message upon receipt of a reliable provisional response. MP-20x does not initiate reliable provisional responses. **Note:** This parameter appears only in 'Advanced' mode.
Include ptime in SDP	When enabled, MP-20x adds the ptime field to the SDP message body. **Note:** This parameter appears only in 'Advanced' mode.
Enable rport	When enabled, MP-20x adds the rport parameter to the relevant SIP Message fields. **Note:** This parameter appears only in 'Advanced' mode.
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. **Note:** This parameter appears only in 'Advanced' mode.
Enable Keep Alive	When enabled, a keep-alive notification is sent every user-defined interval to the SIP registrar entity. **Note:** This parameter appears only in 'Advanced' mode.
Keep Alive Type	The type of keep-alive mechanism sent to the SIP registrar entity: • **Using SIP OPTIONS:** sends a SIP OPTIONS message • **Using an Empty UDP packet:** sends an empty UDP packet **Note:** This parameter appears only if “Enable Keep Alive" is selected.
Keep-Alive Period	Sets the periodic interval. **Note:** This parameter appears only if “Enable Keep Alive" is selected.
SIP Proxy and Registrar	
Use SIP Proxy	When checked, outgoing calls are 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 is also used as the registrar, allowing incoming calls.
Host Name or Address	The IP address or host name of the SIP proxy.

Parameter	Description
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.
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.
Register Expires	The registration timeout, in seconds.
Register Failed Expires	Periodic registration in case of a registration failure (e.g., due to a network problem).
SIP Security	MP-20x'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”. **Note:** This parameter appears only if the parameter 'SIP Security' is set to “Allow SIP traffic from Proxy and Additional SIP Entity”.
SIP Entity Address	The address of the additional SIP entity. **Note:** This parameter appears only if the parameter 'SIP Security' is set to “Allow SIP traffic from Proxy and Additional SIP Entity”.
Use Redundant Proxy	Check the box to use a redundant proxy.
Redundant Proxy Address	The IP address of the redundant proxy.
Redundant Proxy Port	The port of the redundant proxy.
Redundant Proxy Keep Alive Period	The interval between keep-alive packets (SIP OPTIONS) which are used by the proxy redundancy mechanism to check the connection status.
Switch back to Primary SIP proxy when available	When checked, the device switches back to the primary proxy server when communication with it is returned.
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. Note: This parameter appears only if Use SIP Registrar is selected.
Registrar Port	The UDP or TCP port of the registrar server. Note: This parameter appears only if Use SIP Registrar is selected.
Use SIP Outbound Proxy	Use an outbound SIP proxy (all SIP messages are sent to this server as the first hop). Default = unchecked. **Note:** This parameter appears only in 'Advanced' mode.
Outbound Proxy IP	The IP address of the outbound Proxy. If this parameter is set, all outgoing messages (including Registration messages) are sent to this Proxy according to the Stack behavior. **Note:** This parameter appears only if 'Use SIP Outbound Proxy' is selected.

Parameter	Description
Outbound Proxy Port	The Port on which the outbound Proxy listens. **Note:** This parameter appears only if 'Use SIP Outbound Proxy' is selected.
SIP Timers **Note:** This group appears only in 'Advanced' mode.	
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
NAT Traversal	
Enable STUN	When checked, the SIP STUN Manager starts. SIP STUN Manager resolves private addresses that need to be resolved to public addresses. **Note:** This parameter appears only in 'Advanced' mode.
STUN Server Address	The IP address of the STUN server used to resolve private addresses. **Note:** This parameter appears only if 'Enable STUN' is enabled.
STUN Server Port	The port of the STUN server. **Note:** This parameter appears only if 'Enable STUN' is enabled.
Subnet Mask	The subnet mask address of the STUN server used to resolve private addresses. **Note:** This parameter appears only if 'Enable STUN' is enabled.

5.1.1 Configuring Proxy Redundancy

The Redundant Proxy feature allows the configuration of a backup SIP proxy server to increase Quality of Service (QoS). Once this feature is enabled, MP-20x identifies cases where the primary proxy does not respond to SIP signaling messages. In these cases, MP-20x registers to the redundant proxy and seamlessly continues normal functionality, without any noticeable connectivity failure or malfunction with the primary proxy.

The Redundant Proxy feature includes two operational modes:

- **Asymmetric mode:** this mode assigns the primary proxy a higher priority for registration over the redundant proxy. Once MP-20x is registered to the primary proxy, it sends keep-alive messages (using SIP OPTIONS messages) to the primary proxy. If the primary proxy does not respond, MP-20x registers to the redundant proxy, but continues sending keep-alive messages to the primary proxy. If the primary proxy responds to these keep-alive messages, MP-20x re-registers to the primary proxy.
- **Symmetric mode:** in this mode, both proxies are assigned the same priority for registration. Once MP-20x is registered to a proxy (primary or redundant), it sends keep-alive messages to this proxy. MP-20x switches proxies only once the proxy to which it has registered does not respond.

In both modes, the following applies:

- If MP-20x is not registered (i.e., if the proxy server - redundant or primary - to which MP-20x currently tries to register does not respond), MP-20x attempts to register to an alternative proxy. These attempts continue until MP-20x successfully registers.
- If this feature is enabled and you reboot MP-20x, it registers to the last proxy to which it was trying to register (not necessarily to the primary proxy).

➢ To configure proxy redundancy:

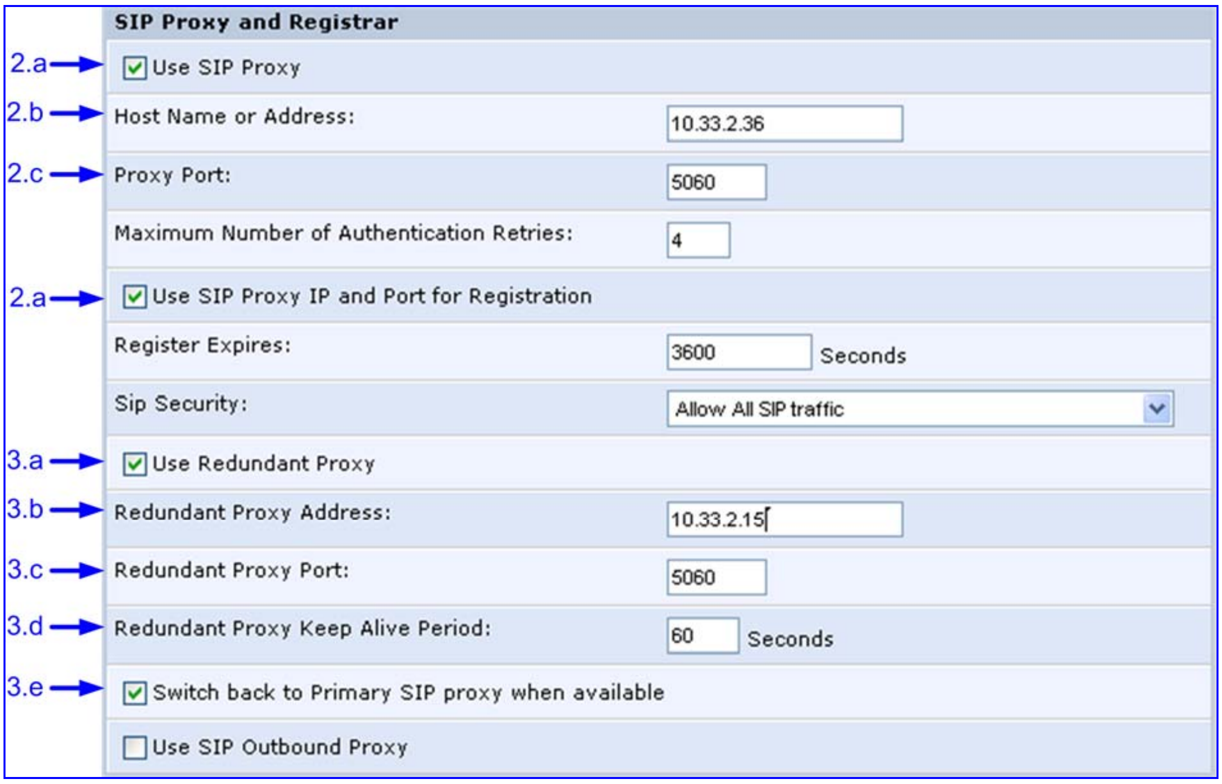
1. From the left sidebar, click the **Voice Over IP** menu; the 'Signaling Protocol' tab screen appears.
2. Define a primary proxy server, by performing the following:
   a. Under the group 'SIP Proxy and Registrar', select one of the following check boxes: 'Use SIP Registrar' or 'Use SIP Proxy IP and Port for SIP Proxy IP and Port for Registration'.
   b. In the 'Host Name or Address' field, enter the primary proxy's IP address.
   c. In the 'Proxy Port' field, enter the primary proxy's port number.
3. Define a redundancy proxy server, by performing the following:
   a. Under the group 'SIP Proxy and Registrar', select the 'Use Redundant Proxy' check box; additional fields relating to proxy redundancy appears.
   b. In the 'Redundant Proxy Address' field, enter the redundant proxy's IP address or DNS name.
   c. In the 'Redundant Proxy Port' field, enter the redundant proxy's port number.

d. In the 'Redundant Proxy Keep Alive Period' field, enter the rate (in seconds) of the keep-alive messages for sending to the proxy. The valid range is 10 to 86,400 seconds (i.e., 24 hours). The default value is 60 sec.

e. To toggle between Symmetric and Asymmetric modes, use the check box 'Switch back to Primary SIP proxy when available'.

- **Asymmetric mode** - select the check box (i.e., mark it)
- **Symmetric mode** - clear the check box

Figure 5-2: Configuring Proxy Redundancy



SIP Proxy and Registrar

2.a → [✓] Use SIP Proxy
2.b → Host Name or Address: 10.33.2.36
2.c → Proxy Port: 5060
Maximum Number of Authentication Retries: 4
2.a → [✓] Use SIP Proxy IP and Port for Registration
Register Expires: 3600 Seconds
Sip Security: Allow All SIP traffic
3.a → [✓] Use Redundant Proxy
3.b → Redundant Proxy Address: 10.33.2.15
3.c → Redundant Proxy Port: 5060
3.d → Redundant Proxy Keep Alive Period: 60 Seconds
3.e → [✓] Switch back to Primary SIP proxy when available
[ ] Use SIP Outbound Proxy

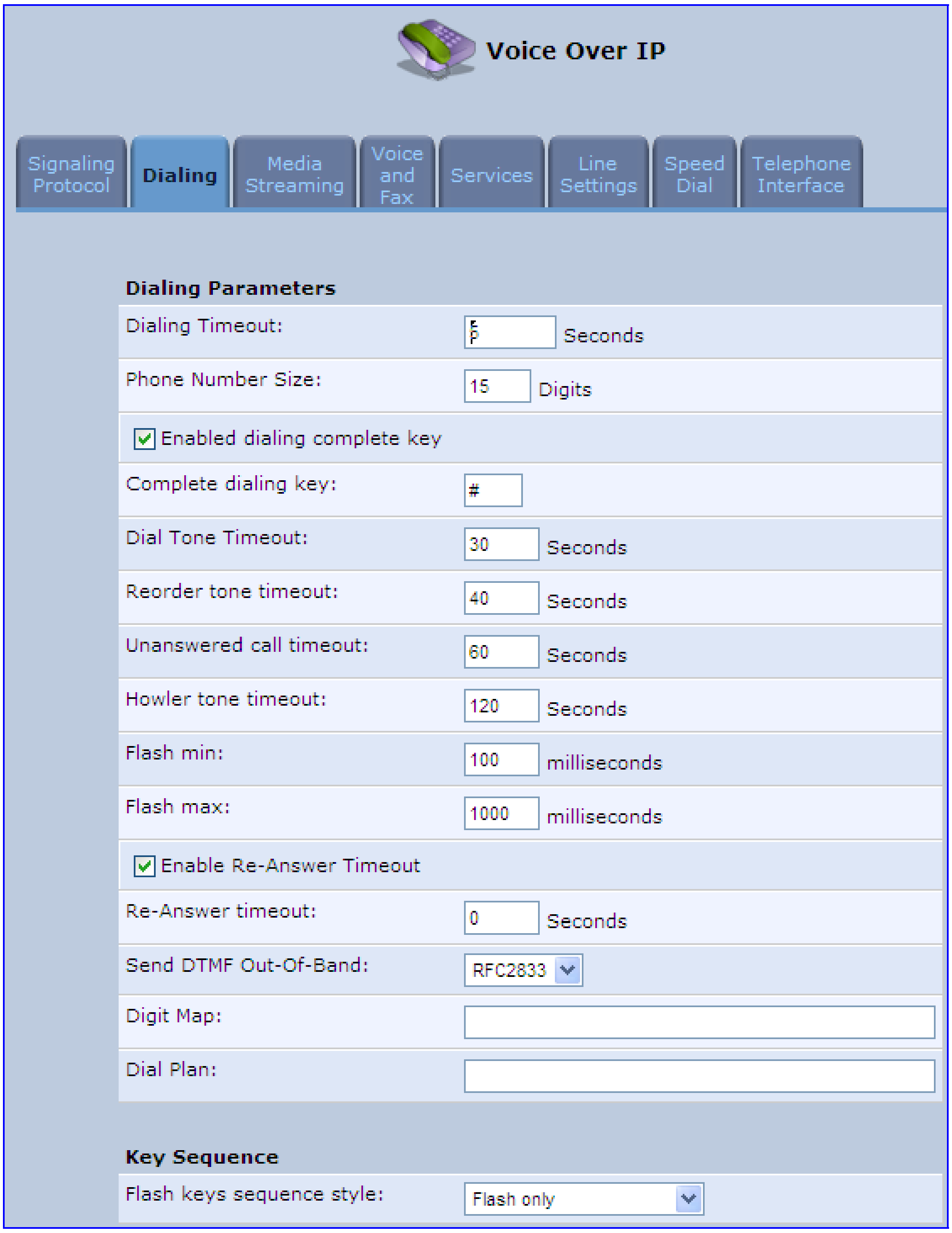
4. Click **OK** to save your settings.

5.2 Configuring Dialing Parameters

➢ **To configure Dialing parameters:**

- In the 'Voice Over IP' screen, click the **Dialing** tab; the basic 'Dialing' parameters screen opens. To view advanced parameters, click the **Advanced** button.

Figure 5-3: Voice Over IP - Dialing Screen



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
Flash min:	100 milliseconds
Flash max:	1000 milliseconds
✓ Enable Re-Answer Timeout	
Re-Answer timeout:	0 Seconds
Send DTMF Out-Of-Band:	RFC2833
Digit Map:	
Dial Plan:	

Key Sequence

Flash keys sequence style:	Flash only

Table 5-2: Dialing Tab Parameters Description

Parameter	Description
Dialing Parameters	
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).
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 MP-20x 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. **Note:** This parameter appears only in 'Advanced' mode.
Complete Dialing Key	Defines the Complete Dialing key. The default value is the pound (#) key. **Note:** This parameter appears only in 'Advanced' mode.
Dial Tone Timeout	The duration of the dial tone, in seconds. If the limit is exceeded, the dial tone stops and you hear a Reorder tone.
Reorder Tone Timeout	The duration (in seconds) of the Reorder tone. The Reorder tone is played for example, when MP-20x receives a 486 Response. If the limit is exceeded, the Reorder tone stops and a Howler tone is played to the user. **Note:** This parameter appears only in 'Advanced' mode.
Unanswered Call Timeout	Timeout before MP-20x automatically sends a Cancel message. When MP-20x makes a call and the other side doesn't answer, MP-20x sends a Cancel after this timeout. **Note:** This parameter appears only in 'Advanced' mode.
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. **Note:** This parameter appears only in 'Advanced' mode.
Flash min	The duration (in ms) after which you can begin to perform a Flash Hook.
Flash max	The maximum duration (in ms) the Flash Hook button can be pressed, after which the call is disconnected.
Enable Re-Answer Timeout	When enabled, the 'Re-Answer Timeout' field appears. The timeout after on-hooking an active call and then off-hooking it again. Once this time expires and the phone has not been off-hooked again, the call is disconnected.
Send DTMF Out-Of-Band	DTMFs are the tones generated by your telephone's keypad. Choose either Inband, RFC 2833, or Via SIP. **Note:** This parameter appears only in 'Advanced' mode.

Parameter	Description
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 is terminated after the third digit and so on. If the user dials a number that does not match any pattern, the number is terminated using the timeout or when the user presses the pound (‘#’) key. For an explanation on digit map syntax, refer to 'Syntax for Digit Maps and Dial Plans' on page 265. **Note:** This parameter appears only in 'Advanced' mode.
Dial Plan	Enables translation of specific patterns to specific SIP destination addresses. Rules are separated by the character ';'. An ‘x’ represents any dialed digit. Each backslash on the right of the ‘=’ sign represents one of the dialed digits. Example: '4xxx=Line_\\\@10.1.2.3' This rule issues a call to 10.1.2.3 with the SIP ID of Line_ followed by the last 3 digits of the dialed number. For dial plan syntax rules for patterns entered to the left of the '=' sign, refer to 'Syntax for Digit Maps and Dial Plans' on page 265. **Note:** This parameter appears only in 'Advanced' mode.
Key Sequence	
Flash keys sequence style	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’ = 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. ▪ 'Send Flash Hook Via SIP' = the user can modify the SIP INFO message that is sent upon Flash. The user can change the Content Type header field and Message Body field. **Note:** This parameter appears only in 'Advanced' mode.

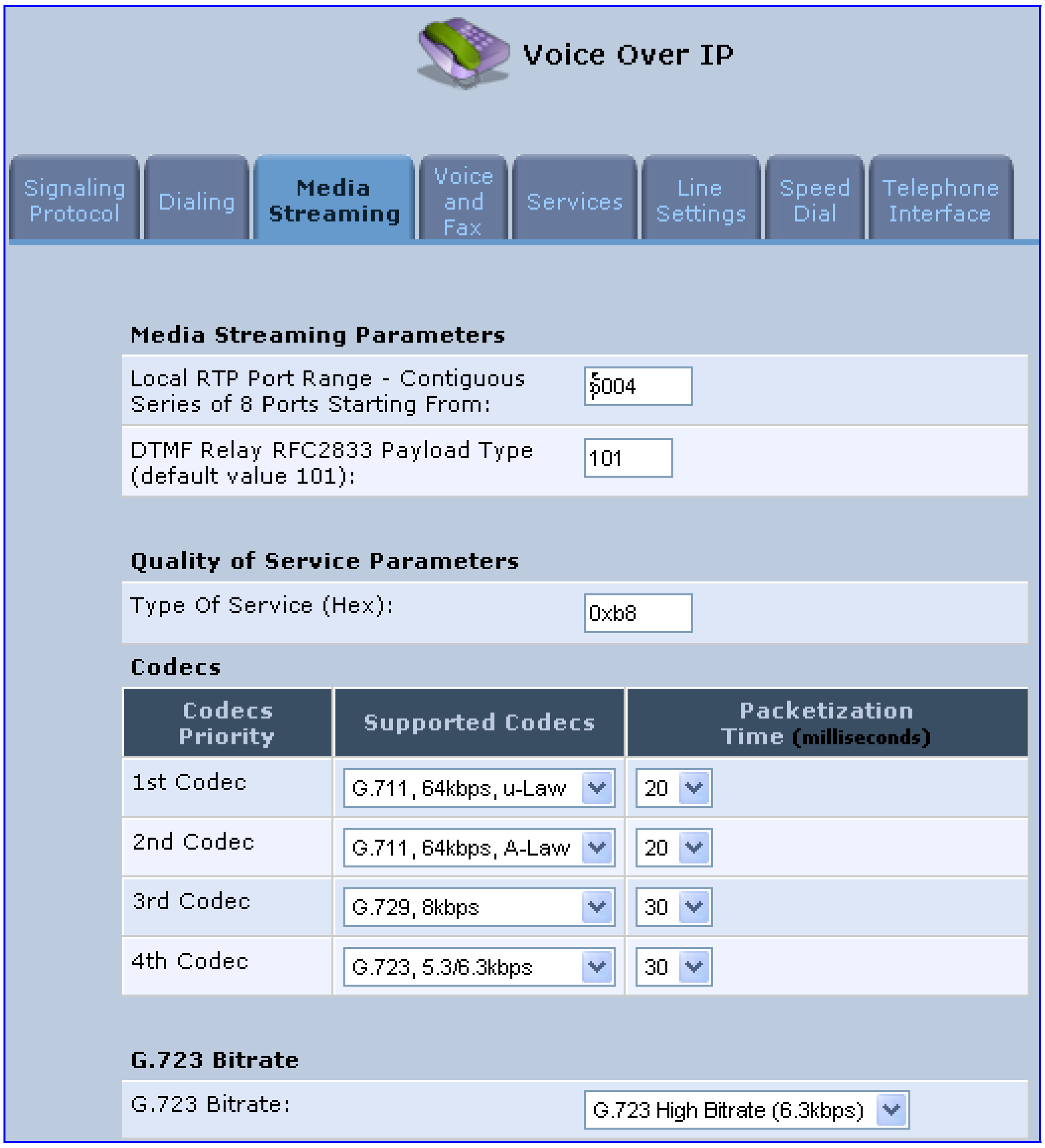
Parameter	Description
SIP INFO Header	When the key sequence is set to 'Send Flash Hook Via SIP', the user can modify the Content Type header field of the SIP INFO message. For example: "application/broadsoft; version = 1.0" **Note:** This parameter appears only when the 'Key Sequence' field is set to 'Send Flash Hook Via SIP'.
SIP INFO Body	When the key sequence is set to 'Send Flash Hook Via SIP', the user can modify the Message Body field of the SIP INFO message. For example: " event flashhook" **Note:** This parameter appears only when the 'Key Sequence' field is set to 'Send Flash Hook Via SIP'.

5.3 Configuring Media Streaming Parameters

➢ To configure media streaming parameters:

- In the 'Voice Over IP' screen, click the **Media Streaming** tab; the basic 'Media Streaming' parameters screen opens. To view advanced parameters, click the **Advanced** button.

Figure 5-4: VoIP - Media Streaming - Advanced



Media Streaming Parameters

Local RTP Port Range - Contiguous Series of 8 Ports Starting From:	5004
DTMF Relay RFC2833 Payload Type (default value 101):	101

Quality of Service Parameters

Type Of Service (Hex):	0xb8

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	30
4th Codec	G.723, 5.3/6.3kbps	30

G.723 Bitrate

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

Table 5-3: Media Streaming Tab Parameters Description

Parameter	Description
Codecs	
1st Codec	Refer to 'Configuring Codecs' on page 49
2nd Codec	Refer to 'Configuring Codecs' on page 49
3rd Codec	Refer to 'Configuring Codecs' on page 49
4th Codec	Refer to 'Configuring Codecs' on page 49
5th Codec	Refer to 'Configuring Codecs' on page 49
6th Codec	Refer to 'Configuring Codecs' on page 49
Media Streaming Parameters	
Local 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.
Quality of Service Parameters	
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 MP-20x. 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.
G.723 Bitrate	
G.723 Bitrate	Toggles between low and high bit rate for G.723.

5.3.1 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.

5.3.1.1 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 is to be used. The priority by which the codecs are compared is according to the descending order of their list. 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 fails. Note that if more than one codec is common to both parties, you cannot force which of the common codecs that were found are used by the remote party's client. If you do wish to force the use of a specific codec, leave only that codec checked.

5.3.1.2 Packetization Time

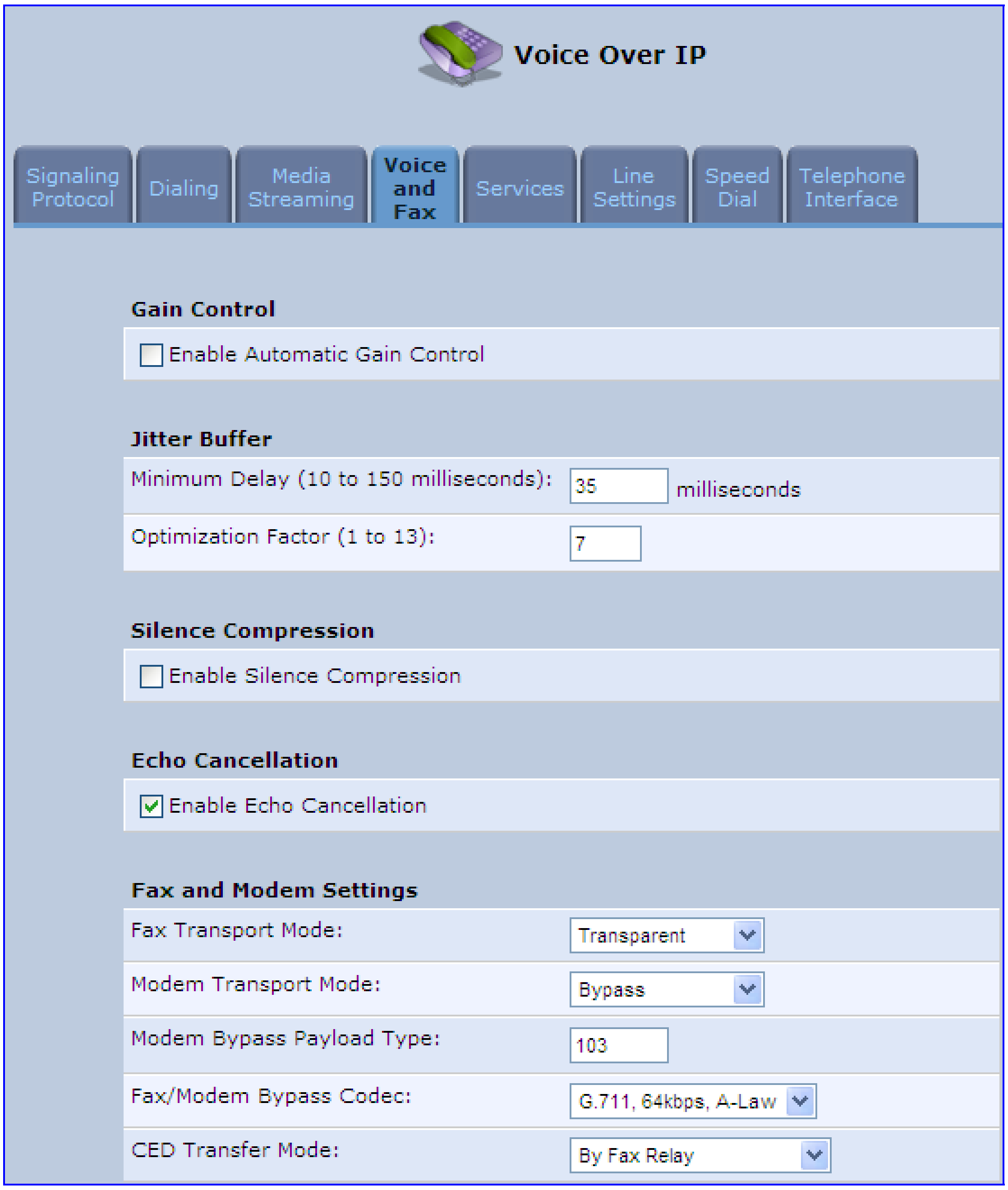
The Packetization Time is the length of the digital voice segment that each packet holds. The default is 20 millisecond packets. Selecting 10 millisecond packets reduces the delay but increases the bandwidth consumption.

5.4 Configuring Voice and Fax Parameters

➢ **To configure voice and fax parameters:**

- In the 'Voice Over IP' screen, click the **Voice and Fax** tab; the basic 'Voice and Fax' parameters screen opens. To view advanced parameters, click the **Advanced** button.

Figure 5-5: Voice Over IP - Voice and Fax Screen



Gain Control

☐ Enable Automatic Gain Control

Jitter Buffer

Minimum Delay (10 to 150 milliseconds): 35 milliseconds

Optimization Factor (1 to 13): 7

Silence Compression

☐ Enable Silence Compression

Echo Cancellation

☑ Enable Echo Cancellation

Fax and Modem Settings

Fax Transport Mode: Transparent

Modem Transport Mode: Bypass

Modem Bypass Payload Type: 103

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

CED Transfer Mode: By Fax Relay

Table 5-4: Voice and Fax Tab Parameters Description

Parameter	Description
Gain Control	
Enable Automatic Gain Control	When enabled (when the box is checked), the device adjusts 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.
Jitter Buffer	
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 milliseconds). Default = 35 msec.
Optimization Factor	The adaptation rate of the jitter buffer mechanism. Higher values cause the jitter buffer to respond faster to increased network jitter. Default = 7.
Silence Compression	
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.
Echo Cancellation	
Enable Echo Cancellation	Check to enable echo cancellation (disabling echo cancellation should be done for testing purposes only). Default = Enabled.
Fax and Modem Settings	
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). **Note:** This parameter appears only if 'Fax Transport Mode' is “T.38 Relay”.
Max Buffer	The maximum amount of T.38 data stored on the MP-20x DSP. The valid range is 128 to 2048. The default is 1024.
Max Datagram	The maximum total size of TCP/UDPTL packets that can be received at the remote gateway. The valid range is 160 to 1020. The default is 320.

Parameter	Description
Image Data Redundancy Level	The level for output Image Data (2400…14400 bps). ▪ 0 = No redundancy ▪ 1 to 3 = Redundancy level
T30 Control Data Redundancy Level	The redundancy level for output T.30 Control Data (300 bps). ▪ 0 = No redundancy ▪ 1 to 7 = Redundancy level
Fax Relay Jitter Buffer Delay	Configures the Fax Relay Jitter Buffer. ▪ 0 = Adaptive Jitter Buffer. The MP-20x DSP device sets the Jitter Buffer size automatically and then adapts it according to network conditions. ▪ 1 to 511 = Fixed Jitter Buffer size (in msec).
Error Correction Mode	Check to enable fax error correction mode (ECM). Default = Enabled. **Note:** This parameter appears only if 'Fax Transport Mode' is "T.38 Relay".
Fax Bypass Payload Type	Defines the payload type for fax in Bypass mode. **Note:** This parameter appears only if 'Fax Transport Mode' is "Bypass".
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. Voice Band Data = Switch to G.711 via SIP messaging. Bypass = An automatic switch to AudioCodes' proprietary payload type (102, 103). **Note:** If the Fax transport mode is Bypass or VBD, it must match the Modem transport mode.
Modem Bypass Payload Type	Defines the payload type for modems in Bypass mode. **Note:** This parameter appears only if 'Modem Transport Mode' is "Bypass".
Fax/Modem Bypass Codec	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
CED Transfer Mode	▪ By Fax Relay: When the MP-20x is the receiver side, Switch to Fax relay is enabled upon CED. This allows a high reliable Fax-over-IP call establishment at the beginning of CED tone. ▪ In Voice Or PCM Bypass: When the MP-20x is the receiver side, to avoid possible conflicts with low-speed modems, the CED (ANS) relay by FoIP protocol may be disabled by setting the CED transfer mode to 'In Voice Or PCM Bypass'. In this case, the MP-20x does not initiate the Fax Relay on detecting CED tone in absence of CNG, but switches to VBD or remains in voice mode (depends on the Modem Transport Mode). The MP-20x switches to FoIP later when it defines exactly that a monitored call is the fax call (CED and CND or V.21 Preamble).

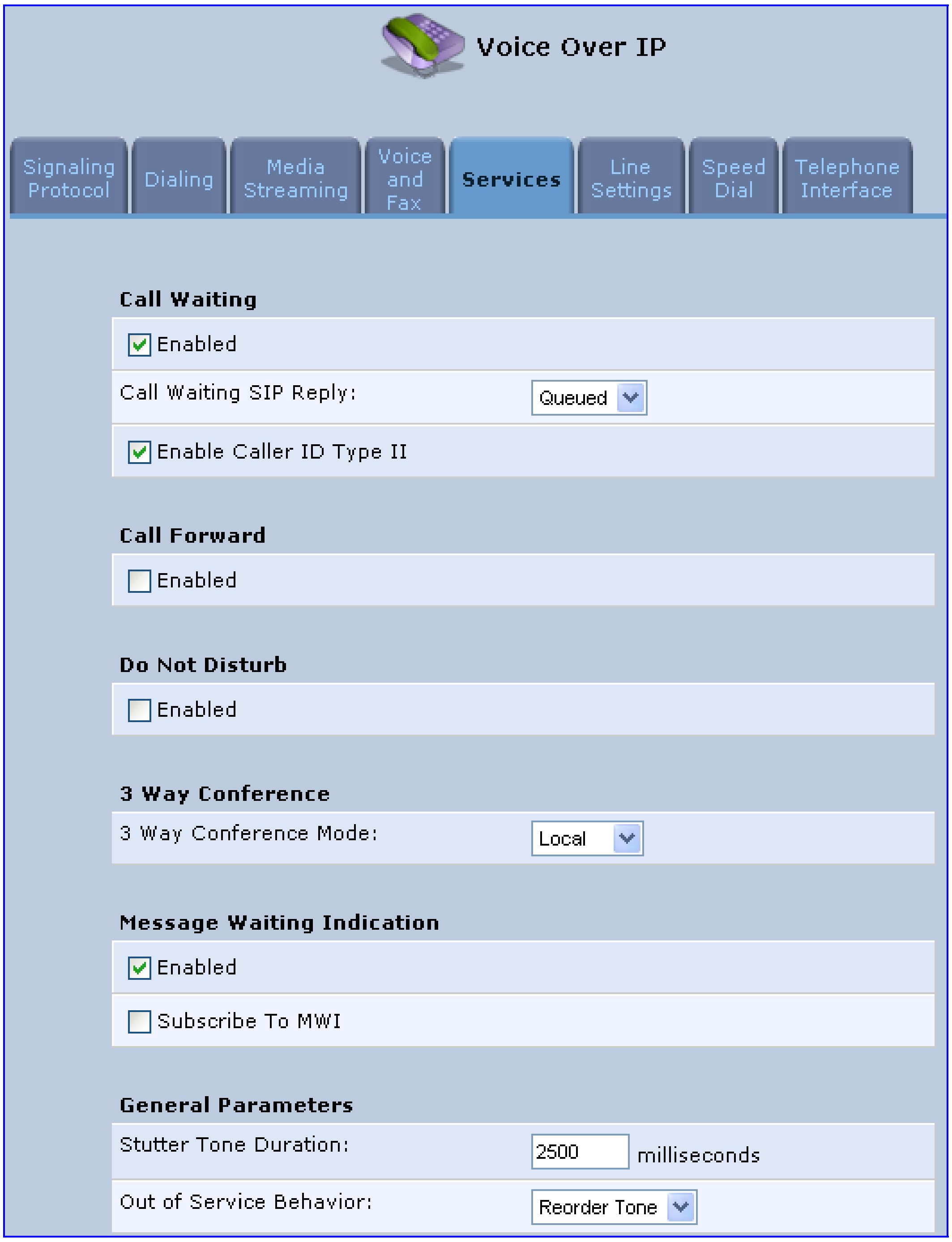
Parameter	Description
Enable CNG Detection	Check to enable detection of the fax CNG signal. When the local fax machine connected to MP-20x receives a fax, MP-20x switches to T.38 fax relay upon detection of the CED signal from the remote fax. If the local fax machine sends a fax, MP-20x switches to T.38 only after detecting the CNG signal from the local side and the CED signal from the remote side. If the “Enable CNG Detection” check box is enabled, MP-20x 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.
Switch To Fax Only By The Answering Side	Typically, switching to fax mode is the responsibility of the answering side. However, in some cases, the sending machine can also switch to fax mode. If this check box is marked, the sending machine does not switch to fax, but allows the answering side to detect the fax and switch to fax mode.

5.5 Configuring Services Parameters

➢ **To configure supplementary services:**

- In the 'Voice Over IP' screen, click the **Services** tab; the basic 'Services' parameters screen opens. To view advanced parameters, click the **Advanced** button.

Figure 5-6: Voice Over IP - Services Screen



Call Waiting

☑ Enabled

Call Waiting SIP Reply: Queued

☑ Enable Caller ID Type II

Call Forward

☐ Enabled

Do Not Disturb

☐ Enabled

3 Way Conference

3 Way Conference Mode: Local

Message Waiting Indication

☑ Enabled

☐ Subscribe To MWI

General Parameters

Stutter Tone Duration: 2500 milliseconds

Out of Service Behavior: Reorder Tone

Table 5-5: Services Tab Parameters Description

Parameter	Description
Call Waiting	
Enabled	Check to enable the Call Waiting feature.
Call Waiting SIP Reply	The response message sent when another call arrives while a call is in progress. There are two possibilities: 180 Ringing or 182 Queued (default).
Enable Caller ID Type II	Checked to enable caller ID of a waiting call (Called Caller ID type 2).
Call Forward	
Enabled	Enables call forwarding. 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. **Note:** The Call Forward feature is functional only when MP-20x is registered to a proxy.
Call Forward Type	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. **Note:** This parameter is available only when "No Reply" is selected for the parameter 'Call Forward Type'.
Key Sequence	The default is *72 but users can modify to any sequence of up to 2 digits, i.e., *n or *nm.
Do Not Disturb	
Enabled	Check this box to enable the Do Not Disturb (DND) feature. This feature allows you to prevent incoming calls from ringing at your phone. When Do Not Disturb is enabled, callers receive a busy signal or an announcement. The DND is activated using the phone keypad. Default is disabled.
Key Sequence	The key sequence to activate/deactivate the DND feature.

Parameter	Description
3 Way Conference	
Notes for MP-202C when three-way conferencing is enabled and two lines are enabled: • When both phone lines are active (off hook or ringing), a user can't place a call on hold. If a call is placed on hold, a busy tone is played. • When there are two active calls on one line(*), the other line is unavailable (i.e., a busy tone is played on the other phone). Any incoming call to the second line is rejected. • When both lines are in a call, a call waiting for either line is rejected. • No confirmation tone is played after a successful call transfer in "flash + digits" mode. * A two active call scenario starts when a user places a call on hold and hears the dial tone.	
3 Way Conference Mode	Selects how 3-way conference calls are handled: ▪ **Local:** locally by the device ▪ **Remote:** by a remote media server (RFC 4240)
Media Server Address	The address of the remote media server that handles conference calls. **Note:** This parameter is available only when "Remote" is selected for the parameter '3 Way Conference Mode'.
Message Waiting Indication	
Enabled	If a user has an unheard voice mail message, a stutter dial tone is heard when the user picks up the phone. In addition, MP-20x generates an FSK signal to the phone to indicate that a message is waiting. If the telephone connected to MP-20x supports this feature, an MWI 'envelope icon' is displayed.
Subscribe to MWI	Select this check box 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. **Note:** This parameter is available only when the check box 'Subscribe to MWI' is selected.
MWI Server Port	The port number of the MWI server. **Note:** This parameter is available only when the check box 'Subscribe to MWI' is selected.
MWI Subscribe Expiration TIme	The interval between registrations. **Note:** This parameter is available only when the check box 'Subscribe to MWI' is selected.
General Parameters	
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 69)
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.

5.6 Configuring Line Settings Screen

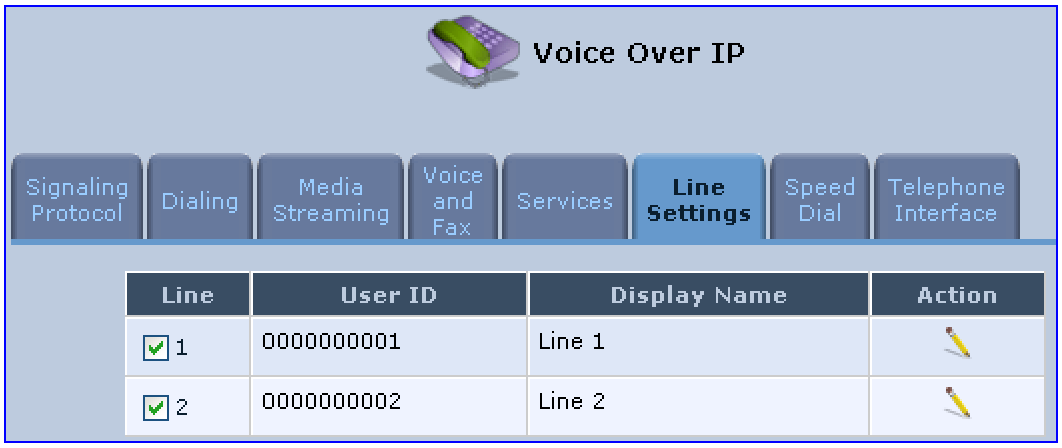
Before starting to make phone calls, configure each line's parameters.

Note: The maximum number of telephone lines that you can configure, depends on the MP-20x model.

➢ **To configure telephone lines (ports):**

1. In the 'Voice Over IP' screen, click the **Line Settings** tab; the 'Line Settings' screen opens.

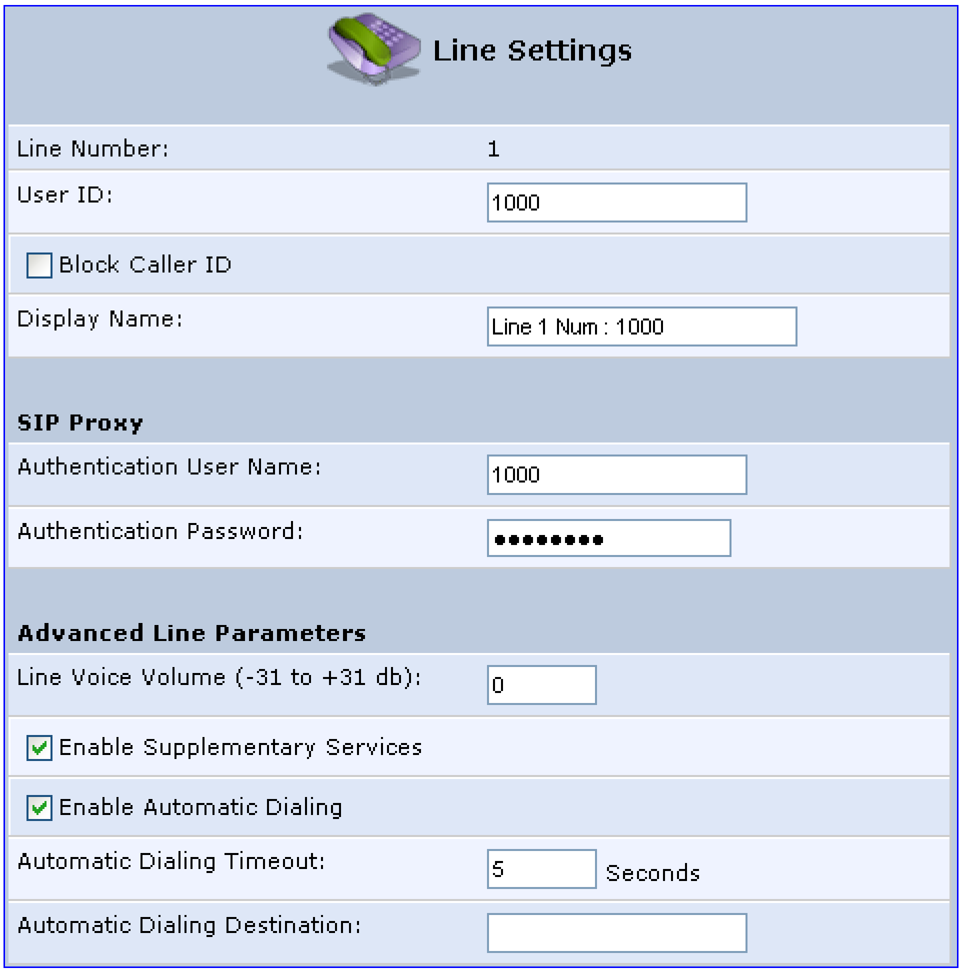
Figure 5-7: Voice Over IP - Line Settings Screen



Line	User ID	Display Name	Action
✓ 1	0000000001	Line 1	✎
✓ 2	0000000002	Line 2	✎

2. Click the **Edit** icon in each line to configure the line's different parameters.

Figure 5-8: VoIP - Line Settings - Defining a New Line



Line Settings

Line Number:	1
User ID:	1000
☐ Block Caller ID	
Display Name:	Line 1 Num : 1000
SIP Proxy	
Authentication User Name:	1000
Authentication Password:	●●●●●●●●●
Advanced Line Parameters	
Line Voice Volume (-31 to +31 db):	0
✓ Enable Supplementary Services	
✓ Enable Automatic Dialing	
Automatic Dialing Timeout:	5 Seconds
Automatic Dialing Destination:	

Table 5-6: Line Settings Tab Parameters Description

Parameter	Description
Line Number	A telephone port of MP-20x 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.
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.
SIP Proxy	
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).

Parameter	Description
Advanced Line Parameters	
Line Voice Volume	The voice volume of line (the gain from the network towards the local phone). Default = 0 dB.
Enable Supplementary Services	If it is checked, the supplementary services are enabled on this line. One can enable/disable the supplementary services per line.
Enable Automatic Dialing	If it is checked, the Automatic Dialing feature is enabled, which allows a user-defined (see below) phone number to be automatically dialed when the line is off-hooked.
Automatic Dialing Timeout	Automatic dialing is activated only after this defined time and if the user has not started dialing before this timeout.
Automatic Dialing Destination	The destination that is automatically dialed. This can be a phone number or a domain name (for example, user@101.10.13.2 or user@domain name).

5.7 Configuring Speed Dial Settings

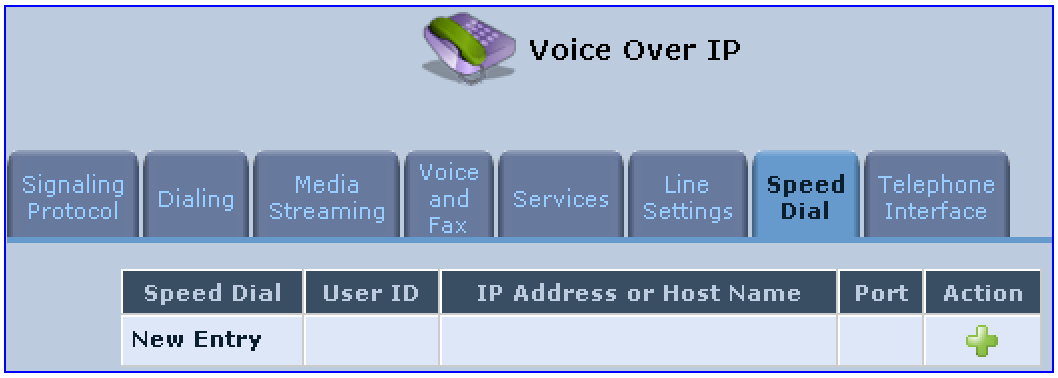
Use the 'Speed Dial Settings' screen to associate a called party's contact parameters (including the IP address of his/her ATA and Line ID) with a number that you'll dial to call the called part. The number of speed-dialing codes that can be defined is unlimited. Use the screen to define a destination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

Note: When connecting MP-20x to a World-Wide SIP Server (refer to 'Connecting MP-20x's VoIP to a VoIP Service Provider' on page 65), you don't need to configure 'Speed Dial Settings'.

➢ To configure speed dialing:

1. In the 'Voice Over IP' screen, click the **Speed Dial** tab; the 'Speed Dial' screen opens.

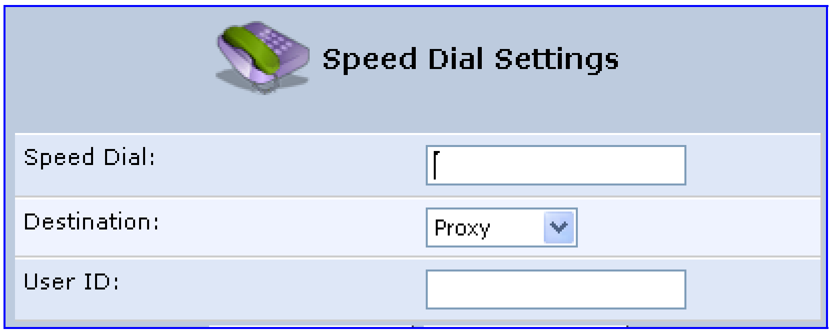
Figure 5-9: Voice Over IP - Speed Dial Screen



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

Click **New** 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 5-10: VoIP - Speed Dial Settings



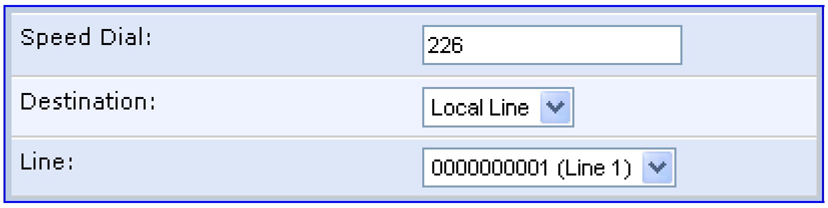
Speed Dial:
Destination: Proxy
User ID:

Table 5-7: 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 MP-20x to port ‘Line 1’ on MP-20x. The speed dial number 226 is now associated with Line 1 on MP-20x.

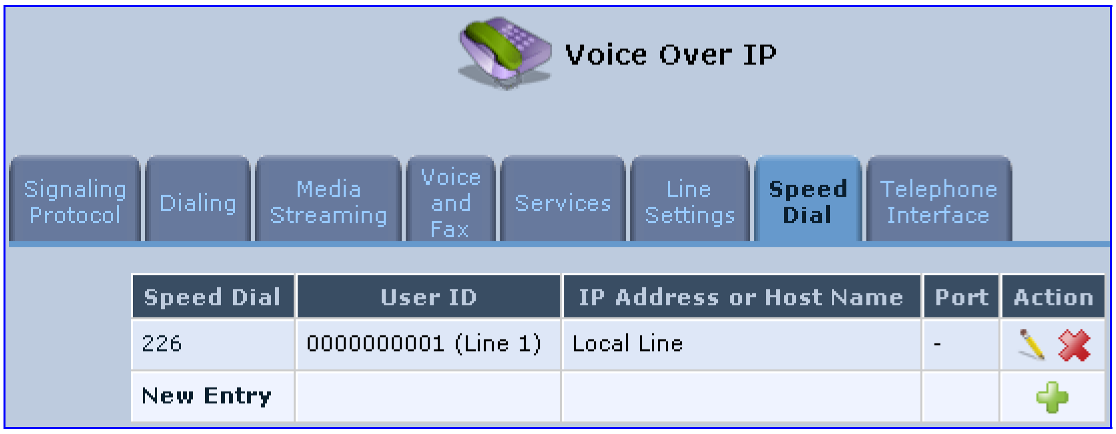
Figure 5-11: VoIP - Speed Dial - Local Line



Speed Dial:	226
Destination:	Local Line
Line:	0000000001 (Line 1)

- 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).

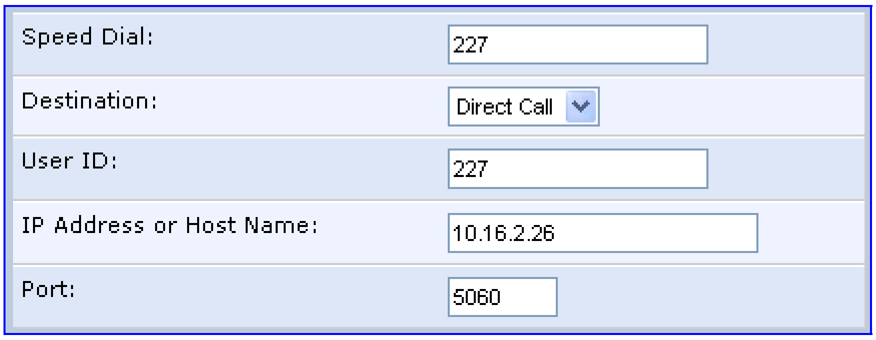
Figure 5-12: VoIP - Speed Dial Settings - Local Line



Speed Dial	User ID	IP Address or Host Name	Port	Action
226	0000000001 (Line 1)	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 5-13: VoIP - Speed Dial - Direct Call



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

Table 5-8: 'Speed Dial Settings' - Direct Call

Parameter	Description
Speed Dial	A shortcut number which you 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.

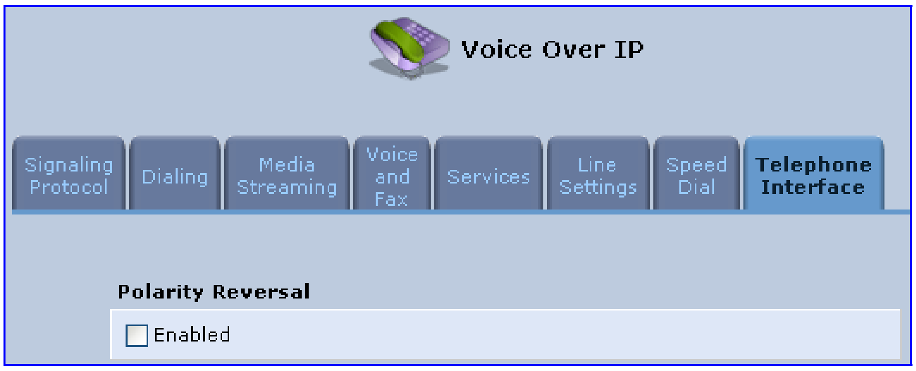
5.8 Configuring Telephone Interfaces

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

➢ To configure polarity reversal:

1. In the 'Voice Over IP' screen, click the **Telephone Interface** tab; the 'Telephone Interface' screen opens.

Figure 5-14: Voice Over IP - Telephone Interface Screen



Polarity Reversal

☐ Enabled

2. Select the check box '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.

Reader’s Notes

6 Connecting MP-20x to a VoIP Service Provider

Using MP-20x'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 MP-20x'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.

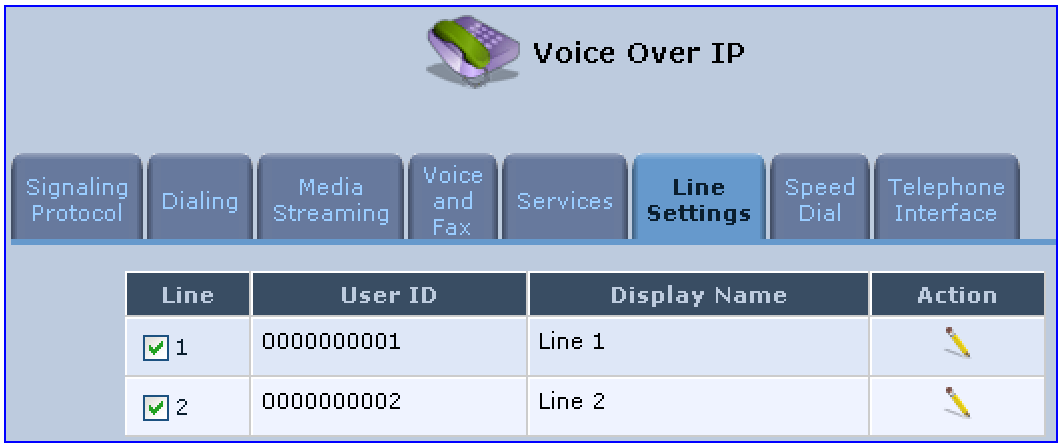
6.2 Configuring VoIP Parameters

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. In the left sidebar, click the menu **Voice Over IP**; the 'Voice Over IP' screen opens.
2. Click the **Line Settings** tab. Enable only the lines that you are using, by selecting the check box, and then click **Apply**.

Figure 6-1: Voice Over IP - Line Settings Screen

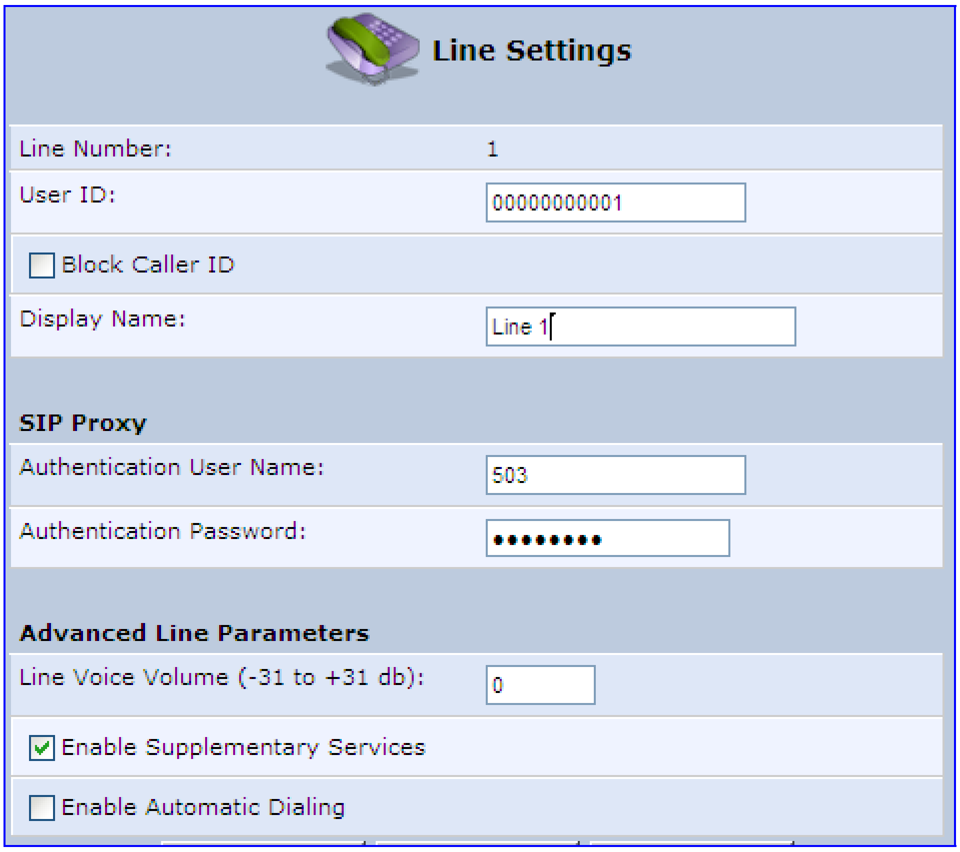


Line	User ID	Display Name	Action
✓ 1	0000000001	Line 1	✎
✓ 2	0000000002	Line 2	✎

Note: The maximum number of telephone lines that you can configure depends on the MP-20x model.

3. Click the **Edit** icon corresponding to the line that you want to configure (example, line 1); the ‘Line Settings’ screen opens. 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 Number: 1

User ID: 00000000001

☐ Block Caller ID

Display Name: Line 1

SIP Proxy

Authentication User Name: 503

Authentication Password: ••••••••

Advanced Line Parameters

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

☑ Enable Supplementary Services

☐ Enable Automatic Dialing

4. Click the **Signaling Protocol** tab and then select the ‘Use SIP Proxy’ check box (refer to 'Configuring Signaling Protocol Parameters' on page 37).
5. In the field ‘Proxy IP Address or Host Name’, define the ISP’s SIP proxy, provided by the ISP (refer to 'Configuring Signaling Protocol Parameters' on page 37).
6. Click **OK** or **Apply** to complete the VoIP configuration.

Note: Check that MP-20x was successfully registered by clicking **System Monitoring** menu > 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 MP-20x's non-volatile memory. From now on, you won’t need the PC to make VoIP calls.

7 Making VoIP Calls

Users connected to MP-20x 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:**

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:**

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:**

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.

For configuring call waiting, refer to 'Configuring Dialing Parameters' on page 43.

7.3 Putting a Call on Hold

➢ **To place the remote party on hold when 'Flash only' is configured:**

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:**

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'.

For configuring parameters for placing a call on hold, refer to 'Configuring Dialing Parameters' on page 43.

7.4 Performing a Call Transfer

➢ **To transfer an existing call with (B) to a third party (C) when 'Flash only' is configured:**

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:**

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.

For configuring call transfer, refer to 'Configuring Dialing Parameters' on page 43.

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:**

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:**

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.

For configuring call transfer parameters, refer to 'Configuring Dialing Parameters' on page 43.

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 54)
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 54).
6. Replace the receiver; from now on, all incoming calls are 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 forwarding:

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.

Note: The Call Forward feature is functional only when MP-20x is registered to a proxy.

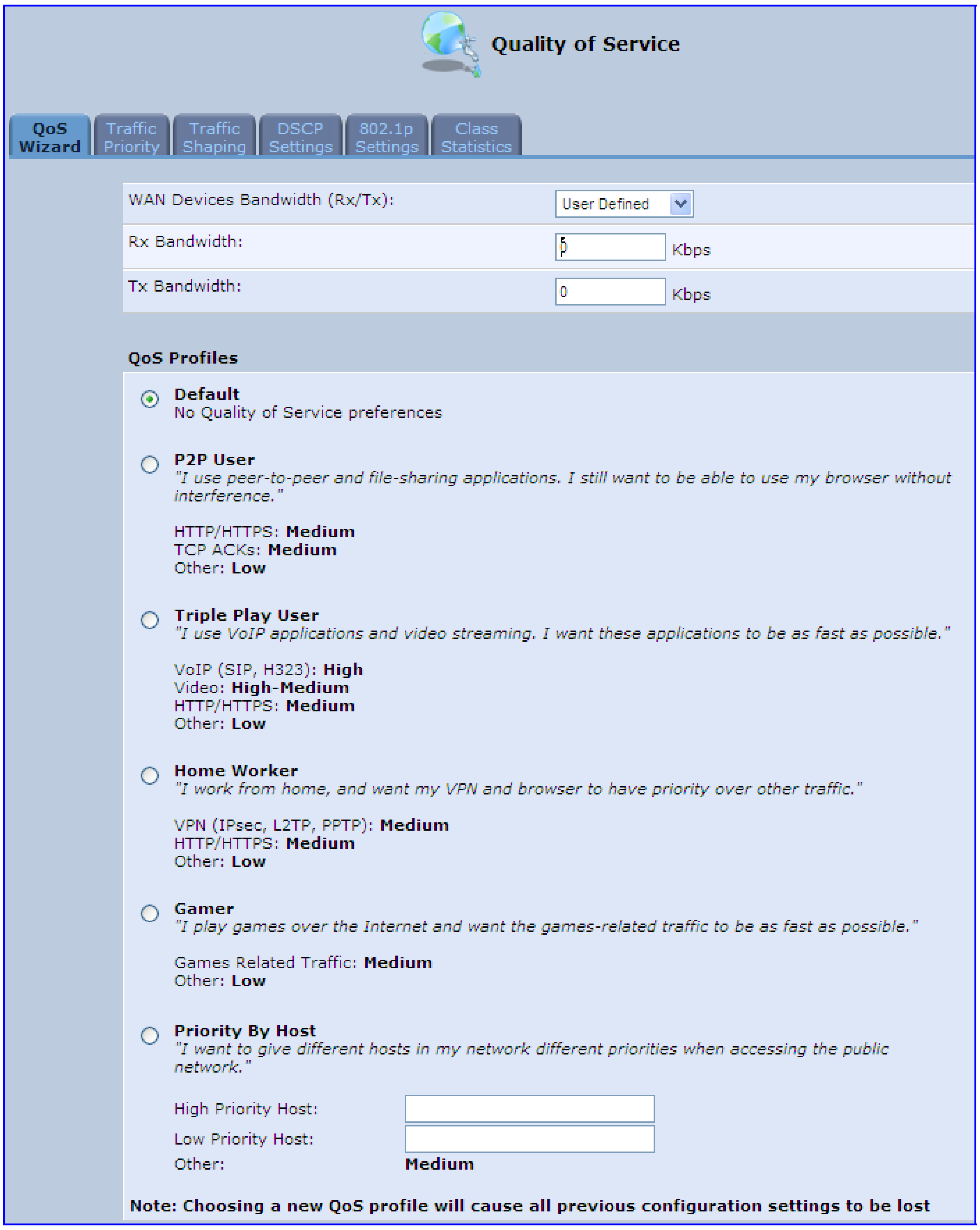
8 Quality of Service (QoS)

8.1 QoS Wizard

➤ To use the QoS Wizard:

1. From the sidebar menu, click the **QoS** menu link; the **QoS Wizard** tab's screen appears by default.

Figure 8-1: QoS Wizard Tab Screen



WAN Devices Bandwidth (Rx/Tx): User Defined

Rx Bandwidth: 5 Kbps

Tx Bandwidth: 0 Kbps

QoS Profiles

[✓ ●] **Default**
No Quality of Service preferences

○ **P2P User**
"I use peer-to-peer and file-sharing applications. I still want to be able to use my browser without interference."

HTTP/HTTPS: **Medium**
TCP ACKs: **Medium**
Other: **Low**

○ **Triple Play User**
"I use VoIP applications and video streaming. I want these applications to be as fast as possible."

VoIP (SIP, H323): **High**
Video: **High-Medium**
HTTP/HTTPS: **Medium**
Other: **Low**

○ **Home Worker**
"I work from home, and want my VPN and browser to have priority over other traffic."

VPN (IPsec, L2TP, PPTP): **Medium**
HTTP/HTTPS: **Medium**
Other: **Low**

○ **Gamer**
"I play games over the Internet and want the games-related traffic to be as fast as possible."

Games Related Traffic: **Medium**
Other: **Low**

○ **Priority By Host**
"I want to give different hosts in my network different priorities when accessing the public network."

High Priority Host:
Low Priority Host:
Other: **Medium**

Note: Choosing a new QoS profile will cause all previous configuration settings to be lost

2. From the 'WAN Devices Bandwidth (Rx/Tx)' drop-down list, select the Rx and Tx bandwidth limitation for the device.
3. In the 'QoS Profiles' group, select a profile.
4. Click **OK**.

Note: Selecting a new QoS profile deletes all previous QoS settings.

8.2 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 2 Mbps. 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

In addition, you can define QoS traffic shaping rules for a default device. These rules are 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.

MP-20x also supports dynamic traffic shaping during a call. Traffic shaping is critical in residential VoIP gateways because of the bottleneck created in the ADSL or Cable modem, mainly in the upload direction. Dynamic traffic shaping ensures a minimum bandwidth for VoIP calls. Without dynamic traffic shaping, traffic shaping limits the bandwidth at all times, even if the user is not making a VoIP call and therefore, the service provider needs to configure the QoS traffic shaping transmit (Tx) bandwidth according to the user's specific upload bandwidth. Configuring a lower value results in a lower upload bandwidth (not only during VoIP calls).

Dynamic traffic shaping enables the service provider to configure two upload traffic shaping bandwidth parameters:

- "Tx Bandwidth" - for all traffic
- "Tx Bandwidth during Call" - for VoIP calls

MP-20x normally uses the "Tx Bandwidth" value. When the user makes a VoIP call (i.e. any phone/s connected to MP-20x is ringing or off-hook), MP-20x switches to use the "Tx Bandwidth during Call" value.

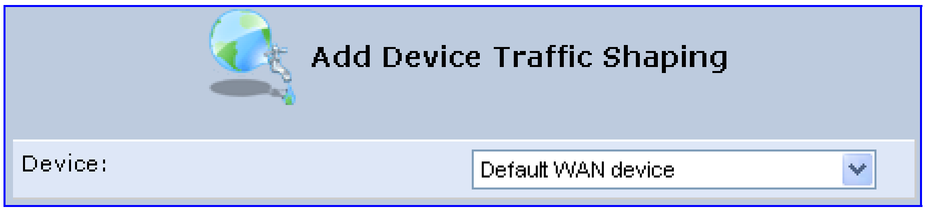
8.2.1 Device Traffic Shaping

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

➢ **To add a traffic shaping device:**

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

Figure 8-2: QoS - Add Device Traffic Shaping

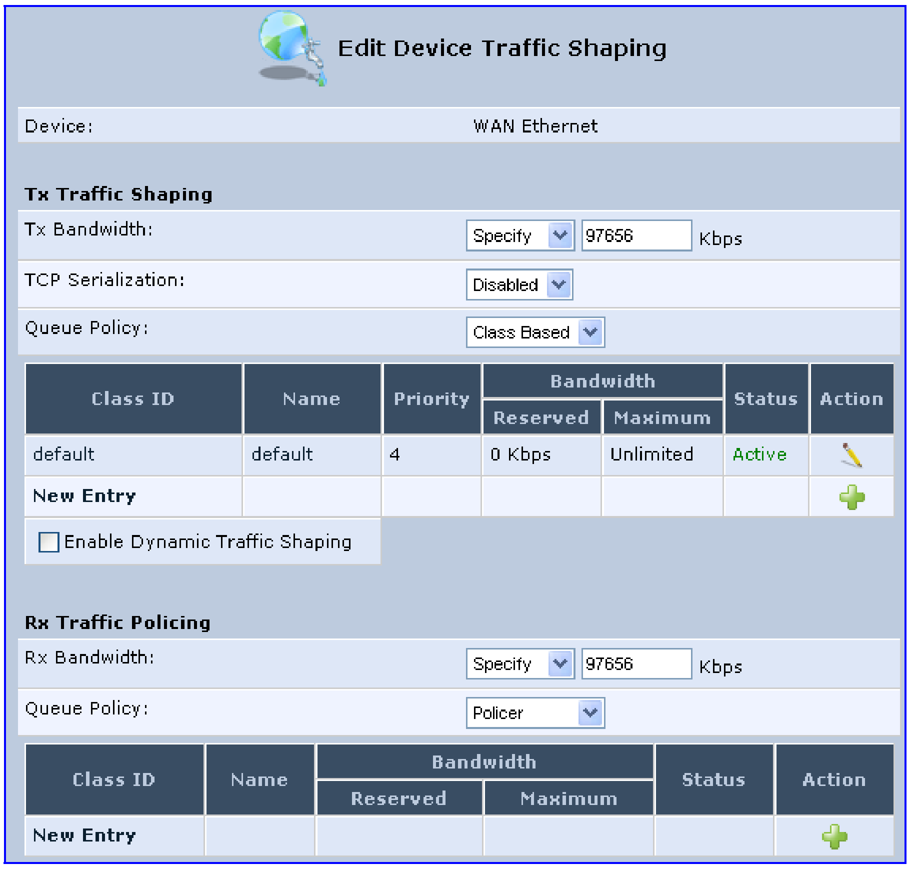


Add Device Traffic Shaping

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). For example, select the option 'WAN Ethernet', and then click **OK**; the 'Edit Device Traffic Shaping' screen opens (refer to the figure).

Figure 8-3: QoS - Edit Device Traffic Shaping



Edit Device Traffic Shaping

Device:	WAN Ethernet

Tx Traffic Shaping

Tx Bandwidth:	Specify 97656 Kbps
TCP Serialization:	Disabled
Queue Policy:	Class Based

Class ID	Name	Priority	Bandwidth		Status	Action
			Reserved	Maximum		
default	default	4	0 Kbps	Unlimited	Active	
New Entry						

☐ Enable Dynamic Traffic Shaping

Rx Traffic Policing

Rx Bandwidth:	Specify 97656 Kbps
Queue Policy:	Policer

Class ID	Name	Bandwidth		Status	Action
		Reserved	Maximum		
New Entry					

4. Configure the following fields:

Table 8-1: Edit Traffic Shaping - Parameter Descriptions

Parameter	Description
Tx Bandwidth	This parameter limits MP-20x'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 MP-20x 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 MP-20x QoS useless.
Rx Bandwidth	In the same manner, this parameter limits MP-20x's bandwidth reception rate to that of the DSL modem.
TCP Serialization	You can enable TCP Serialization in its drop-down list, either for active voice calls only or for all traffic. The screen refreshes, 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 is fragmented to smaller sections. This avoids transmission of large, bursty packets that may cause delay or jitter for real-time traffic such as VoIP.
Enable Dynamic Traffic Shaping	Select this check box if you want to configure traffic shaping specifically for VoIP calls (refer to Section 8.2 on page 72). When selected, the "Tx Bandwidth During VoIP Call" field appears. Enter the bandwidth for VoIP calls. MP-20x normally uses the "Tx Bandwidth" parameter value. When the user makes a VoIP call (i.e. any phone/s connected to MP-20x is ringing or off-hook), MP-20x switches to use the "Tx Bandwidth during Call" parameter value.

8.2.2 Shaping Classes

The bandwidth of a device can be divided 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 is then 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.

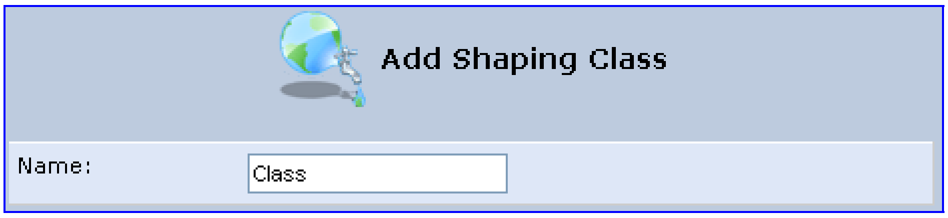
When a shaping class is defined for a specific traffic type, two shaping classes are created. The second class is the 'Default Class', responsible for all the packets that do not match the defined shaping class, or any other classes that may be defined on the device. This can be viewed in the Class Statistics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

➢ **To add a shaping class:**

1. On the sidebar, click the **QoS** menu, and then click the tab **Traffic Shaping**.
2. Click the **Edit** icon corresponding to the Device (e.g., WAN); the screen 'Edit Device Traffic Shaping' opens.

3. In the section 'Tx Traffic Shaping', click the **New** icon; the screen 'Add Shaping Class' opens.

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

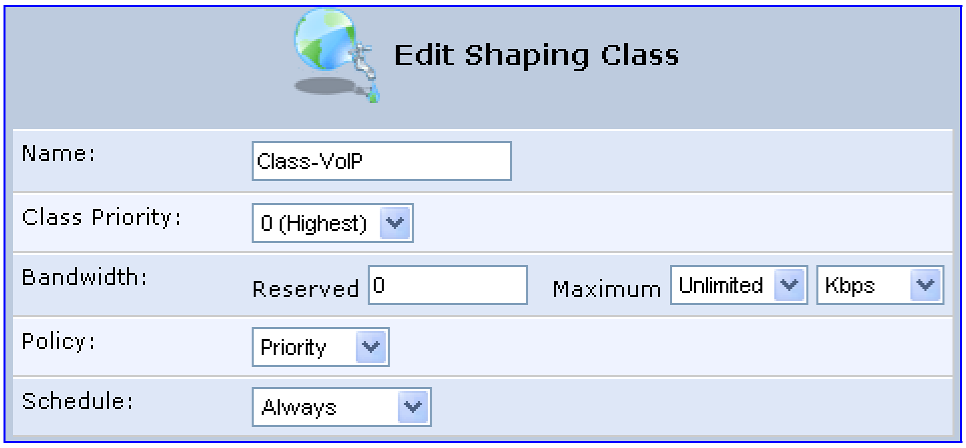

Add Shaping Class

Name: Class

4. Name the new class, and then click **OK** to save the settings; the screen 'Edit Device Traffic Shaping' opens.

5. Edit the shaping class, by clicking the **Edit** icon corresponding to the class that you added; the 'Edit Class' screen opens (refer to the figure).

Figure 8-5: QoS - Edit Device Traffic Shaping - Edit Class


Edit Shaping Class

Name: Class-VoIP

Class Priority: 0 (Highest)

Bandwidth: Reserved 0 Maximum Unlimited Kbps

Policy: Priority

Schedule: Always

6. Configure the following fields:

Table 8-2: Edit Shaping Class - Parameter Descriptions

Parameter	Description
Name:	The name of the class.
Class Priority	The class can be granted one of eight priority levels, zero being the highest and seven the lowest.
Tx Bandwidth	The reserved transmission bandwidth (Committed Information Rate, or CIR), in kbps, for each class
Rx Bandwidth	The reserved reception bandwidth (Committed Information Rate, or CIR) , in kbps, for each class

Parameter	Description
Policy	The class policy determines the policy of routing packets inside the class: ▪ **Priority:** 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. ▪ **FIFO:** First In First Out. This priority queue ignores any previously-marked priority that packets may have. ▪ **Fairness:** The fairness algorithm ensures no starvation by granting all packets a certain level of priority. ▪ **RED:** 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.
Schedule:	By default, the class is always active. However, you can configure scheduler rules to define time segments during which the class may be active.

8.2.2.1 Class Rules

Class rules define which packets belong to the class. They must be defined to associate packets that meet them with the shaping class. Without class rules, the shaping class has 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 are 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).

8.2.2.1.1 Inbound and Outbound Data

MP-20x 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. MP-20x cannot queue packets, since in most cases the LAN is much faster then the WAN, and when MP-20x 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, MP-20x cannot control the behavior of its WAN MP-20x (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 outbound/inbound class rules, refer to 'Traffic Priority' on page 77.

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 MP-20x are associated with the specific class. Any rules defined later do not have any effect.

8.3 Traffic Priority

Traffic Priority allows you to manage and avoid traffic congestion by defining inbound and outbound priority rules for each device on your MP-20x. These rules determine the priority assigned to packets traveling through the device. 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; MP-20x 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) takes precedence.

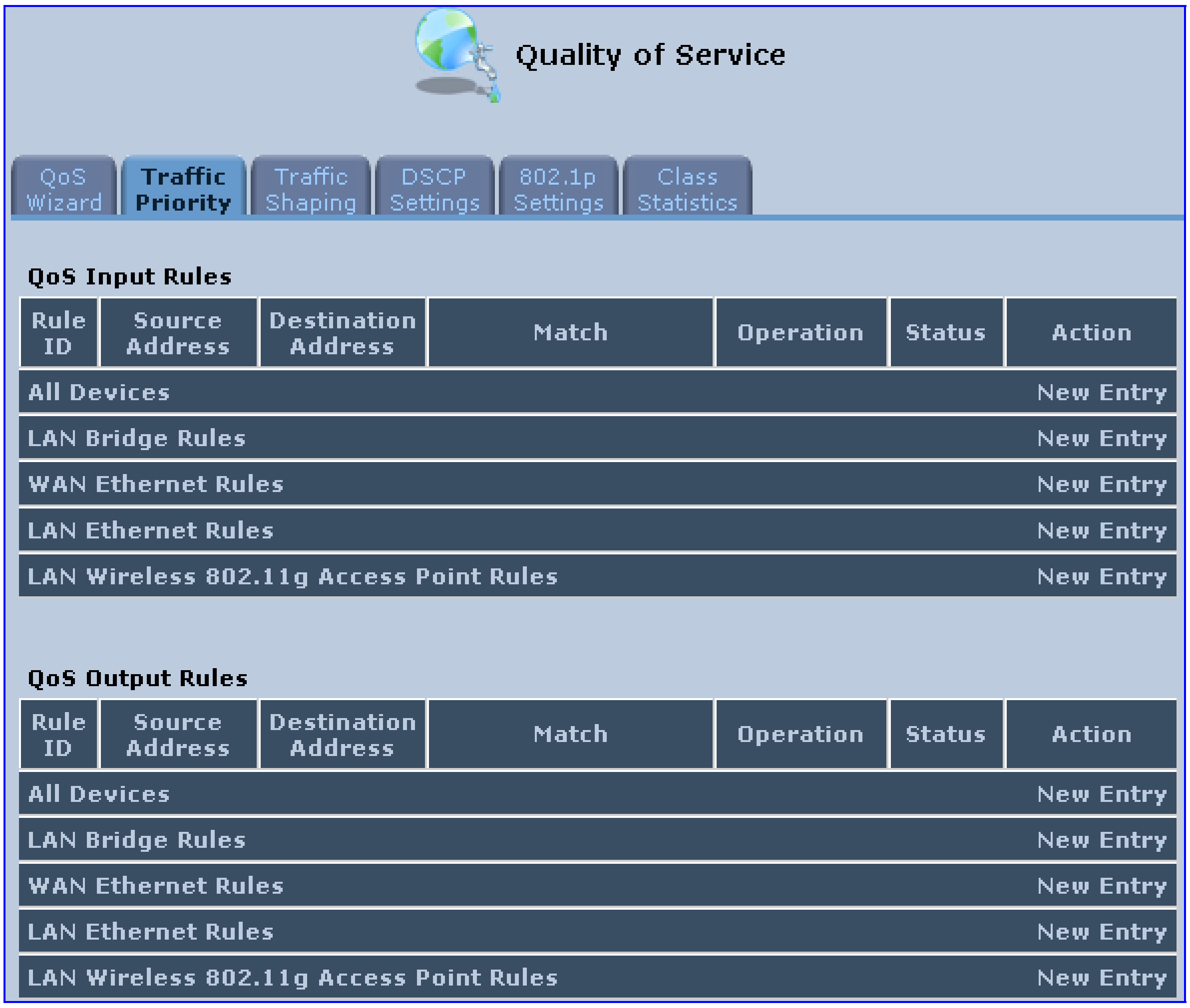
Connection-based QoS also allows inheriting QoS parameters by some of the applications that open subsequent connections. For instance, you can define QoS rules on SIP, and the rules then apply to both control and data ports (even if the data ports are unknown). This feature applies to all applications 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. From the sidebar menu, click the **QoS** menu, and then select the **Traffic Priority** tab; the 'Traffic Priority' screen 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** corresponding to 'All Devices'.

Figure 8-6: QoS - Traffic Shaping



QoS Input Rules

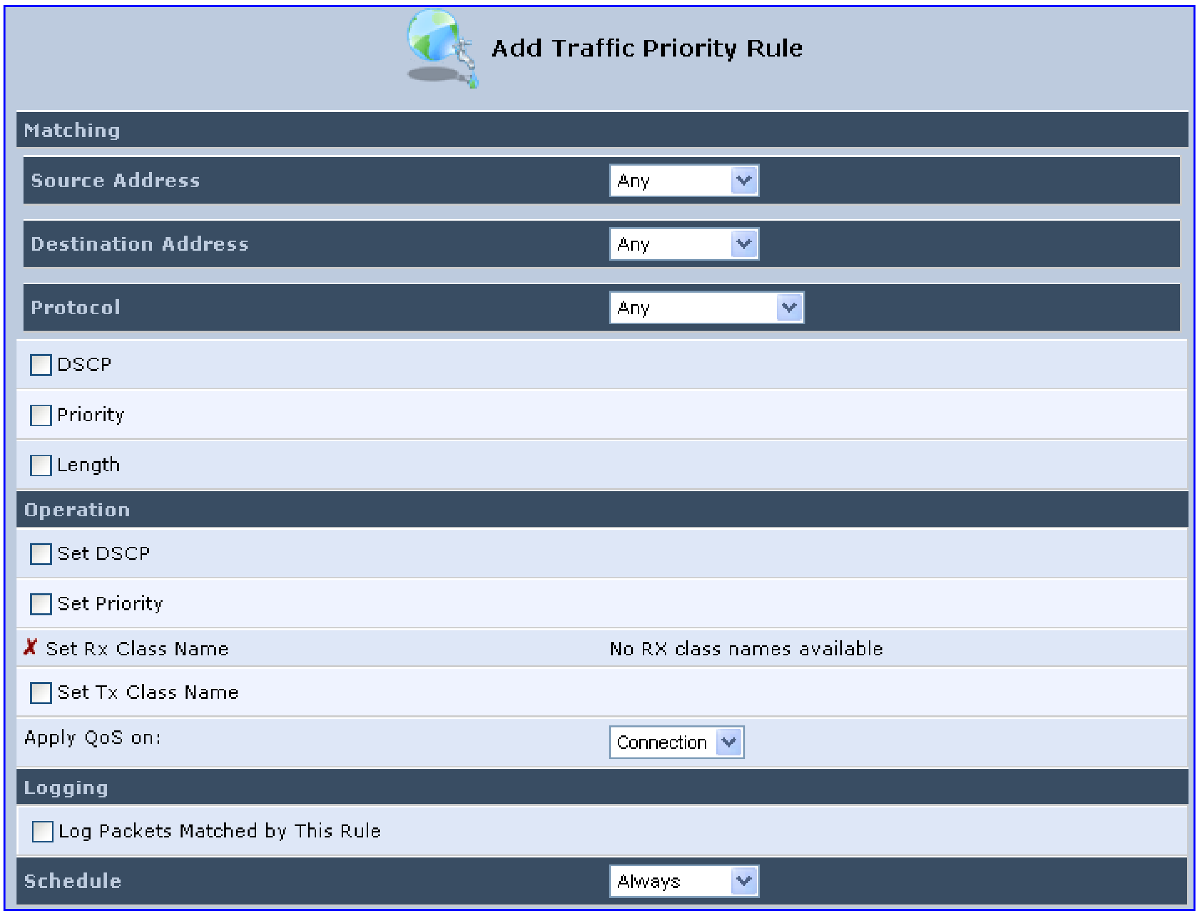
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
All Devices						New Entry
LAN Bridge Rules						New Entry
WAN Ethernet Rules						New Entry
LAN Ethernet Rules						New Entry
LAN Wireless 802.11g Access Point Rules						New Entry

QoS Output Rules

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
All Devices						New Entry
LAN Bridge Rules						New Entry
WAN Ethernet Rules						New Entry
LAN Ethernet Rules						New Entry
LAN Wireless 802.11g Access Point 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


Add Traffic Priority Rule

Matching

Source Address: Any

Destination Address: Any

Protocol: Any

☐ DSCP

☐ Priority

☐ Length

Operation

☐ Set DSCP

☐ Set Priority

✗ Set Rx Class Name: No RX class names available

☐ Set Tx Class Name

Apply QoS on: Connection

Logging

☐ Log Packets Matched by This Rule

Schedule: Always

Table 8-3: 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.

Parameter	Description
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 is always 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.

8.4 DSCP Mapping

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.

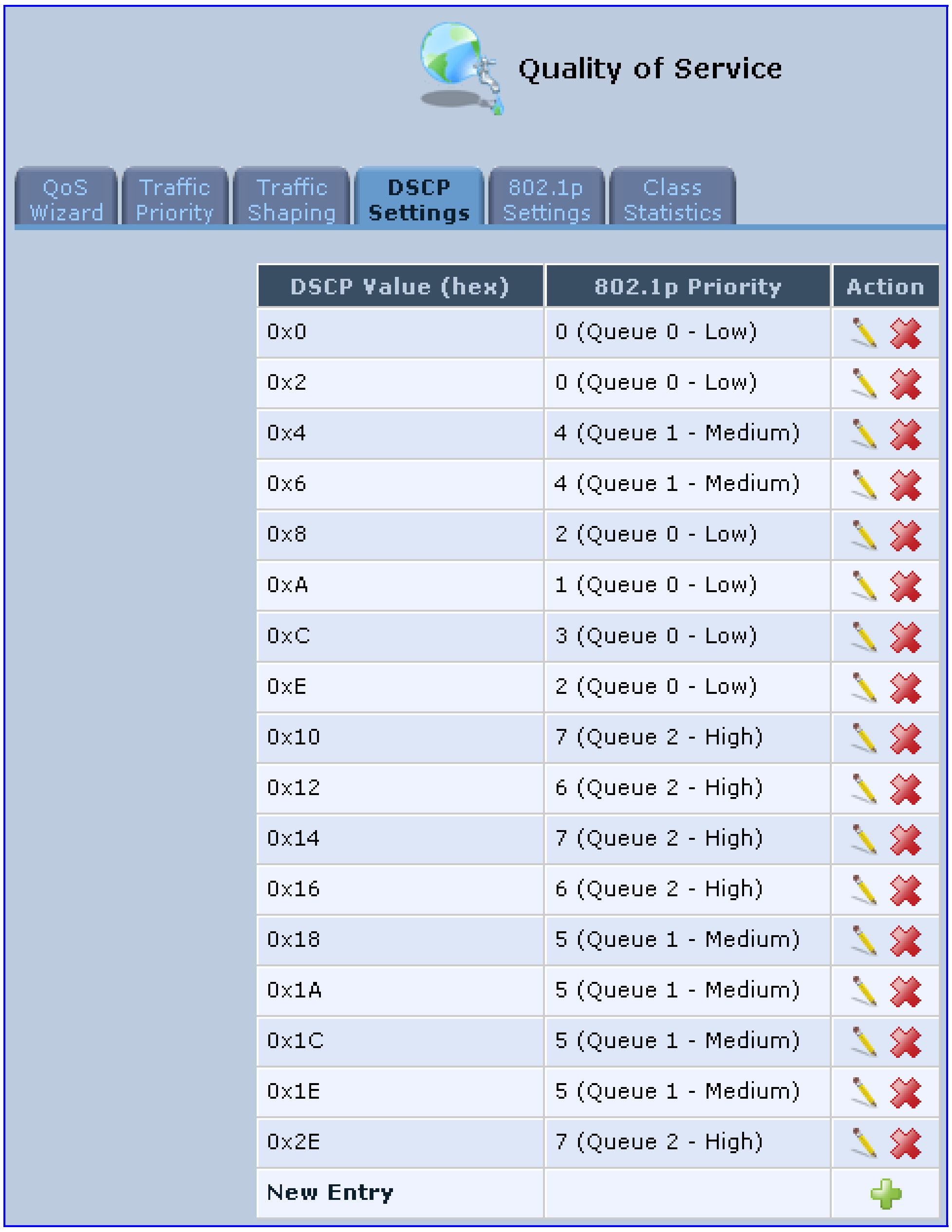
Diffserv defines a field in IP packet headers referred to as DSCP. Hosts or routers passing traffic to a Diffserv-enabled network typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular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

MP-20x 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.

➢ To set DSCP rules:

1. From the sidebar menu, click the **QoS** menu link, and then click the **DSCP Settings** tab; The following screen appears:

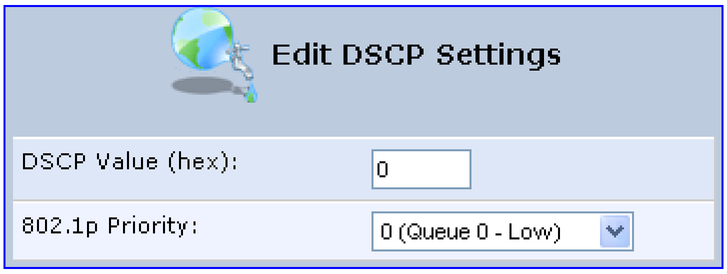
Figure 8-8: QoS - DSCP Settings



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

2. To edit an existing entry, click its corresponding **Edit** icon. To add a new entry, click the **New** icon. In both cases, the 'Edit DSCP Settings' screen appears:

Figure 8-9: QoS - Edit DSCP Settings


Edit DSCP Settings

DSCP Value (hex): 0

802.1p Priority: 0 (Queue 0 - Low)

3. Configure the following fields:

Table 8-4: Edit DSCP Settings- Parameter Descriptions

Parameter	Description
DSCP Value (hex)	Enter a hexadecimal number to serve as the DSCP value.
802.1p Priority	Select a 802.1p priority level from the drop-down list (each priority level is mapped to low/medium/high priority).

4. Click **OK** to save the settings.

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

8.5 802.1p Mapping

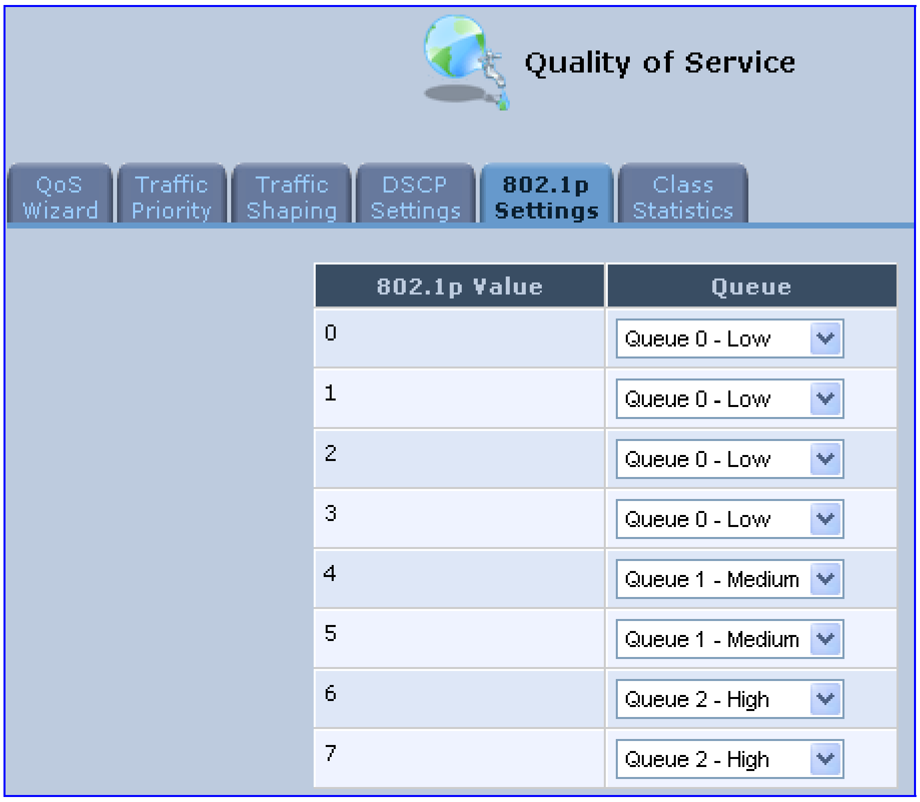
The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer. 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority. MP-20x 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.

➢ To set 802.1p rules:

1. From the sidebar menu, click the **QoS** menu link, and then click the **802.1p Settings** tab; the following screen opens:

Figure 8-10: QoS - 802.1p Settings


Quality of Service

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

2. 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 drop-down list.

3. Click **OK** to save the settings.

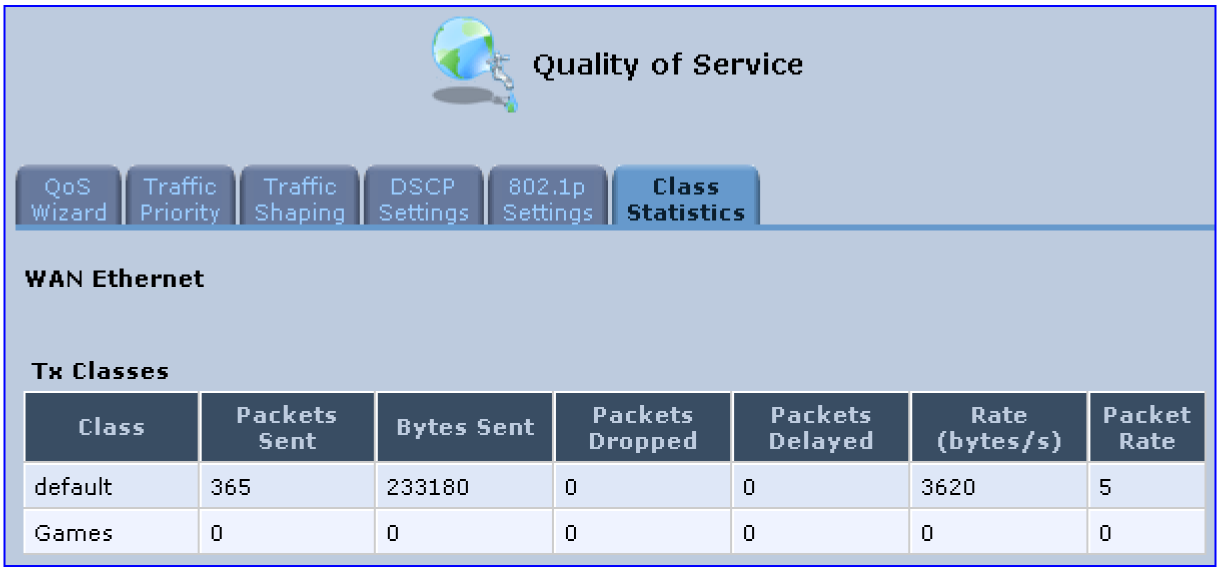
8.6 Class Statistics

MP-20x provides you with accurate, real-time information on the traffic passing 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:**

- From the sidebar menu, click the **QoS** menu link, and then click the **Class Statistics** tab; the following screen opens:

Figure 8-11: QoS - Class Statistics



WAN Ethernet

Tx Classes

Class	Packets Sent	Bytes Sent	Packets Dropped	Packets Delayed	Rate (bytes/s)	Packet Rate
default	365	233180	0	0	3620	5
Games	0	0	0	0	0	0

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

8.7 Configuring Basic VoIP QoS

The 'Traffic Shaping' feature only ensures priority to calls that originate from *inside* MP-20x. When giving VoIP priority over data, the bottleneck is effectively moved from the Cable / ADSL modem into MP-20x. 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).

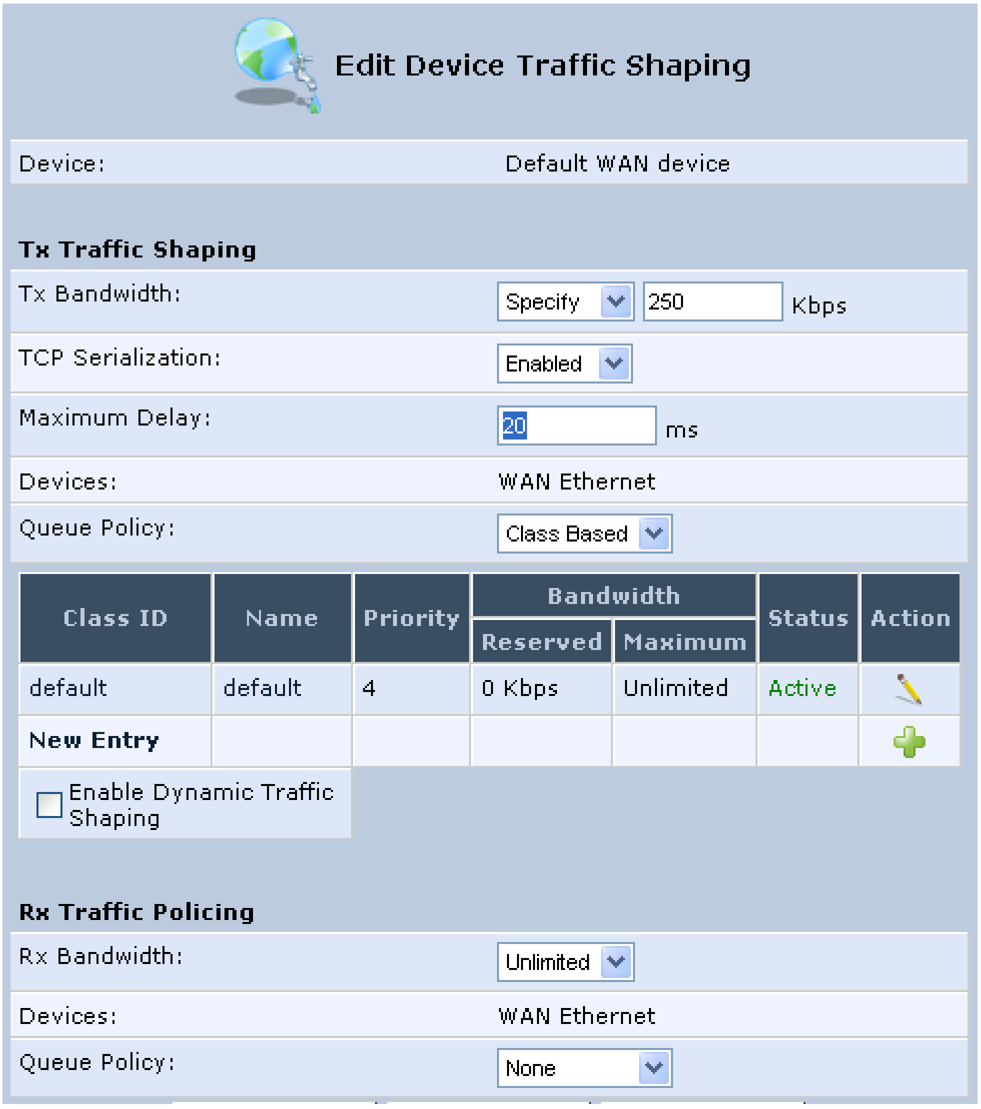
This section recommends a minimal QoS configuration that ensures sufficient QoS for VoIP calls when MP-20x is connected behind a broadband (cable or DSL) modem with limited uplink bandwidth and the user runs bandwidth-consuming applications on their PC.

Since most modems do not have any priority mechanisms, the Tx bandwidth of MP-20x should be limited according to the modem’s uplink bandwidth. Since MP-20x automatically gives 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. From the sidebar menu, click the **QoS** menu link, and then click the **Traffic Shaping** tab; the Quality of Service - Traffic Shaping screen opens.
2. Click the **New** icon; the screen 'Add Device Traffic Shaping' opens.
3. From the 'Device' drop-down list, select 'Default WAN Device' (or your PPTP/L2TP connection you have created) and then 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, from the 'TCP Serialization' drop-down list, select 'Enabled', and then use parameter 'Maximum Delay' to define the maximum allowed delay (e.g. 20 milliseconds). This causes 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

Tx Traffic Shaping

Tx Bandwidth:	Specify 250 Kbps
TCP Serialization:	Enabled
Maximum Delay:	20 ms
Devices:	WAN Ethernet
Queue Policy:	Class Based

Class ID	Name	Priority	Bandwidth		Status	Action
			Reserved	Maximum		
default	default	4	0 Kbps	Unlimited	Active	
New Entry						

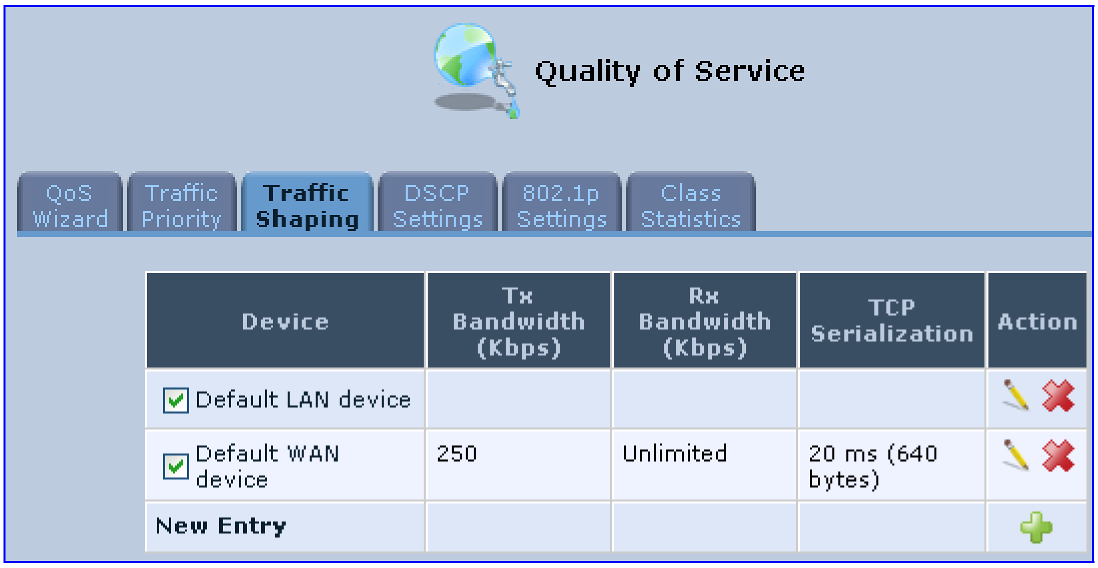
☐ Enable Dynamic Traffic Shaping

Rx Traffic Policing

Rx Bandwidth:	Unlimited
Devices:	WAN Ethernet
Queue Policy:	None

6. Click **OK** to apply the new definition.

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



Device	Tx Bandwidth (Kbps)	Rx Bandwidth (Kbps)	TCP Serialization	Action
✓ Default LAN device				
✓ Default WAN device	250	Unlimited	20 ms (640 bytes)	
New Entry				

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

9 LAN Wireless Connection

You can configure MP-20x's wireless connection, using one of the following methods:

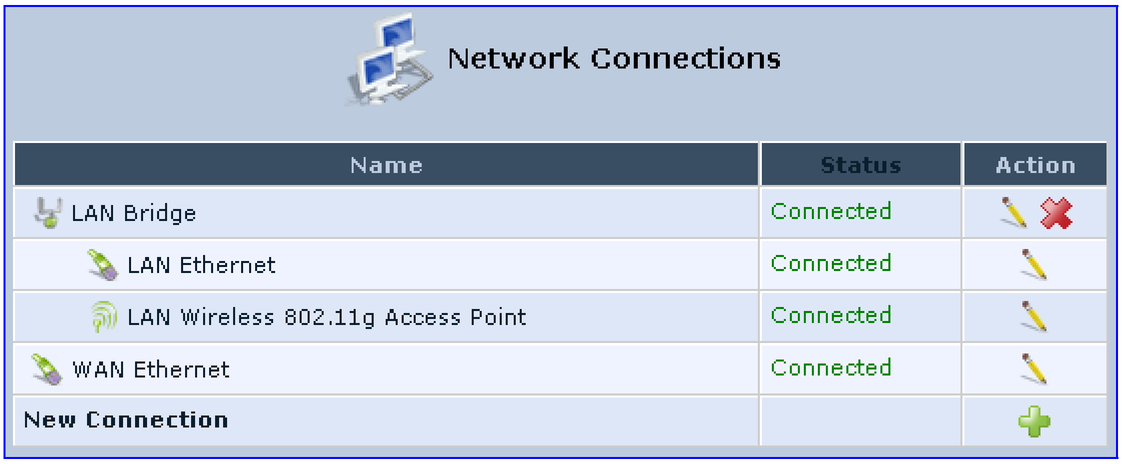
- 'Quick Setup' screen (**Quick Setup** menu - refer to 'Configuring VoIP Parameters' on page 37) - mainly for enabling wireless.
- 'Network Connections' screen (**Network Connections** menu), for (enabling wireless) advanced wireless settings, as discussed in this section.

Note: To establish a wireless network connection between a computer and the MP-20x, you must also configure the PC for wireless (refer to 'Wireless LAN Connection' on page 22).

➢ To access the Network Connections Screen for configuring wireless connection:

1. From the sidebar menu, click the **Network Connections** menu; the 'Network Connections' screen appears.

Figure 9-1: Network Connections Screen Listing LAN Wireless Interface



Network Connections

Name	Status	Action
LAN Bridge	Connected	
LAN Ethernet	Connected	
LAN Wireless 802.11g Access Point	Connected	
WAN Ethernet	Connected	
New Connection		

The 'name' column denotes the wireless LAN connection as 'LAN Wireless 802.11g Access Point'. The 'Status' column indicates whether the wireless connection is enabled or disabled ("Connected" or "Disconnected").

2. Click the **Edit** icon in the 'Action' column corresponding to the 'LAN Wireless 802.11g Access Point' network name; the 'LAN Wireless 802.11g Access Point Properties' screen appears, displaying the contents of the **General** tab.

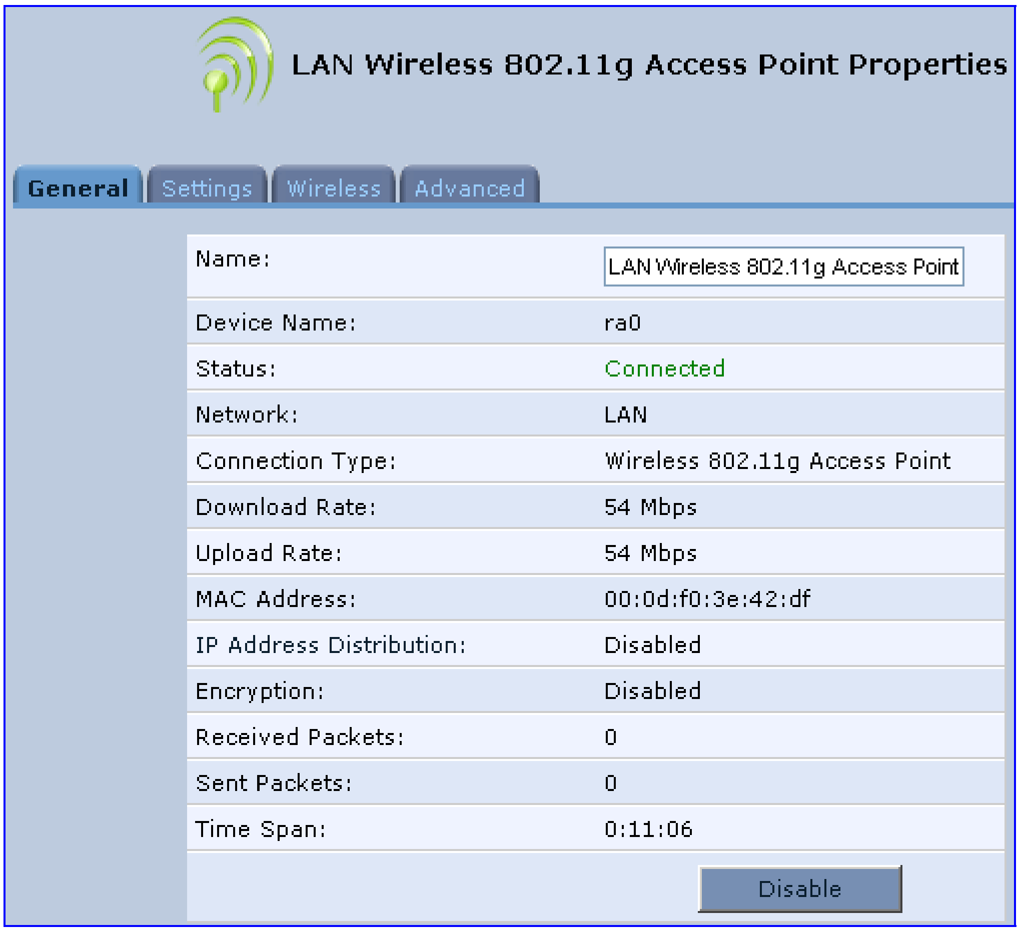
For a description of the tabs of the 'LAN Wireless 802.11g Access Point Properties' screen, refer to the following:

- **General** tab - refer to 'General Tab' on page 88
- **Settings** tab - refer to 'Settings Tab' on page 88
- **Wireless** tab - refer to 'Wireless Tab' on page 89
- **Advanced** tab - refer to 'Advanced Tab' on page 103

9.1 General Tab

The **General** tab allows you to change the name of your wireless network and allows you to enable or disable the wireless connection. In addition, this screen displays various statistics such as download and upload rate, as well as other informative parameters such as whether encryption is enabled or disabled. These parameters can be configured in the rest of the screen's tabs.

Figure 9-2: 'LAN Wireless 802.11g Access Point Properties - General' Screen



Name:	LAN Wireless 802.11g Access Point
Device Name:	ra0
Status:	Connected
Network:	LAN
Connection Type:	Wireless 802.11g Access Point
Download Rate:	54 Mbps
Upload Rate:	54 Mbps
MAC Address:	00:0d:f0:3e:42:df
IP Address Distribution:	Disabled
Encryption:	Disabled
Received Packets:	0
Sent Packets:	0
Time Span:	0:11:06

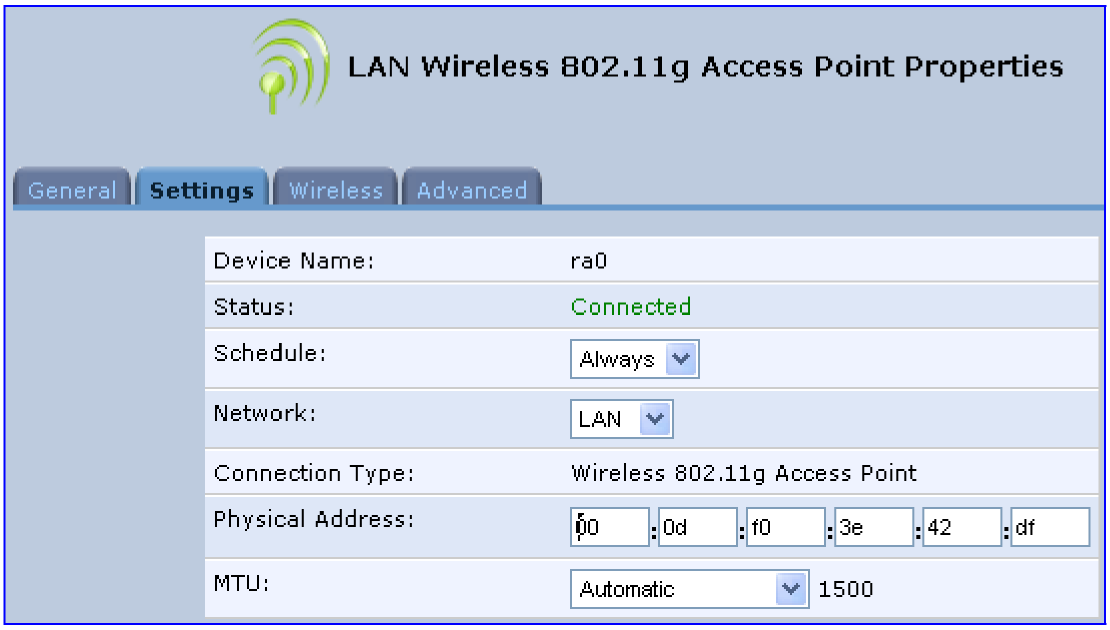
➢ To activate the wireless connection:

- Click the **Enable** button; the screen refreshes and the 'Status' field changes to "Connected".

9.2 Settings Tab

The **Settings** tab displays the connection's general parameters. It is recommended not to change the default values unless you are familiar with the networking concepts they represent. Since your MP-20x is configured to operate with the default values, no parameter modification is necessary.

Figure 9-3: LAN Wireless 802.11g Access Point Properties - Settings Screen



Device Name: ra0
Status: Connected
Schedule: Always
Network: LAN
Connection Type: Wireless 802.11g Access Point
Physical Address: 00 : 0d : f0 : 3e : 42 : df
MTU: Automatic 1500

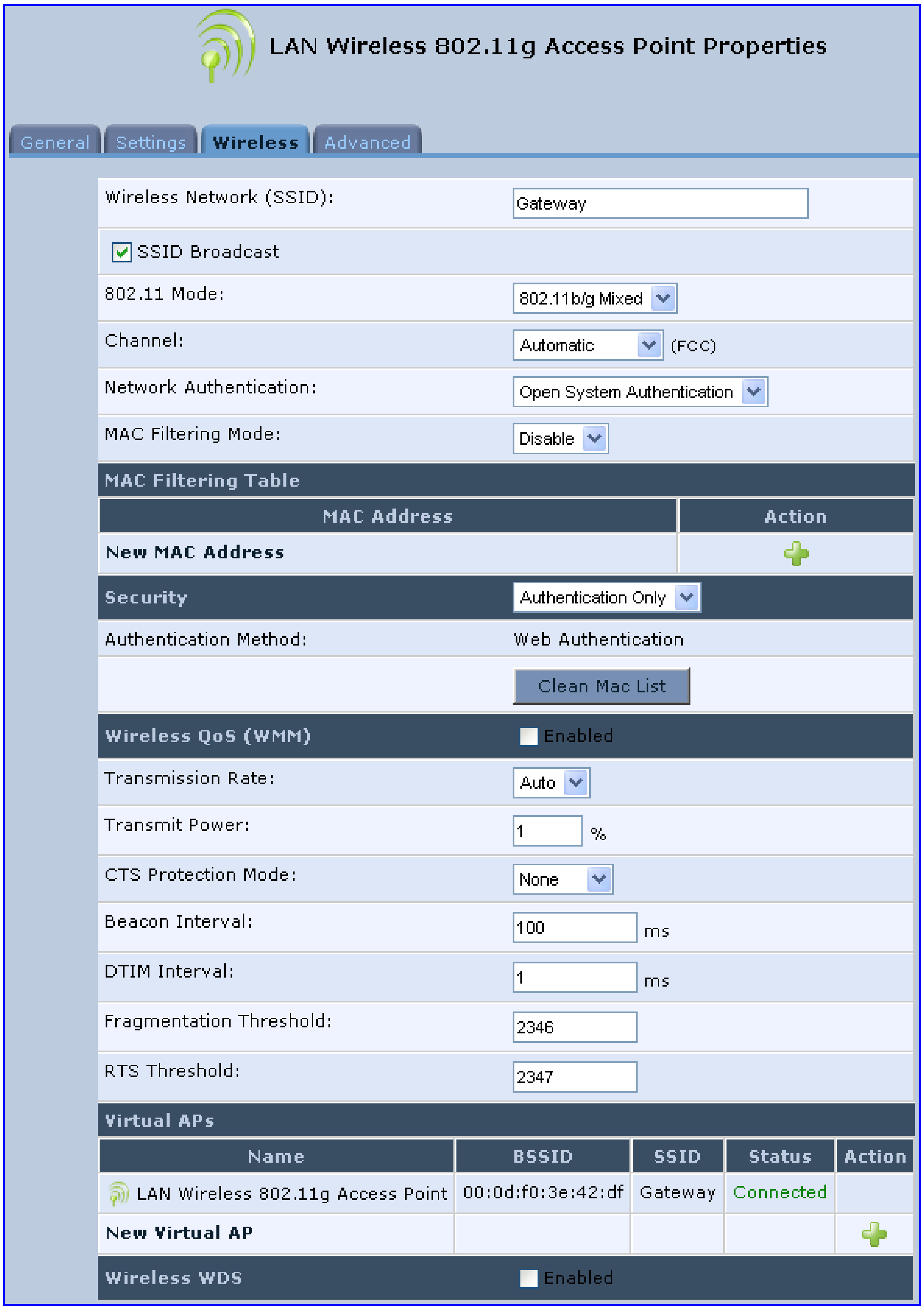
Table 9-1: LAN Wireless Settings Tab Parameter Descriptions

Parameter	Description
Schedule	You can configure scheduler rules to define time segments during which the connection is active (refer to 'Scheduler Rules' on page 248). Once a scheduler rule(s) is defined, the drop-down list displays available rules.
Network	Select whether the parameters you are configuring relate to a LAN/WAN/DMZ connection.
Physical Address	The physical address of the network card used for your network. Some cards allow you to change this address.
Clone My MAC Address	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. By default, it is set to 'Automatic', whereby 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.

9.3 Wireless Tab

The **Wireless** tab allows you define the basic wireless access point settings.

Figure 9-4: LAN Wireless 802.11g Access Point Properties - Wireless Screen



LAN Wireless 802.11g Access Point Properties

Wireless Network (SSID):	Gateway
✓ SSID Broadcast	
802.11 Mode:	802.11b/g Mixed
Channel:	Automatic (FCC)
Network Authentication:	Open System Authentication
MAC Filtering Mode:	Disable

MAC Filtering Table

MAC Address	Action
New MAC Address	

Security	Authentication Only
Authentication Method:	Web Authentication
	Clean Mac List
Wireless QoS (WMM)	☐ Enabled
Transmission Rate:	Auto
Transmit Power:	1 %
CTS Protection Mode:	None
Beacon Interval:	100 ms
DTIM Interval:	1 ms
Fragmentation Threshold:	2346
RTS Threshold:	2347

Virtual APs

Name	BSSID	SSID	Status	Action
LAN Wireless 802.11g Access Point	00:0d:f0:3e:42:df	Gateway	Connected	
New Virtual AP				

Wireless WDS ☐ Enabled

Table 9-2: Wireless Tab Parameter Descriptions

Parameter	Description
SSID Broadcast	Select this check box to enable the SSID's broadcast. SSID broadcast is used to hide the name of the AP (SSID) from clients.
802.11 Mode	Select the wireless communication standard that is compatible with your client's wireless card: 802.11g Only, 802.11b Only or 802.11b/g Mixed.
Channel	Select the appropriate channel to correspond with your network settings. All devices in your wireless network must broadcast on different channels in order to function correctly. The channels conform to the U.S.A. Regulatory Authority FCC (Federal Communications Commission).
Network Authentication	The WPA network authentication method is 'Open System Authentication', meaning that a network key is not used for authentication. When using the 802.1X WEP or Non-802.1X WEP security protocols, this field changes to a drop-down list, offering the 'Shared Key Authentication' method (which uses a network key for authentication), or both methods combined.
MAC Filtering Mode	You can filter wireless users according to their MAC address, either allowing or denying access. Choose the action to be performed by selecting it from the drop-own list.
MAC Filtering Table	For a description on adding MAC filtering addresses to the 'MAC Filtering Table', refer to 'MAC Filtering' on page 91.
Security	Configures your wireless security settings. Select the type of security protocol in the drop-down list. The screen refreshes, presenting each protocol's configuration respectively. For a detailed description on configuring the different security protocols, refer to 'Wireless Security' on page 92.
Wireless QoS (WMM)	Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance certification based on the IEEE 802.11e draft standard. It provides basic Quality of Service (QoS) features to IEEE 802.11 networks. For a detailed explanation on configuring WMM, refer to 'Wireless QoS (WMM)'.
Transmission Rate, Transmission Power, CTS Protection Mode, Beacon Interval, DTIM Interval, Fragmentation Threshold, RTS Threshold	These are wireless transmission parameters. For a detailed explanation on each of these parameters, refer to 'Transmission Properties' on page 97.
Virtual APS	You can set up multiple virtual wireless LAN's on MP-20x, limited only to the number supported by your wireless card. Such virtual wireless LANs are referred to as "Virtual APs" (virtual access points). For a detailed description on configuring Virtual APS, refer to 'Virtual Access Points' on page 99.

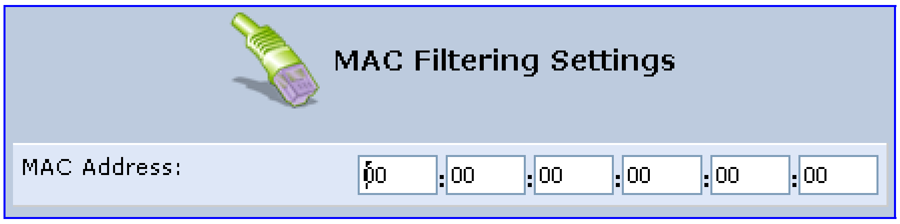
9.3.1 MAC Filtering

You can filter wireless users according to their MAC address, by either allowing or denying access.

➤ **To define MAC filtering:**

1. In the **Wireless** tab's screen, from the 'MAC Filtering Mode' drop-down list, select either 'Allow' or 'Deny'.
2. In the 'MAC Filtering Table', click **New MAC Address**; the 'MAC Filtering Settings' screen appears.

Figure 9-5: MAC Filtering Settings Screen

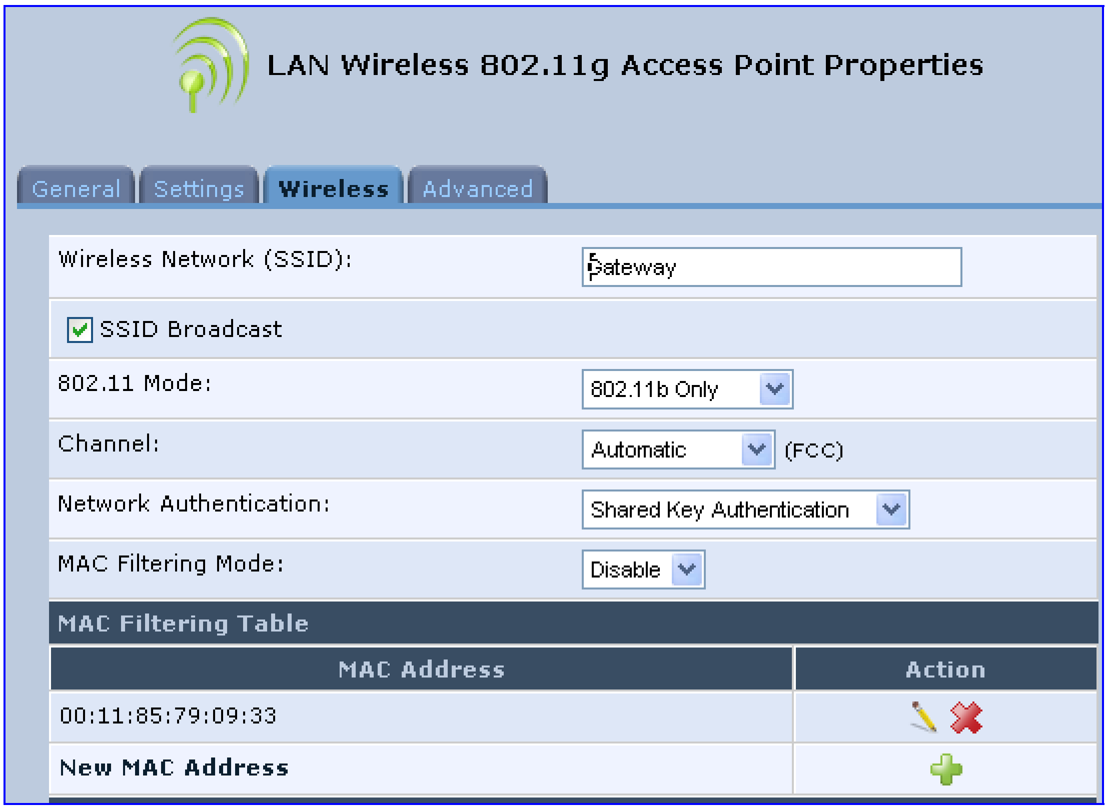


MAC Filtering Settings

MAC Address: 00 : 00 : 00 : 00 : 00 : 00

3. In the 'MAC Address' field, enter the MAC address to be filtered.
4. Click **OK**; a MAC address list appears, upon which the selected filtering action (allow/deny) will be performed.

Figure 9-6: MAC Address Added to MAC Filtering Table



LAN Wireless 802.11g Access Point Properties

Wireless Network (SSID): Gateway

✓ SSID Broadcast

802.11 Mode: 802.11b Only

Channel: Automatic (FCC)

Network Authentication: Shared Key Authentication

MAC Filtering Mode: Disable

MAC Filtering Table

MAC Address	Action
00:11:85:79:09:33	✎ ✖
New MAC Address	✚

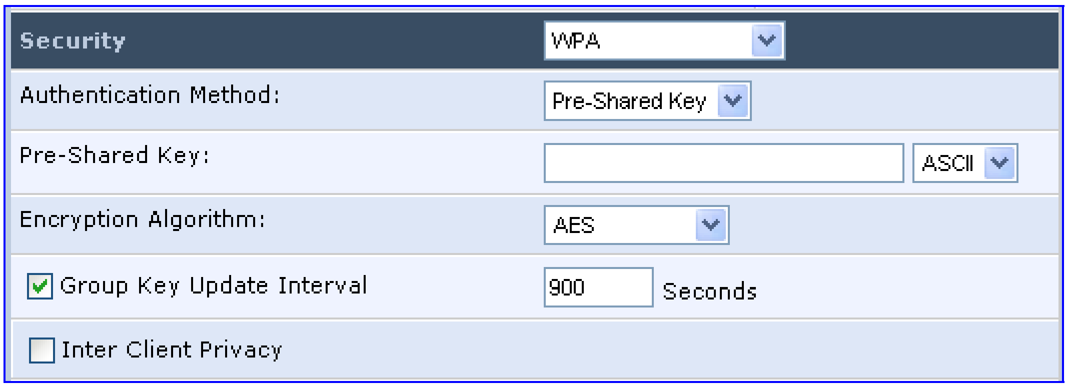
9.3.2 Wireless Security

➢ To define wireless security:

1. In the **Wireless** tab's screen, from the 'Security' drop-down list, select the type of security protocol; the screen refreshes, presenting each protocol's configuration respectively:

   - **None:** this option disables security on your wireless connection.
   - **WPA:** WPA is a data encryption method for 802.11 wireless LANs.

Figure 9-7: Configuring WPA Security



Security	WPA
Authentication Method:	Pre-Shared Key
Pre-Shared Key:	ASCII
Encryption Algorithm:	AES
✓ Group Key Update Interval	900 Seconds
☐ Inter Client Privacy	

Configure the following fields:

a. **Authentication Method:** select the authentication method ('Pre-Shared Key' and '802.1x') you would like to use.

b. **Pre-Shared Key:** this entry appears only if you selected this authentication method. Enter your encryption key (using either an ASCII or a Hex value by selecting the value type in the drop-down list provided.

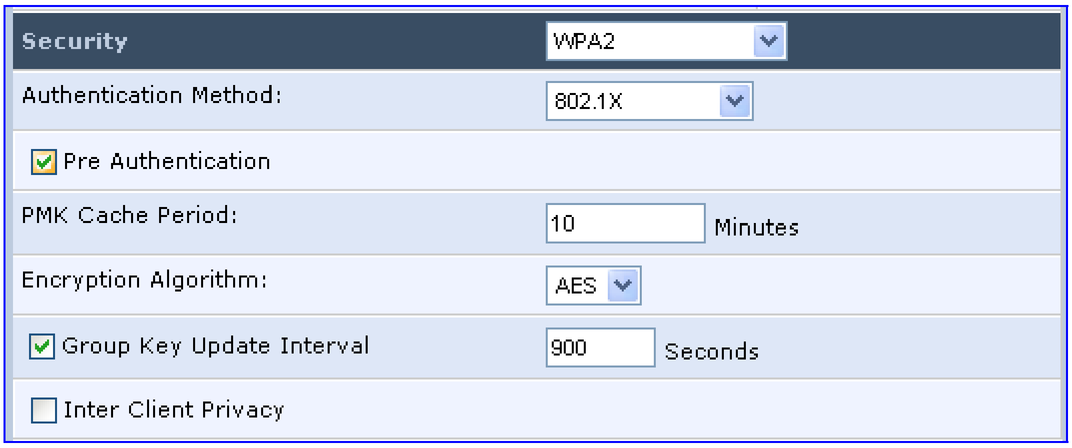
c. **Encryption Algorithm:** select between 'TKIP' (Temporal Key Integrity Protocol), 'AES' (Advanced Encryption Standard) or both ('TKIP and AES') for the encryption algorithm.

d. **Group Key Update Interval:** select the check box, and then enter the time interval in seconds for updating a group key.

e. **Inter Client Privacy:** select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

- **WPA2:** WPA2 is an enhanced version of WPA, and defines the 802.11i protocol.

Figure 9-8: Configuring WPA2 Security



Security	WPA2
Authentication Method:	802.1X
✓ Pre Authentication	
PMK Cache Period:	10 Minutes
Encryption Algorithm:	AES
✓ Group Key Update Interval	900 Seconds
☐ Inter Client Privacy	

a. **Authentication Method:** select the authentication method ('Pre-Shared Key' and '802.1x') you would like to use.

b. **Pre-Shared Key:** this entry appears only if you had selected this authentication method. Enter your encryption key in either an ASCII or a Hex value (by selecting the value type in the drop-down list provided).

c. **Pre Authentication:** (only appears when selecting the 802.1x authentication method) Select this option to enable MP-20x to accept RADIUS authentication requests from computers connected to other access points. This enables roaming from one wireless network to another.

d. **PMK Cache Period:** (only appears when selecting the 802.1x authentication method) number of minutes before deletion (and renewal) of the Pairwise Master Key used for authentication.

e. **Encryption Algorithm:** encryption algorithm used for WPA2 is the Advanced Encryption Standard (AES).

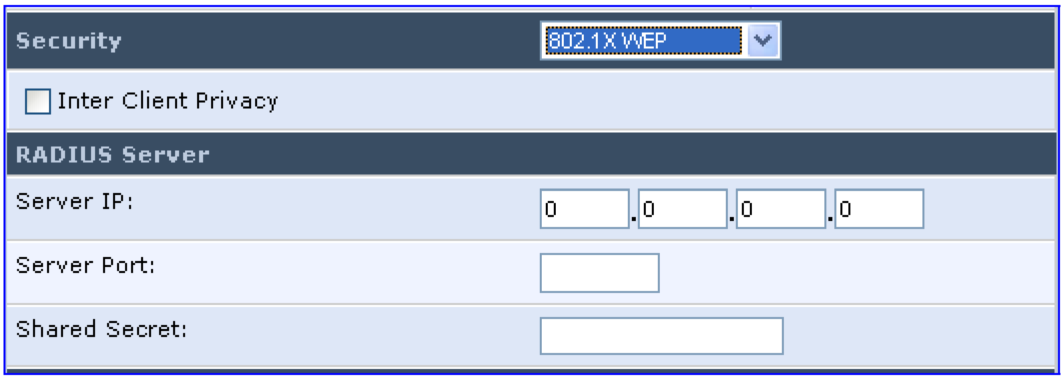
f. **Group Key Update Interval:** Defines the time interval in seconds for updating a group key.

g. **Inter Client Privacy:** select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

- **WPA and WPA2:** WPA and WPA2 is a mixed data encryption method. For a description of these fields, see WPA and WPA2 above.

- **802.1x WEP:** data encryption method utilizing an automatically defined key for wireless clients that use 802.1x for authentication and WEP for encryption.

Figure 9-9: Configuring 802.1x WEP Security



Security	802.1X WEP
☐ Inter Client Privacy	
RADIUS Server	
Server IP:	0 . 0 . 0 . 0
Server Port:	
Shared Secret:	

a. **Inter Client Privacy:** select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

b. **RADIUS Server:** configure the RADIUS Server parameters

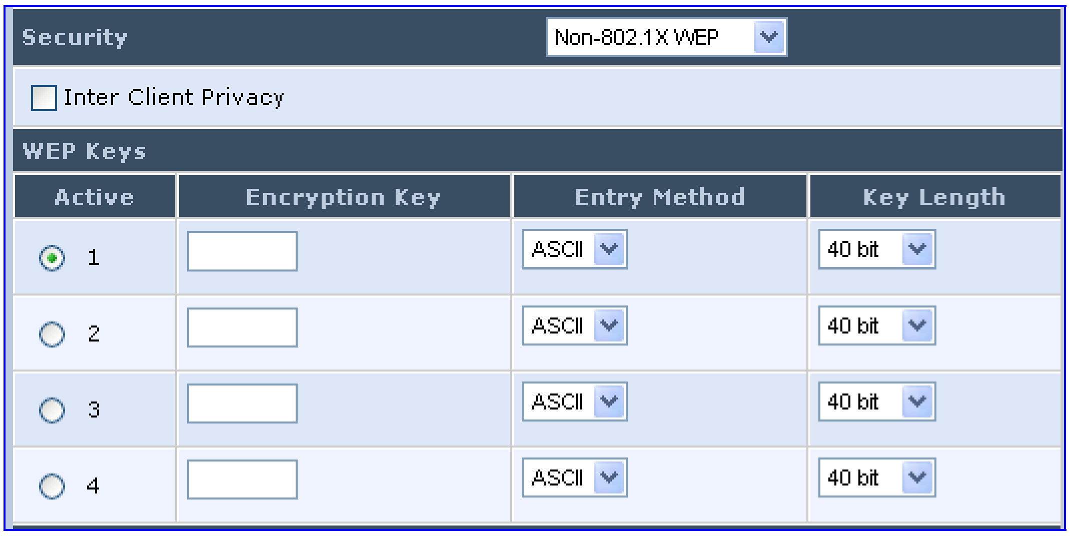
  ✓ **Server IP:** RADIUS server's IP address.

  ✓ **Server Port:** RADIUS server's port.

  ✓ **Shared Secret:** your shared secret.

- **Non-802.1x WEP:** data encryption method utilizing a statically defined key for wireless clients that do not use 802.1x for authentication, but use WEP for encryption. You may define up to four keys but use only one at a time.

Figure 9-10: Configuring Non-WEP Security



Security: Non-802.1X WEP

☐ Inter Client Privacy

WEP Keys

Active	Encryption Key	Entry Method	Key Length
● 1		ASCII	40 bit
○ 2		ASCII	40 bit
○ 3		ASCII	40 bit
○ 4		ASCII	40 bit

a. **Inter Client Privacy:** select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

b. **WEP Keys table:**

  ✓ **Active:** select the encryption key to be activated.

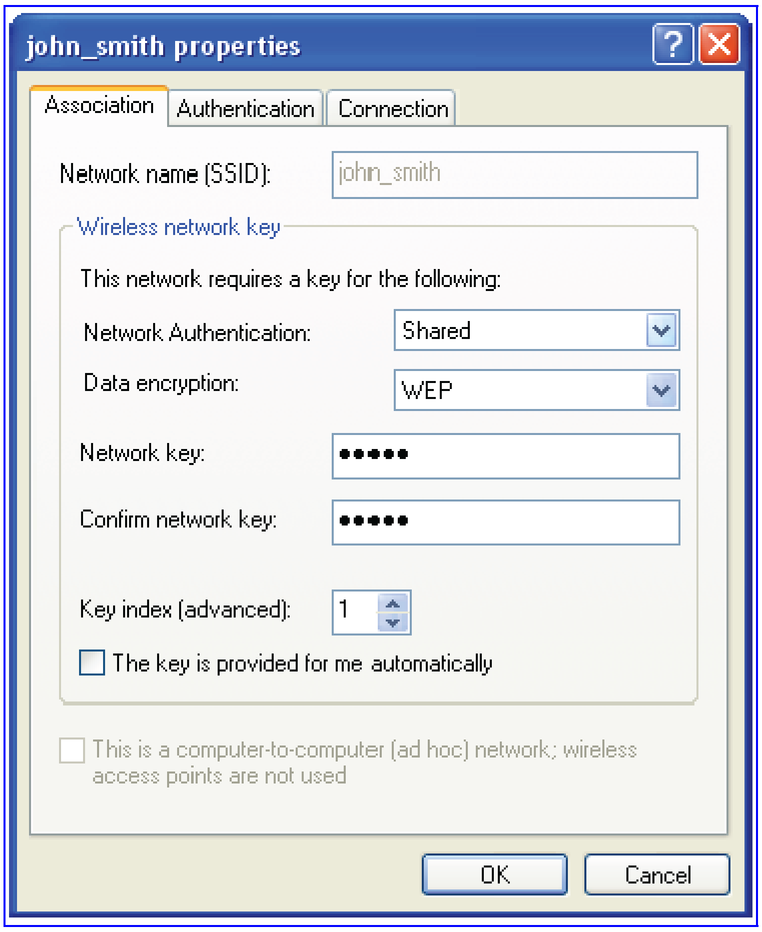
  ✓ **Encryption Key:** enter the encryption key until the entire field is filled. The key cannot be shorter than the field's length.

  ✓ **Entry Method:** select the character type for the key: ASCII or HEX.

  ✓ **Key Length:** select the key length in bits: 40 or 104 bits.

Note: The encryption key must be defined in the wireless Windows client as well. This is done in the Connection Properties Configuration window (your encryption key is entered in both the 'Network key' and 'Confirm network key' fields, as shown in the figure below.

Figure 9-11: Configuring Encryption Key in Windows Wireless Client



Network name (SSID): john_smith

Wireless network key

This network requires a key for the following:

Network Authentication: Shared

Data encryption: WEP

Network key: ●●●●●

Confirm network key: ●●●●●

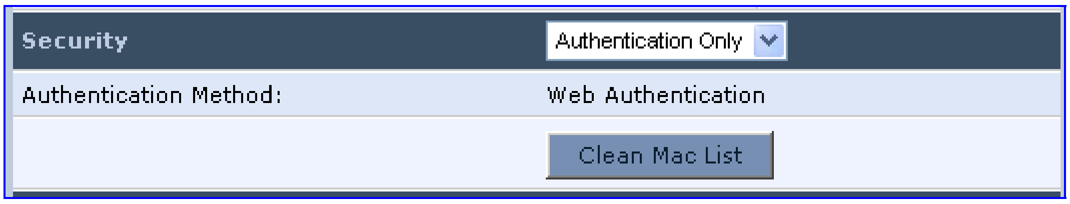
Key index (advanced): 1

☐ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

- **Authentication Only:** wireless clients attempting to connect to the wireless connection will receive MP-20x's main login screen, along with a message. Clients authenticate themselves and are then able to use the connection. MP-20x keeps record of authenticated clients. To clear this list, click the **Clean Mac List** button. Clients will have to re-authenticate themselves to use the wireless connection.

Figure 9-12: Configuring Authentication Only Security



Security: Authentication Only

Authentication Method: Web Authentication

9.3.3 Wireless QoS (WMM)

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance certification based on the IEEE 802.11e draft standard. It provides basic Quality of Service (QoS) features to IEEE 802.11 networks. WMM can be enabled only if your wireless card supports WMM.

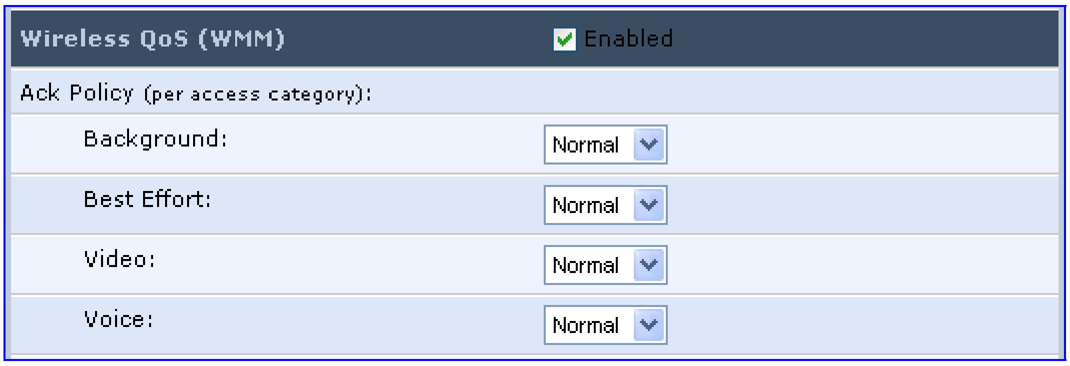
Background, Best Effort, Video, and Voice are access categories for packet prioritization. Upon enabling WMM, the highest priority is given to Voice packets, decreasing towards Background packets which receive the lowest priority. In addition, you can control the reliability of traffic flow.

By default, the 'Ack Policy' for each access category is set to 'Normal', meaning that an Acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. You may choose to cancel the acknowledgement by selecting 'No Ack' in the drop-down list corresponding to each access category, thus changing the Ack policy. This can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.

➢ To enable WMM:

1. In the **Wireless** tab's screen, under the section 'Wireless QoS (WMM)', select the 'Enabled' check box; the screen refreshes.

Figure 9-13: Wireless QoS (WMM)



Wireless QoS (WMM)	✓ Enabled
Ack Policy (per access category):	
Background:	Normal
Best Effort:	Normal
Video:	Normal
Voice:	Normal

2. For each category, select whether an Acknowledge packet is returned for every packet received ('Normal') or no Acknowledge packet is returned ('No Ack').

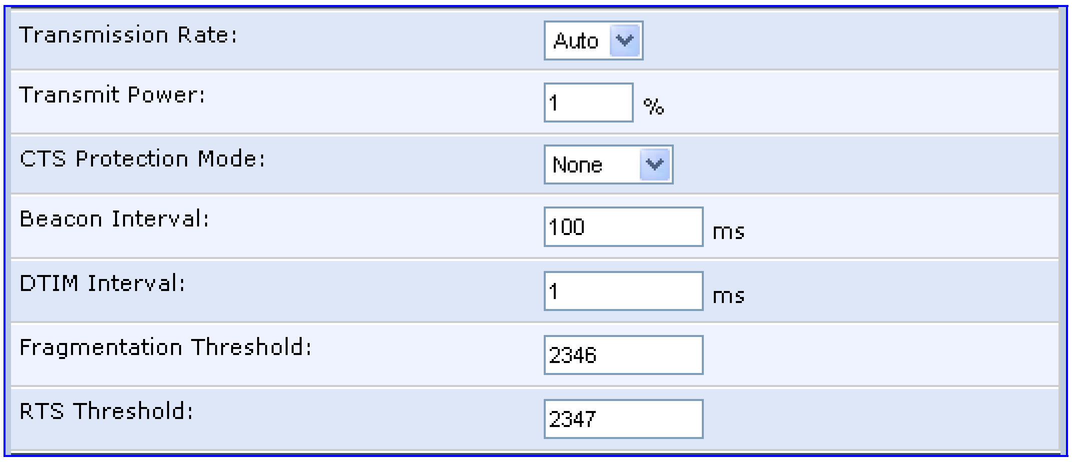
9.3.4 Transmission Properties

Use this section to define the wireless transmission settings.

➢ **To configure the transmission properties:**

1. In the **Wireless** tab's screen, under the section 'Wireless QoS (WMM)', select the 'Enabled' check box; the screen refreshes.

Figure 9-14: Transmission Properties



Transmission Rate:	Auto
Transmit Power:	1 %
CTS Protection Mode:	None
Beacon Interval:	100 ms
DTIM Interval:	1 ms
Fragmentation Threshold:	2346
RTS Threshold:	2347

2. Configure the parameters according to the table below:

Table 9-3: Wireless Tab - Transmission Parameter Descriptions

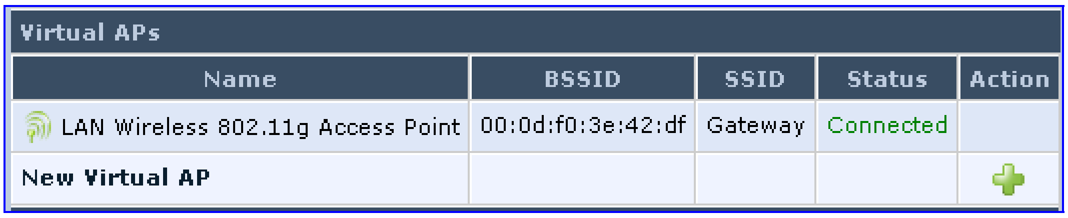
Parameter	Description
Transmission Rate	The transmission rate is set according to the speed of your wireless connection. Select the transmission rate from the drop-down list or select 'Auto' to have MP-20x automatically use the fastest possible data transmission rate. Note that if your wireless connection is weak or unstable, it is best to select a low transmission rate.
Transmit Power	The percentage of maximum transmission power.
CTS Protection Mode	CTS Protection Mode boosts your MP-20x's ability to intercept 802.11g and 802.11b transmissions. Conversely, CTS Protection Mode decreases performance. Leave this feature disabled unless you encounter severe communication difficulties between MP-20x and 802.11g products. If enabling, select 'Always'. Select 'Auto' to have MP-20x automatically decide whether or not to use this feature.
Beacon Interval	A beacon is a packet broadcast by MP-20x to synchronize the wireless network. The Beacon Interval value indicates how often the beacon is sent.
DTIM Interval	The Delivery Traffic Indication Message (DTIM) is a countdown value that informs wireless clients of the next opportunity to receive multicast and broadcast messages. This value ranges between 1 and 16384.

Parameter	Description
Fragmentation Threshold	Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
RTS Threshold	MP-20x sends Request to Send (RTS) packets to the wireless client to negotiate the dispatching of data. The wireless client responds with a Clear to Send (CTS) packet, signaling that transmission can commence. In case packets are smaller than the preset threshold, the RTC/CTS mechanism is not active. If you encounter inconsistent data flow, try a minor reduction of the RTS threshold size.

9.3.5 Virtual Access Points

You can set up multiple virtual wireless LAN's on MP-20x, limited only to the number supported by your wireless card. Such virtual wireless LANs are referred to as "Virtual APs" (virtual access points). In the **Wireless** tab's screen, under the section 'Virtual APs' section, MP-20x's physical wireless access point is displayed first, and on top of which virtual connections may be created.

Figure 9-15: Virtual APs Table



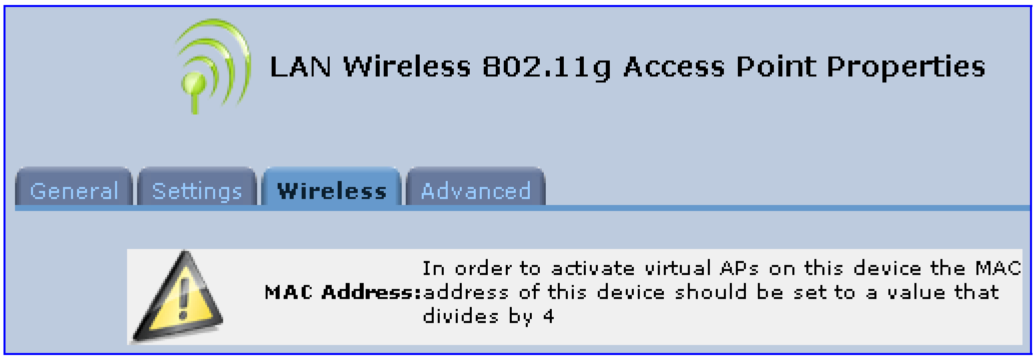
Virtual APs

Name	BSSID	SSID	Status	Action
LAN Wireless 802.11g Access Point	00:0d:f0:3e:42:df	Gateway	Connected	
New Virtual AP				➕

➢ To create a virtual connection:

1. In the **Wireless** tab's screen, under the section 'Virtual APs' section, click the **New Virtual AP** link; a warning message appears.

Figure 9-16: Virtual AP Warning

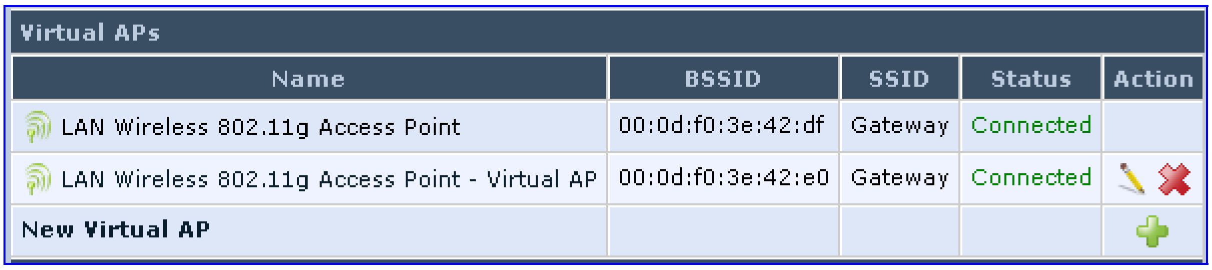


LAN Wireless 802.11g Access Point Properties

MAC Address: In order to activate virtual APs on this device the MAC address of this device should be set to a value that divides by 4

2. Click **OK**; the screen refreshes, displaying the new virtual connection.

Figure 9-17: New Virtual AP



Virtual APs

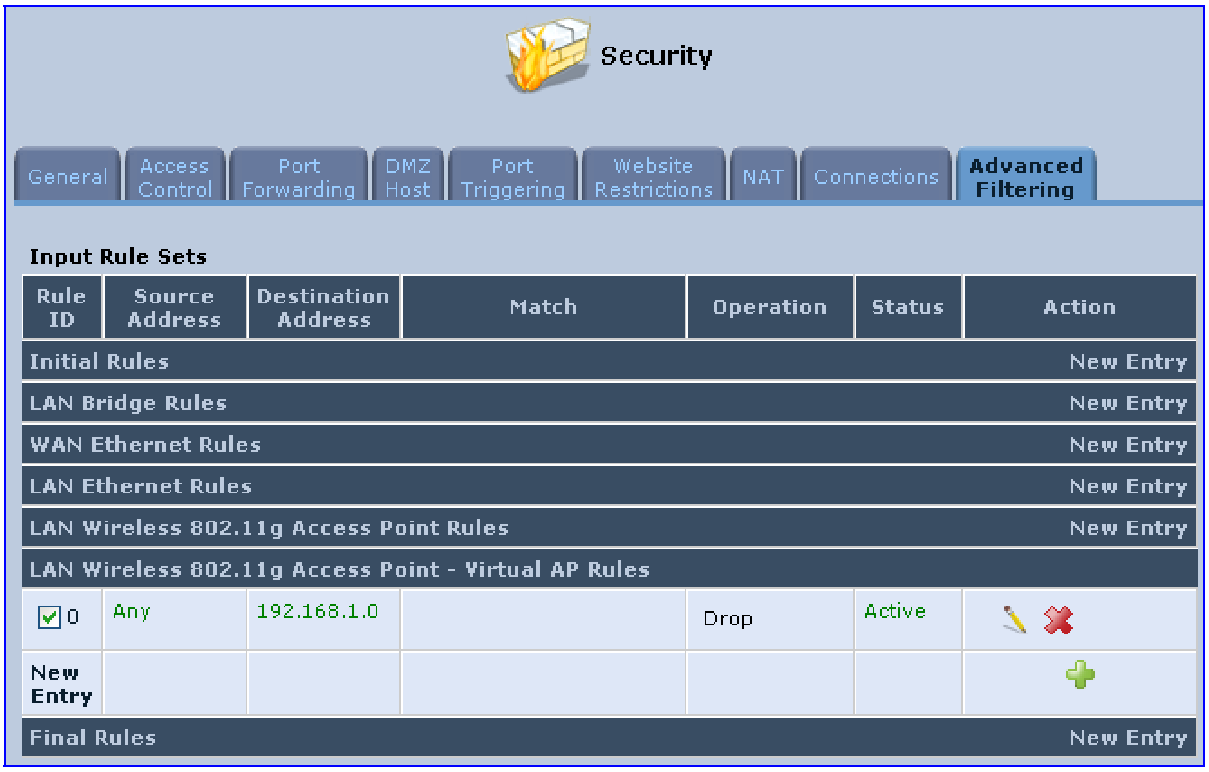
Name	BSSID	SSID	Status	Action
LAN Wireless 802.11g Access Point	00:0d:f0:3e:42:df	Gateway	Connected	
LAN Wireless 802.11g Access Point - Virtual AP	00:0d:f0:3e:42:e0	Gateway	Connected	
New Virtual AP				

The new virtual connection is also added to the list of connections in the 'Network Connections' screen (**Network Connections** menu), and is configurable like any other connection (by clicking its corresponding **Edit** button).

A useful implementation of Virtual AP's is to define a virtual connection with a different SSID value to dedicate it for guest access. Through this connection, guests are able to access the WAN, but they are denied access to other wireless LANs provided by MP-20x. To do so, perform the following:

1. Set a firewall rule that blocks access to all other MP-20x LANs (**Security** menu > **Advanced Filtering** tab).

Figure 9-18: Firewall Blocking Access to All Other LANs



Input Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						New Entry
LAN Bridge Rules						New Entry
WAN Ethernet Rules						New Entry
LAN Ethernet Rules						New Entry
LAN Wireless 802.11g Access Point Rules						New Entry
LAN Wireless 802.11g Access Point - Virtual AP Rules						
✓ 0	Any	192.168.1.0		Drop	Active	
New Entry						
Final Rules						New Entry

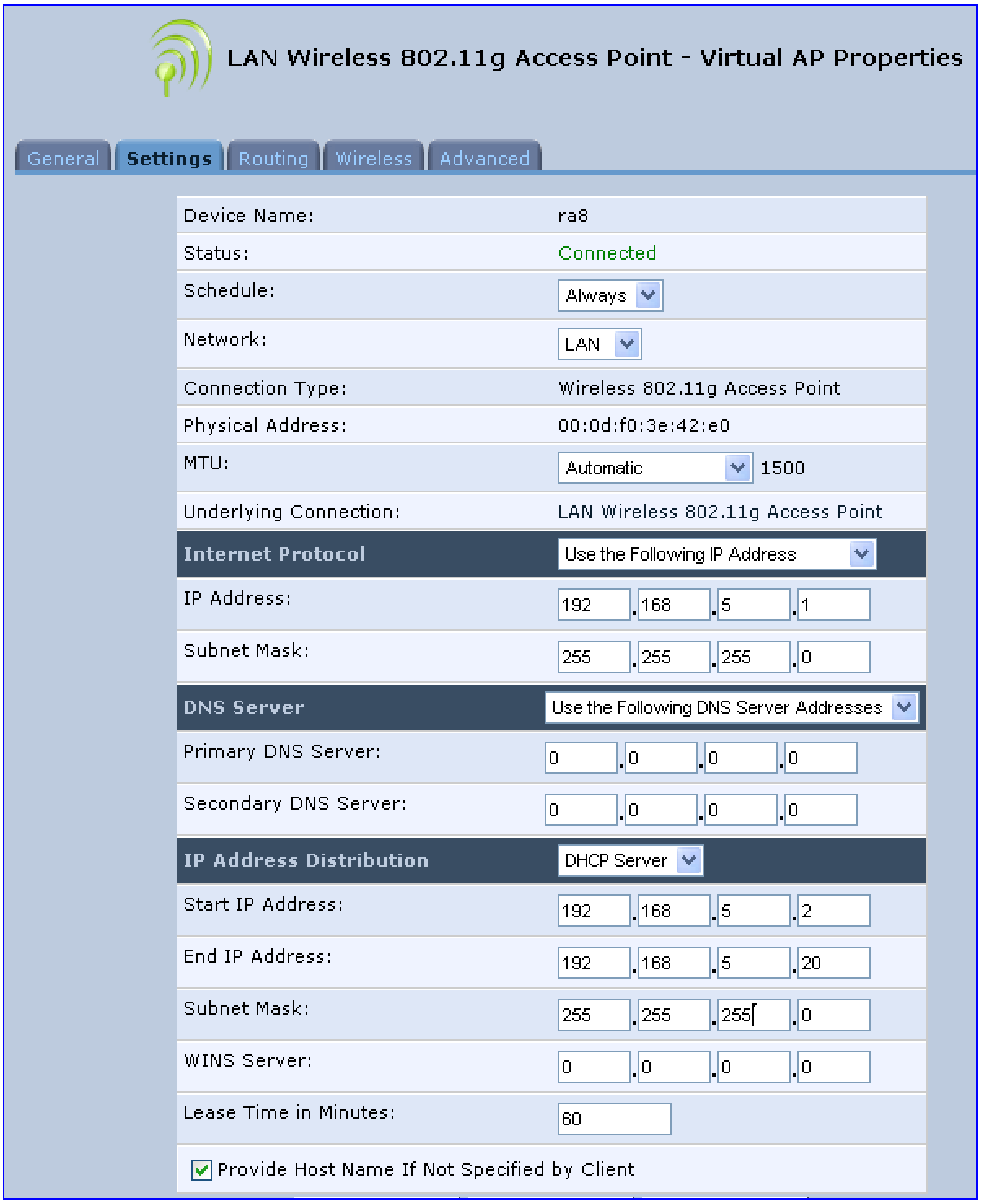
2. In the virtual connection's 'LAN Wireless 802.11g Access Point - Virtual AP Properties' screen:

   a. In the 'Internet Protocol' section under the 'Settings' sub-tab, enter an IP address for the connection by selecting 'Use the Following IP Address'.

b. In the 'IP Address Distribution' section, select 'DHCP Server' and enter the IP range from which IP addresses will be granted to wireless guests.

c. Click **OK**.

Figure 9-19: Example Virtual AP



Device Name:	ra8
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Wireless 802.11g Access Point
Physical Address:	00:0d:f0:3e:42:e0
MTU:	Automatic 1500
Underlying Connection:	LAN Wireless 802.11g Access Point
Internet Protocol	Use the Following IP Address
IP Address:	192.168.5.1
Subnet Mask:	255.255.255.0
DNS Server	Use the Following DNS Server Addresses
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
IP Address Distribution	DHCP Server
Start IP Address:	192.168.5.2
End IP Address:	192.168.5.20
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	

After performing this procedure, you have secured all of your wireless connections. A guest is only able to connect to the "Guests" wireless LAN, from which only the WAN access is granted.

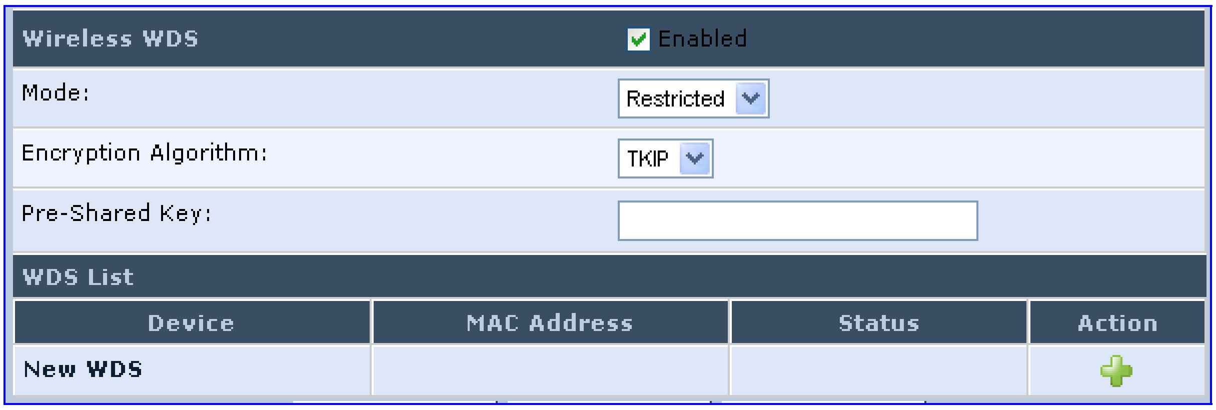
9.3.6 Wireless Distribution System

MP-20x supports Wireless Distribution System (WDS), which enables wireless bridging of access points within its range. Virtual access points are used to interact with MP-20x's WDS peers, granting LAN users access to remote wireless networks.

➢ To enable WDS:

1. In the **Wireless** tab's screen, under the section 'Wireless WDS' section, select the 'Enabled' check box; the screen refreshes, displaying additional fields.

Figure 9-20: Wireless WDS



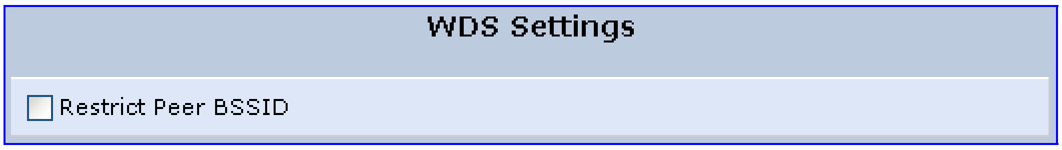
Wireless WDS	✓ Enabled
Mode:	Restricted
Encryption Algorithm:	TKIP
Pre-Shared Key:	

WDS List

Device	MAC Address	Status	Action
New WDS			✚

2. From the 'Mode' drop-down list, select the WDS mode of operation:
   - **Restricted:** WDS peers must be registered with MP-20x (by MAC addresses).
   - **Bridge:** MP-20x functions as a wireless bridge, merely forwarding traffic between access points, and does not respond to wireless requests. The WDS peers must be manually stated and wireless stations cannot connect to MP-20x.
   - **Repeater:** MP-20x acts as a repeater, interconnecting between access points. WDS peers can be determined by the user ('Restricted' mode) or auto-detected ('Lazy' mode).
   - **Lazy:** automatic detection of WDS peers: when a LAN user searches for a network, MP-20x attempts to connect to WDS devices in its vicinity.
3. From the 'Encryption Algorithm' drop-down list, select the encryption algorithms available for encrypting the communication between access points (this is only when wireless security is enabled).
4. Add a WDS device, by performing the following:
   a. In the 'WDS List' table, click the **New WDS** link; the 'WDS Settings' screen appears.

Figure 9-21: WDS Settings Screen



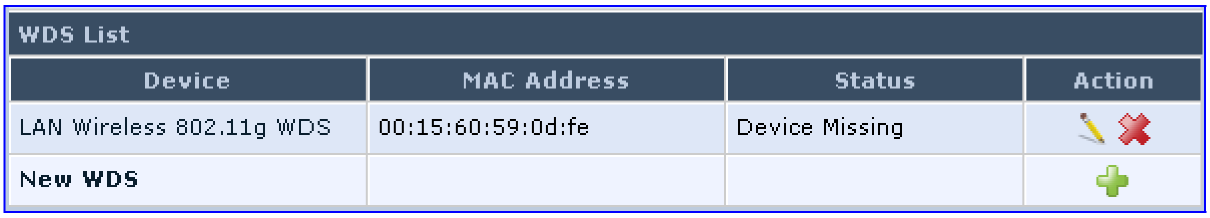
WDS Settings

☐ Restrict Peer BSSID

   b. Select the 'Restrict Peer BSSID' check box, and then enter the MAC address of the WDS peer with which this virtual access point is to interact.

c. Click **OK**; a new virtual device appears in the 'WDS List' table, with the initial status of disabled.

Figure 9-22: New WDS in WDS List Table



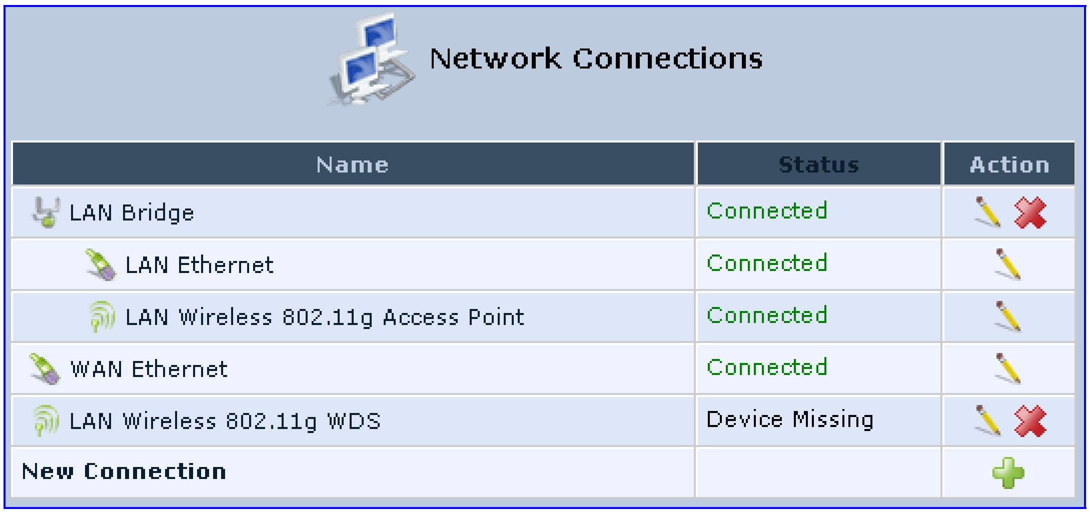
WDS List

Device	MAC Address	Status	Action
LAN Wireless 802.11g WDS	00:15:60:59:0d:fe	Device Missing	
New WDS			

Note that devices added to the 'WDS List' table before the WDS feature is enabled in the main device appears as missing.

d. Click **OK**; the new virtual 'LAN Wireless 802.11g WDS' connection is listed In the 'Network Connections' screen (**Network Connections** menu).

Figure 9-23: LAN Wireless 802.11g WDS Properties Screen



Network Connections

Name	Status	Action
LAN Bridge	Connected	
LAN Ethernet	Connected	
LAN Wireless 802.11g Access Point	Connected	
WAN Ethernet	Connected	
LAN Wireless 802.11g WDS	Device Missing	
New Connection		

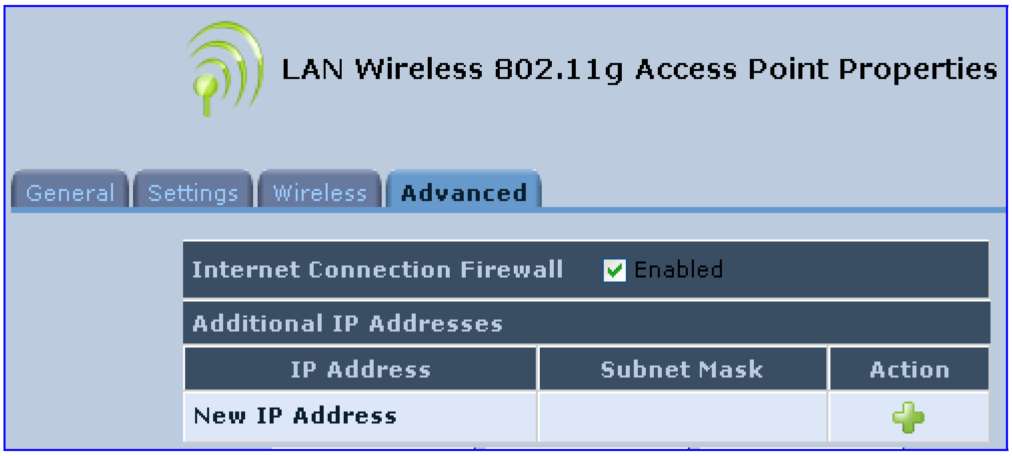
e. Click the virtual connection's **Edit** icon; the 'LAN Wireless 802.11g WDS Properties' screen reappears.

f. Click the **Enable** button; the virtual connection is now enabled.

If the WDS peer also operates in 'Restricted' mode, it should similarly be configured with MP-20x's MAC address for both access points to communicate.

9.4 Advanced Tab

The **Advanced** tab allows you to enable your firewall on your wireless network connection as well as define alias names.


LAN Wireless 802.11g Access Point Properties

Internet Connection Firewall ✓ Enabled

Additional IP Addresses

IP Address	Subnet Mask	Action
New IP Address		✚

Internet Connection Firewall: Your MP-20x'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.

Additional IP Addresses: You can add alias names (additional IP addresses) to MP-20x by clicking the **New IP Address** link. This enables you to access MP-20xusing these aliases in addition to the 192.168.1.1 and the http://mp202.home.

10 WAN Settings

You can change the WAN mode from its default connection type (Ethernet), using one of the following methods:

- 'Quick Setup' screen (**Quick Setup** menu): use the 'Connection Type' drop-down list.
- 'Network Connections' screen (**Network Connections** menu): click the link **New Connection**, select the 'Advanced Connection' option, and then choose the connection type.

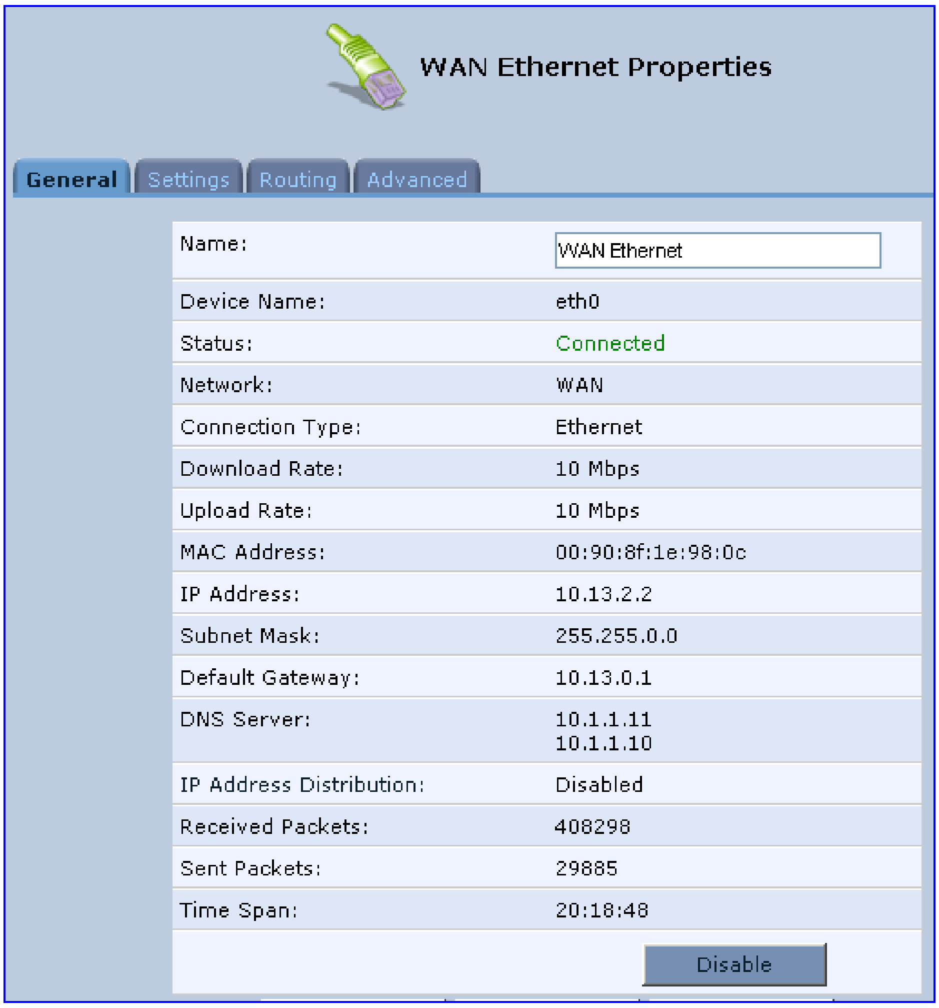
10.1 WAN Ethernet

WAN Ethernet is the default mode. WAN Ethernet is used to connect MP-20x to the network either directly or via an external modem.

➢ To access its properties:

- From the sidebar menu, click the **Network Connections** menu, and in the screen 'Network Connections', click the **Edit** icon corresponding to the 'WAN Ethernet' connection name; the screen 'WAN Ethernet Properties' opens.

Figure 10-1: WAN Ethernet Properties

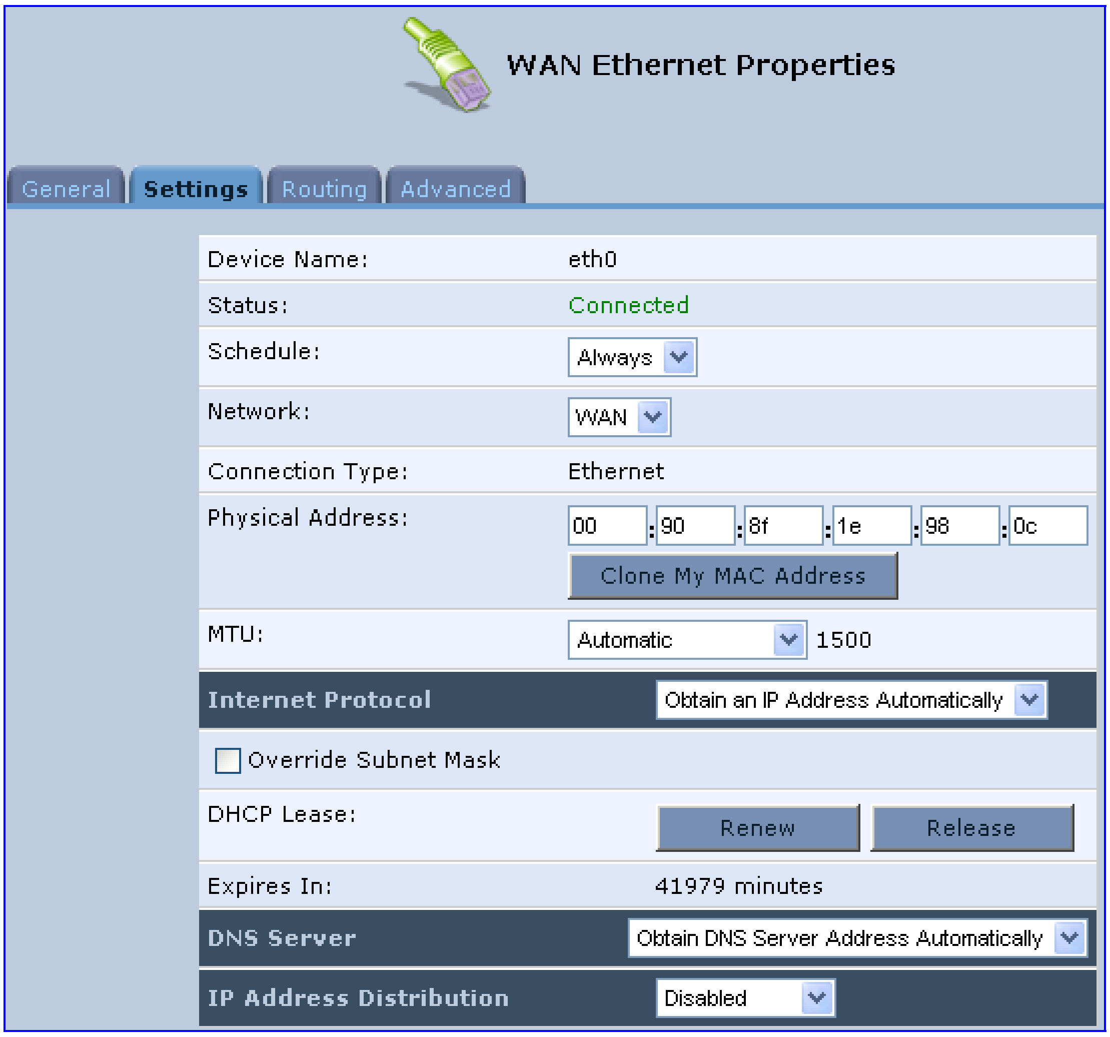


Name:	WAN Ethernet
Device Name:	eth0
Status:	Connected
Network:	WAN
Connection Type:	Ethernet
Download Rate:	10 Mbps
Upload Rate:	10 Mbps
MAC Address:	00:90:8f:1e:98:0c
IP Address:	10.13.2.2
Subnet Mask:	255.255.0.0
Default Gateway:	10.13.0.1
DNS Server:	10.1.1.11 10.1.1.10
IP Address Distribution:	Disabled
Received Packets:	408298
Sent Packets:	29885
Time Span:	20:18:48

➢ **To configure the WAN Ethernet connection:**

- In the 'WAN Ethernet Properties' screen, click the **Settings** tab; the following screen opens:

Figure 10-2: WAN Ethernet Configuration



Device Name: eth0
Status: Connected
Schedule: Always
Network: WAN
Connection Type: Ethernet
Physical Address: 00 : 90 : 8f : 1e : 98 : 0c
MTU: Automatic 1500
Internet Protocol: Obtain an IP Address Automatically
☐ Override Subnet Mask
DHCP Lease:
Expires In: 41979 minutes
DNS Server: Obtain DNS Server Address Automatically
IP Address Distribution: Disabled

10.1.1 Settings Tab

The top part of the screen 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 10-1: Settings Tab - 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).

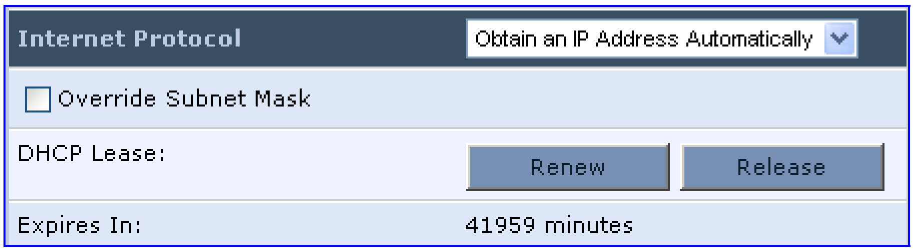
Parameter	Description
Network	Select whether the parameters you are configuring relate to a LAN/WAN/DMZ connection, by selecting LAN/WAN from the drop down list.
Physical Address	The physical address of the network card used for your network. Some cards allow you to change this address.
Clone My MAC Address	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.

10.1.1.1 Internet Protocol Settings

The 'Internet Protocol' group defines the Internet Protocol options. Select one of the following Internet Protocol options from the 'Internet Protocol' drop-down list:

- **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.

Figure 10-3: Automatically Obtaining an IP Address



Internet Protocol: Obtain an IP Address Automatically

Override Subnet Mask

DHCP Lease:

Expires In: 41959 minutes

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' check box and specifying your own mask instead.

You can click 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.

Note that according to the selection above, the screen refreshes and displays relevant configuration parameters.

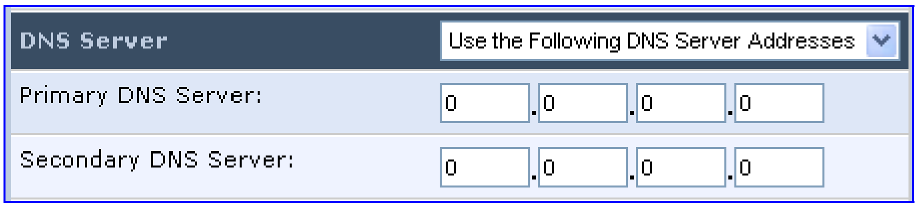
10.1.1.2 DNS Server

Domain Name System (DNS) is the method by which websites 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.

From the 'DNS Server' drop-down list, you can select one of the following methods:

- **Obtain DNS Server Address Automatically:** to configure the connection to automatically obtain a DNS server address.
- **Use the Following DNS Server Addresses:** to manually configure DNS server addresses, and then specify up to two different DNS server addresses - one primary, the other secondary:

Figure 10-4: Manually Defining DNS Server

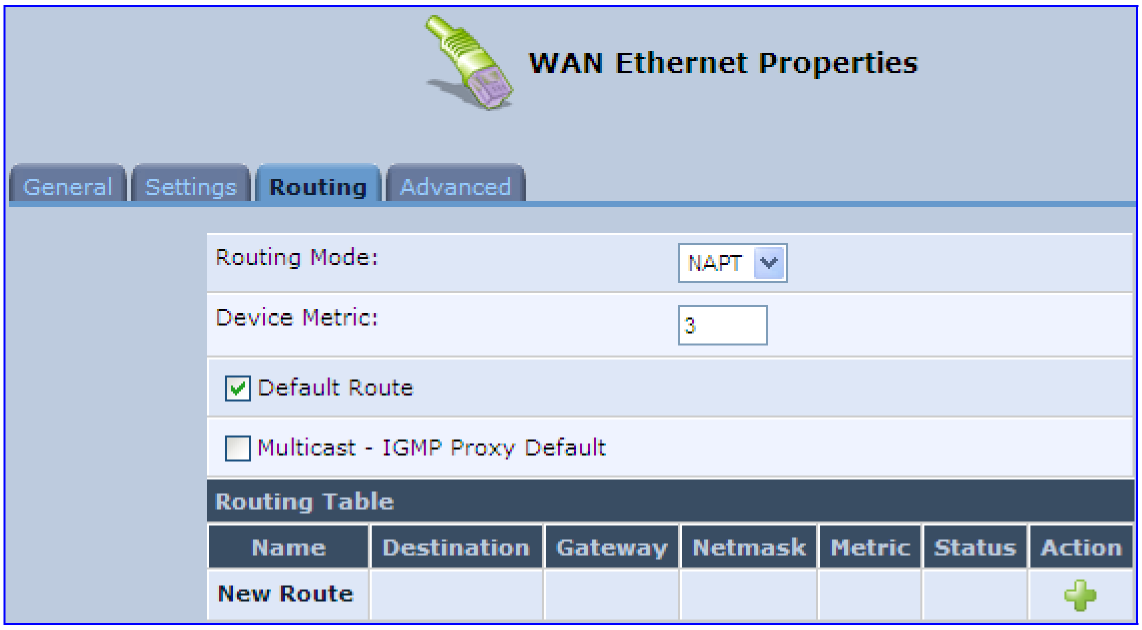


DNS Server	Use the Following DNS Server Addresses
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

10.1.2 Routing Tab

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.

Figure 10-5: Routing Tab (WAN)



Routing Mode:	NAPT
Device Metric:	3

[✓] Default Route

[ ] Multicast - IGMP Proxy Default

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						✚

Table 10-2: Routing Parameters

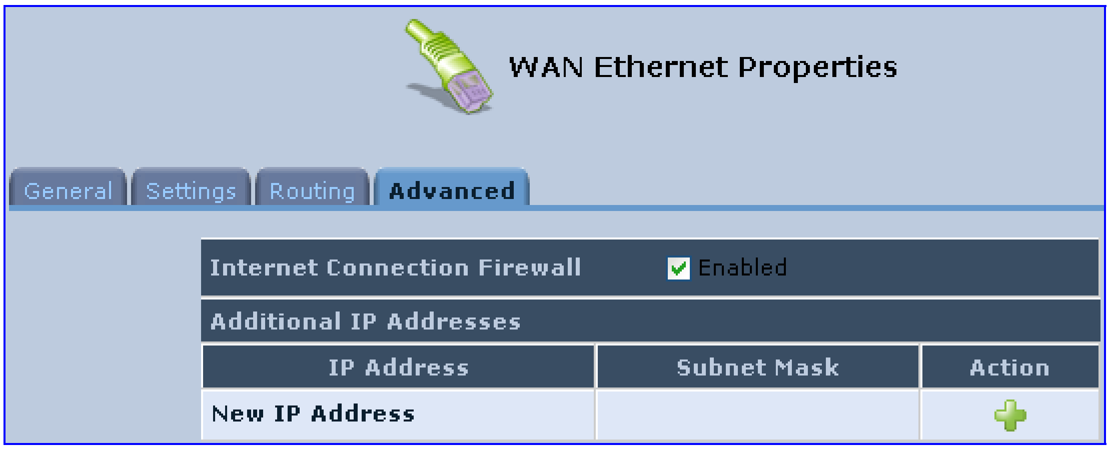
Parameter	Description

Parameter	Description	
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.
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.	
Multicast - IGMP Proxy Default	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 Default' 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.	

10.1.3 Advanced Tab

The Advanced tab is shown below: .

Figure 10-6: Internet Connection Firewall



Internet Connection Firewall ✓ Enabled

Additional IP Addresses

IP Address	Subnet Mask	Action
New IP Address		✚

Internet Connection Firewall: Your MP-20x’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 177.

Additional IP Addresses: You can add alias names (additional IP addresses) to MP-20x by clicking the **New IP Address** link. This enables you to access MP-20x using these aliases in addition to the 192.168.1.1 and the http://mp202.home.

10.2 WAN PPPoE

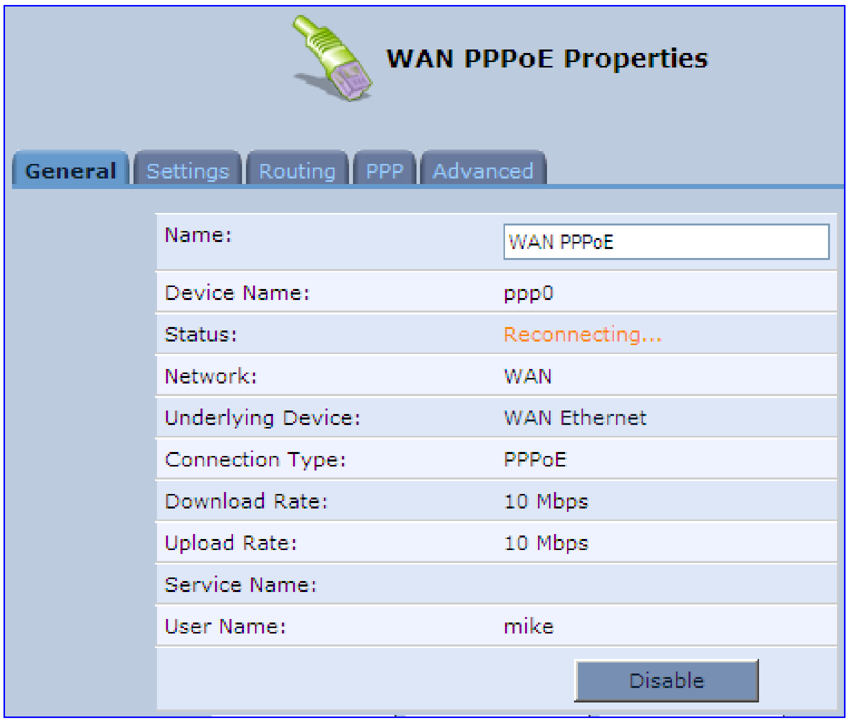
Point-to-Point Protocol over Ethernet (PPPoE) relies on two widely accepted standards, PPP and Ethernet. PPPoE enables your home network PCs that communicate on an Ethernet network to exchange information with PCs on the Internet. PPPoE supports the protocol layers and authentication widely used in PPP 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.

10.2.1 General

Table 10-3: 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 for transmitting. 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 is initiated.

Figure 10-7: General PPPoE Settings



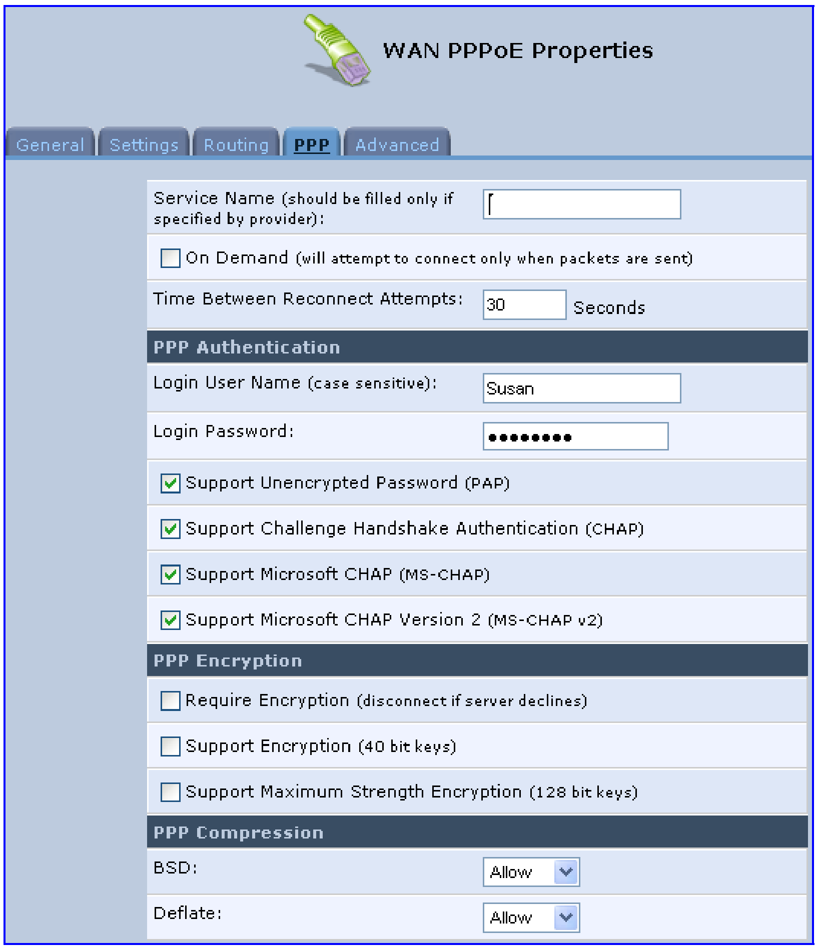
Name:	WAN PPPoE
Device Name:	ppp0
Status:	Reconnecting...
Network:	WAN
Underlying Device:	WAN Ethernet
Connection Type:	PPPoE
Download Rate:	10 Mbps
Upload Rate:	10 Mbps
Service Name:	
User Name:	mike

10.2.2 PPP Tab

The **PPT** tab displays the PPPoE settings.

➢ **To configure the WAN Ethernet - PPPoE properties**

- In the 'WAN Ethernet Properties' screen, click the **PPP** tab; the following screen opens:



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

PPP Authentication

Login User Name (case sensitive): Susan

Login Password: ●●●●●●●●●

☑ Support Unencrypted Password (PAP)

☑ Support Challenge Handshake Authentication (CHAP)

☑ Support Microsoft CHAP (MS-CHAP)

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

PPP Encryption

☐ Require Encryption (disconnect if server declines)

☐ Support Encryption (40 bit keys)

☐ Support Maximum Strength Encryption (128 bit keys)

PPP Compression

BSD: Allow

Deflate: Allow

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 10-4: 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.

10.2.2.1 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 MP-20x 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.

Table 10-5: 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.

10.2.2.2 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.

Table 10-6: 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.

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

Table 10-7: 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.

10.2.3 Internet Protocol

Refer to 'Settings Tab' on page 106.

10.2.4 DNS Server

Refer to 'Settings Tab' on page 106.

10.2.5 Routing

Refer to 'Routing Tab' on page 108.

10.2.6 Internet Connection Firewall

Refer to 'Advanced Tab' on page 109.

10.3 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 MP-20x 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 MP-20x, PPTP is targeted at serving two purposes:

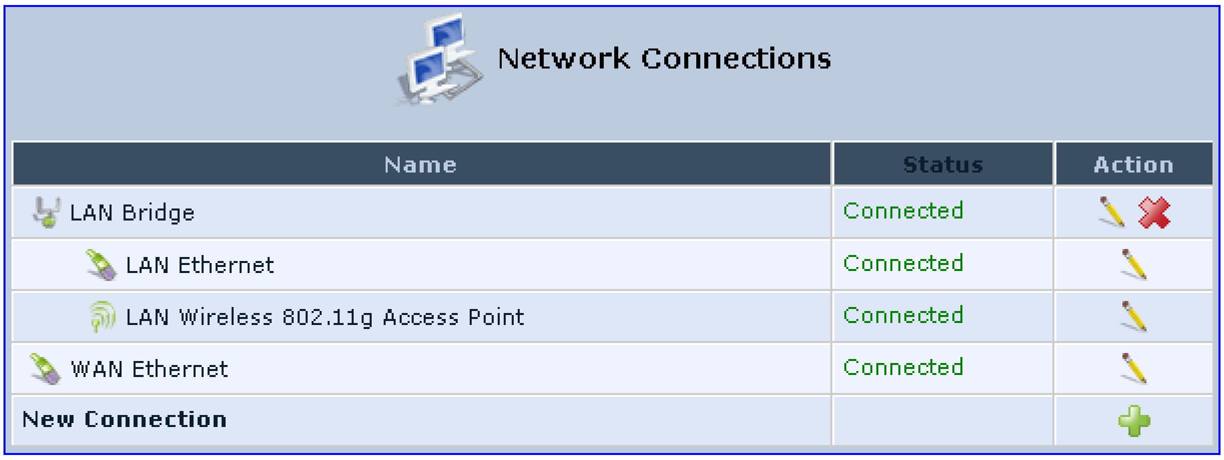
1. Connecting MP-20x to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established using user name and password authentication.
2. Connecting MP-20x to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, using user name and password authentication.

10.3.1 Creating a PPTP Connection with the Connection Wizard

➢ To create a new PPTP connection:

1. From the sidebar menu, click the **Network Connections** menu; the screen 'Network Connections' opens.

Figure 10-8: Network Connections Screen

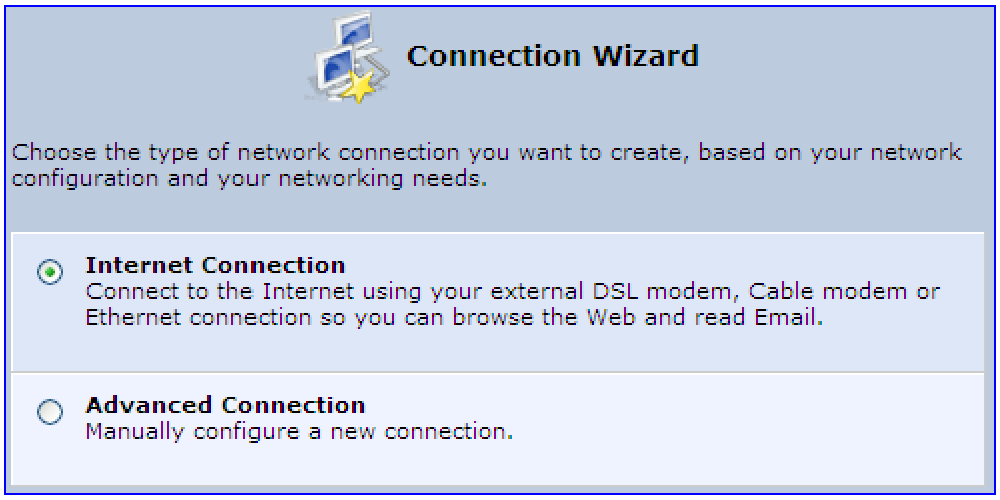


Network Connections

Name	Status	Action
LAN Bridge	Connected	✎ ✖
LAN Ethernet	Connected	✎
LAN Wireless 802.11g Access Point	Connected	✎
WAN Ethernet	Connected	✎
New Connection		✚

2. Click the link **New Connection**; the 'Connection Wizard' screen opens.

Figure 10-9: Connection Wizard Screen



Connection Wizard

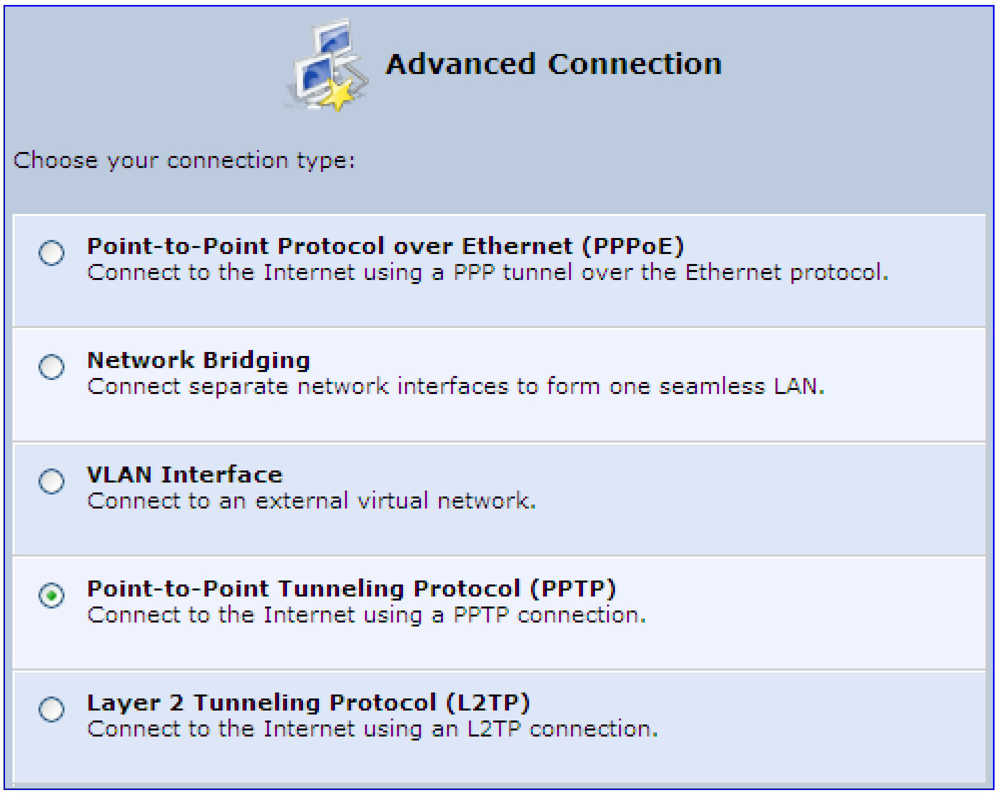
Choose the type of network connection you want to create, based on your network configuration and your networking needs.

[✓ **Internet Connection**]
Connect to the Internet using your external DSL modem, Cable modem or Ethernet connection so you can browse the Web and read Email.

Advanced Connection
Manually configure a new connection.

3. Select the 'Advanced Connection' option, and then click **Next**; the screen 'Internet Connection' opens.

Figure 10-10: Advanced Connection



Advanced Connection

Choose your connection type:

Point-to-Point Protocol over Ethernet (PPPoE)
Connect to the Internet using a PPP tunnel over the Ethernet protocol.

Network Bridging
Connect separate network interfaces to form one seamless LAN.

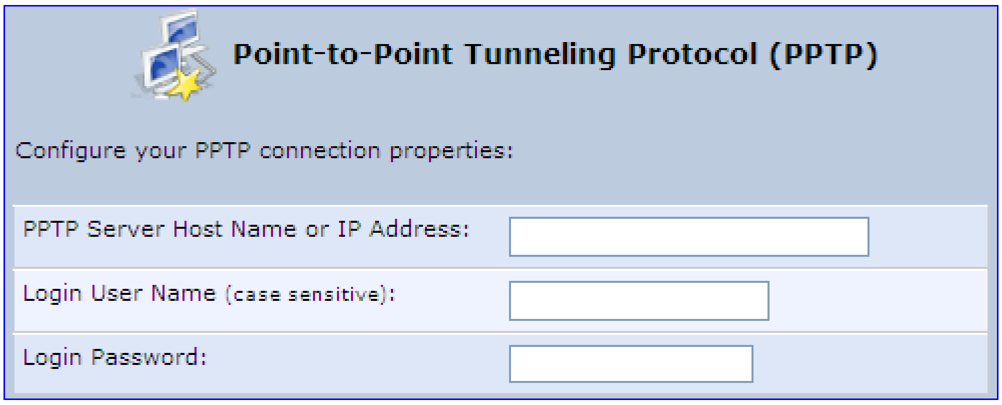
VLAN Interface
Connect to an external virtual network.

[✓ **Point-to-Point Tunneling Protocol (PPTP)**]
Connect to the Internet using a PPTP connection.

Layer 2 Tunneling Protocol (L2TP)
Connect to the Internet using an L2TP connection.

4. Select the ‘Point-to-Point Tunneling Protocol (PPTP)’ option ,and then click **Next**; the screen ‘Point-to-Point Tunneling Protocol (PPTP)’ opens.

Figure 10-11: Point-to-Point Tunneling Protocol (PPTP) Screen

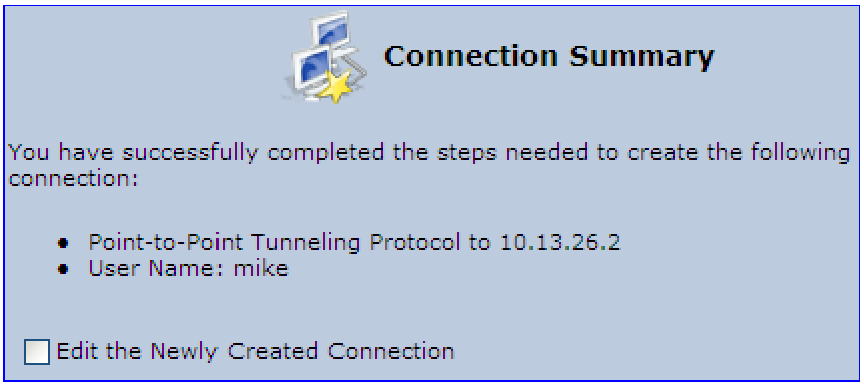

Point-to-Point Tunneling Protocol (PPTP)

Configure your PPTP connection properties:

PPTP Server Host Name or IP Address:	
Login User Name (case sensitive):	
Login Password:	

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. Click **Next**; the screen 'Connection Summary' opens.

Figure 10-12: Connection Summary


Connection Summary

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

- Point-to-Point Tunneling Protocol to 10.13.26.2
- User Name: mike

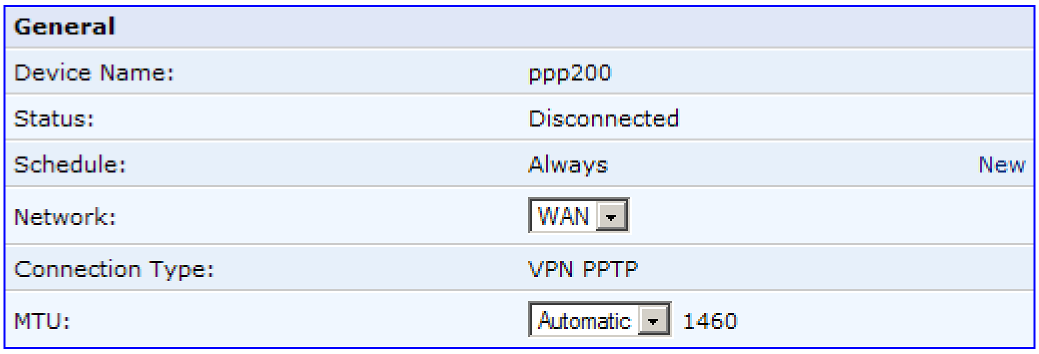
☐ Edit the Newly Created Connection

8. 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**.
9. Click **Finish** to save the settings; the new PPTP connection is added to the network connections list and is configurable like any other connection.

10.3.2 General

This section displays the connection's general parameters.

Figure 10-13: General PPTP Settings



General

Device Name: ppp200

Status: Disconnected

Schedule: Always New

Network: WAN

Connection Type: VPN PPTP

MTU: Automatic 1460

Table 10-8: 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), MP-20x 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.

10.3.3 PPP Configuration

Refer to 'PPP Tab' on page 110.

10.3.4 PPP Authentication

Refer to 'PPP Tab' on page 110.

10.3.5 PPP Encryption

Refer to 'PPP Tab' on page 110.

10.3.6 Internet Protocol

Refer to 'Settings Tab' on page 106.

10.3.7 DNS Server

Refer to 'Settings Tab' on page 106.

10.3.8 Routing

Refer to 'Routing Tab' on page 108.

10.3.9 Internet Connection Firewall

Refer to 'Advanced Tab' on page 109.

10.4 WAN L2TP

Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol, enabling your MP-20x 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 MP-20x, L2TP is targeted at serving two purposes:

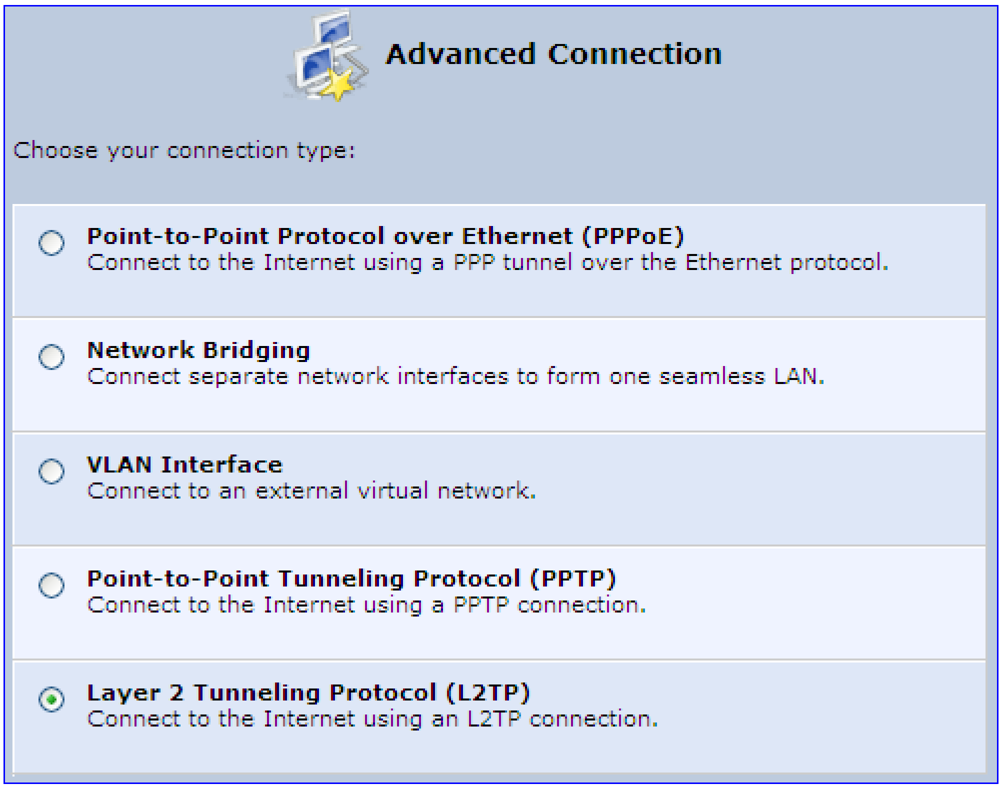
1. Connecting MP-20x to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established using user name and password authentication.
2. Connecting MP-20x to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables 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.

➢ To create a new L2TP connection:

1. From the sidebar menu, click the **Network Connections** menu; the screen 'Network Connections' opens.
2. Click the link **New Connection**; the 'Connection Wizard' screen opens.

3. Select the 'Advanced Connection' option, and then click **Next**; the screen 'Advanced Connection' opens.

Figure 10-14: VPN Client or Point-To-Point


Advanced Connection

Choose your connection type:

◯ **Point-to-Point Protocol over Ethernet (PPPoE)**
Connect to the Internet using a PPP tunnel over the Ethernet protocol.

◯ **Network Bridging**
Connect separate network interfaces to form one seamless LAN.

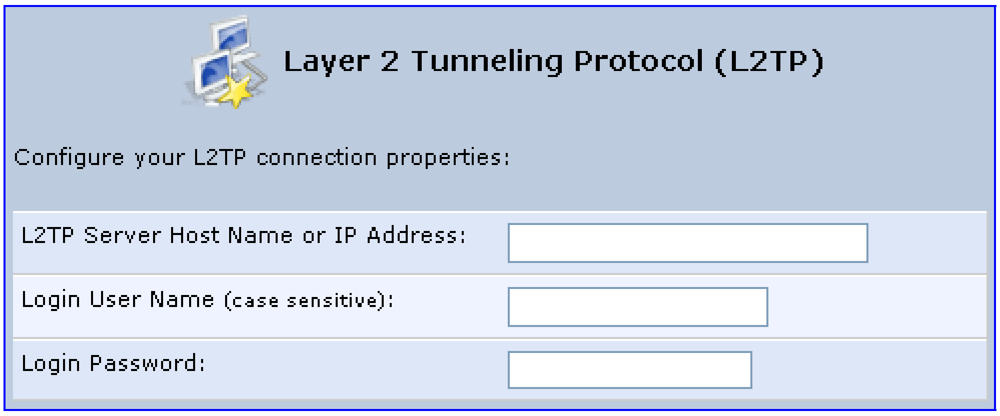
◯ **VLAN Interface**
Connect to an external virtual network.

◯ **Point-to-Point Tunneling Protocol (PPTP)**
Connect to the Internet using a PPTP connection.

[✓ **Layer 2 Tunneling Protocol (L2TP)**]
Connect to the Internet using an L2TP connection.

4. Select the 'Layer 2 Tunneling Protocol (L2TP)' option, and then click **Next**; the screen 'Layer 2 Tunneling Protocol (L2TP)' opens.

Figure 10-15: Layer 2 Tunneling Protocol (L2TP)


Layer 2 Tunneling Protocol (L2TP)

Configure your L2TP connection properties:

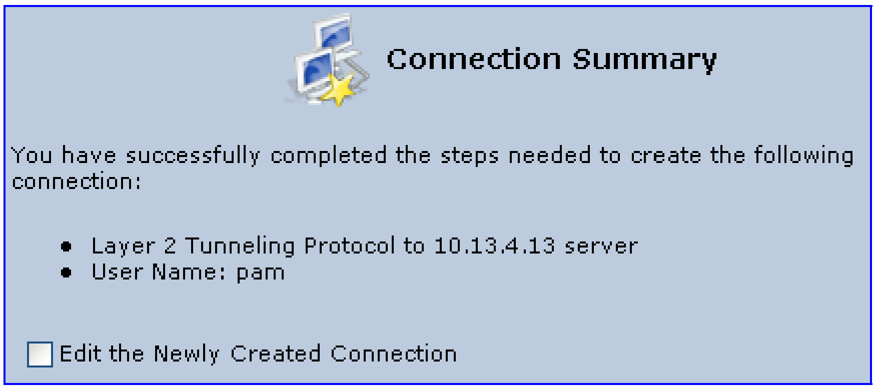
L2TP Server Host Name or IP Address:	
Login User Name (case sensitive):	
Login Password:	

5. Enter the login user name 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.

Figure 10-16: Connection Summary



Connection Summary

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

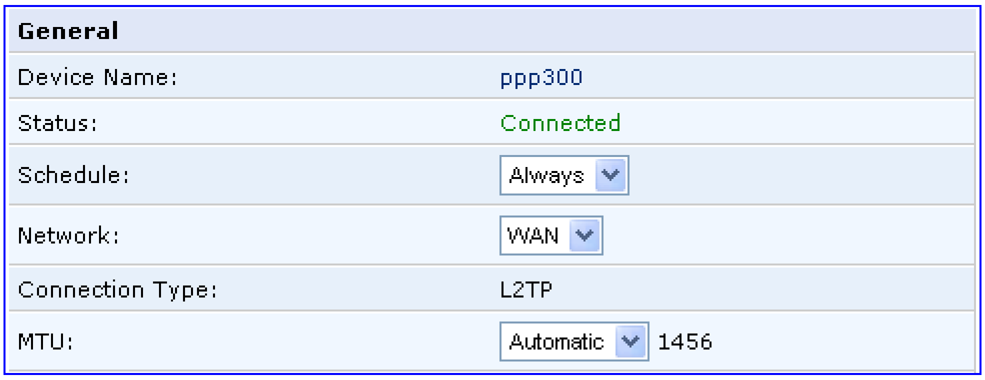
- Layer 2 Tunneling Protocol to 10.13.4.13 server
- User Name: pam

☐ Edit the Newly Created Connection

8. Select the check box 'Edit the Newly Created Connection' to be routed to the new connection's configuration screen after clicking **Finish**.
9. Click **Finish** to save the settings; the new L2TP VPN connection is added to the network connections list and is configurable like any other connection.

10.4.1 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 10-9: 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), MP-20x 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.

10.4.2 PPP Configuration

Refer to 'PPP Tab' on page 110.

10.4.3 PPP Authentication

Refer to 'PPP Tab' on page 110.

10.4.4 PPP Encryption

Refer to 'PPP Tab' on page 110.

10.4.5 PPP Compression

Refer to 'PPP Tab' on page 110.

10.4.6 Internet Protocol

Refer to 'Settings Tab' on page 106.

10.4.7 DNS Server

Refer to 'Settings Tab' on page 106.

10.4.8 Routing

Refer to 'Routing Tab' on page 108.

10.4.9 Internet Connection Firewall

Refer to 'Advanced Tab' on page 109.

Reader’s Notes

11 VLAN and Bridge Settings

Note: Currently, the MP-202C model does not support VLANs.

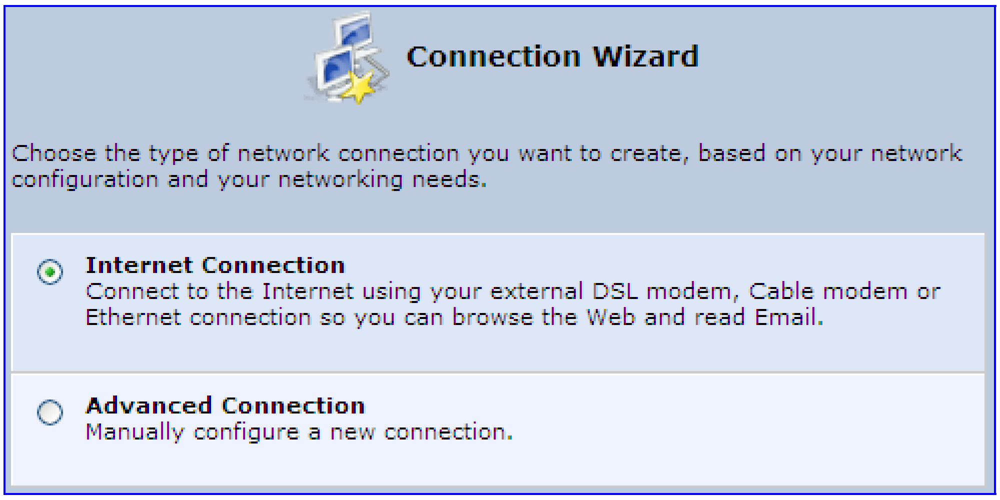
11.1 Virtual LAN Interface (VLAN)

11.1.1 Creating with the Connection Wizard

➢ **To create a new VLAN interface:**

1. From the sidebar menu, click the **Network Connections** menu, and in the screen 'Network Connections' click the **New Connection** link; the 'Connection Wizard' screen opens.

Figure 11-1: Connection Wizard Screen



Connection Wizard

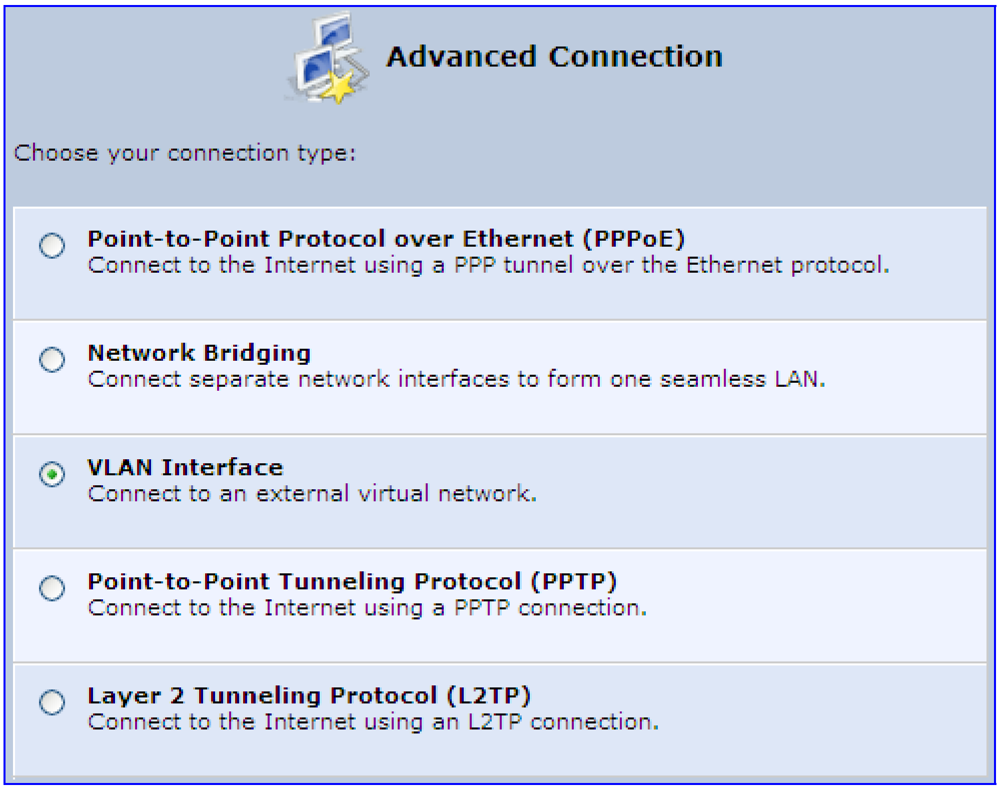
Choose the type of network connection you want to create, based on your network configuration and your networking needs.

[✓ **Internet Connection**]
Connect to the Internet using your external DSL modem, Cable modem or Ethernet connection so you can browse the Web and read Email.

Advanced Connection
Manually configure a new connection.

2. Select the 'Advanced Connection' option, and then click **Next**; the 'Advanced Connection' screen appears.

Figure 11-2: VPN Client or Point-To-Point

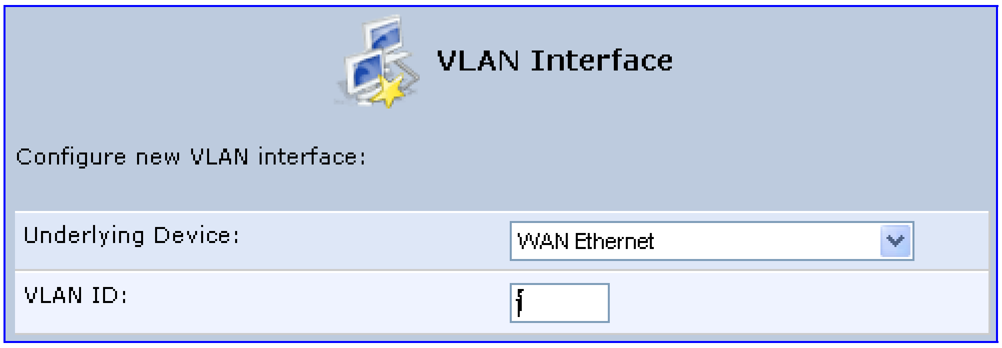

Advanced Connection

Choose your connection type:

- ○ **Point-to-Point Protocol over Ethernet (PPPoE)** Connect to the Internet using a PPP tunnel over the Ethernet protocol.
- ○ **Network Bridging** Connect separate network interfaces to form one seamless LAN.
- ◉ **VLAN Interface** Connect to an external virtual network.
- ○ **Point-to-Point Tunneling Protocol (PPTP)** Connect to the Internet using a PPTP connection.
- ○ **Layer 2 Tunneling Protocol (L2TP)** Connect to the Internet using an L2TP connection.

3. Select the 'VLAN Interface' option, and then click **Next**; the 'VLAN Interface' screen appears.

Figure 11-3: VLAN Interface


VLAN Interface

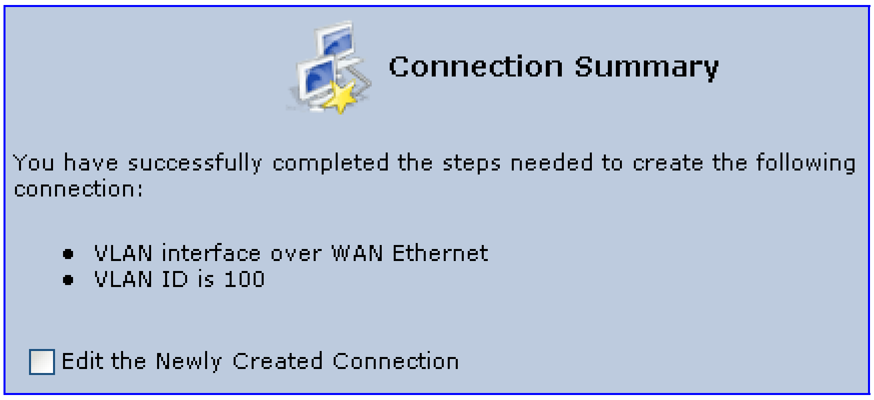
Configure new VLAN interface:

Underlying Device:	WAN Ethernet
VLAN ID:	

4. From the 'Underlying Device' drop-down list, select the underlying device (device's Ethernet connections) for this interface.

5. In the 'VLAN ID' field, enter a value to serve as the VLAN ID, and then click **Next**; the 'Connection Summary' screen appears.

Figure 11-4: Connection Summary



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

- VLAN interface over WAN Ethernet
- VLAN ID is 100

☐ Edit the Newly Created 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.

11.1.2 Settings Tab

The **Settings** tab of the 'VLAN Properties' 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 11-1: VLAN Interface - General Communication Parameters

Parameter	Description
Schedule	By default, the connection is always 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 drop-down list, 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 drop-down list. 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 refreshes and displays 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.
- **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 click 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.

11.1.2.1.1 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.

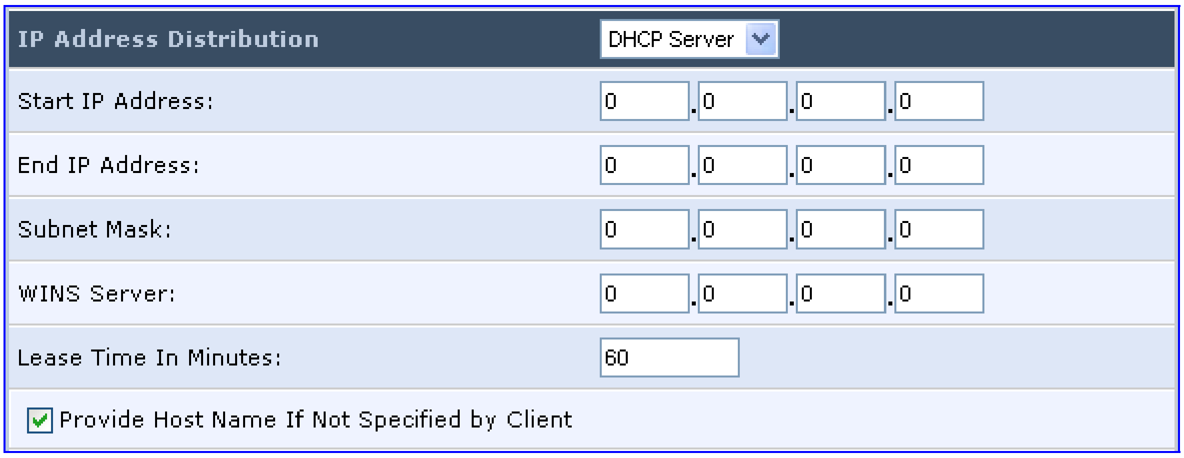
Select one of the following options from the 'IP Address Distribution' drop-down list:

Table 11-2: 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 is 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 determines 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 become available for other computers on the network.

Parameter	Description
Provide Host Name If Not Specified by Client	If the DHCP client does not have a host name, the device automatically assigns one for him.

Figure 11-5: IP Address Distribution - DHCP Server



IP Address Distribution: DHCP Server

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

WINS Server: 0 . 0 . 0 . 0

Lease Time In Minutes: 60

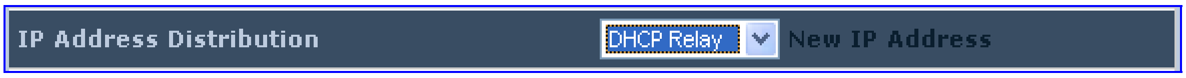
✓ Provide Host Name If Not Specified by Client

Table 11-3: DHCP Relay

Parameter	Description
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 list, a **New IP Address** link appears:

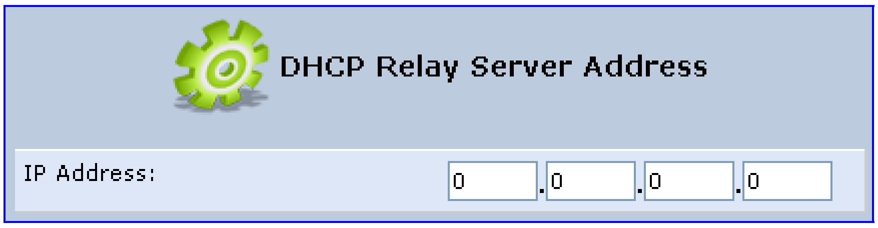
Figure 11-6: IP Address Distribution - DHCP Relay



IP Address Distribution: DHCP Relay New IP Address

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

Figure 11-7: DHCP Relay Server Address



DHCP Relay Server Address

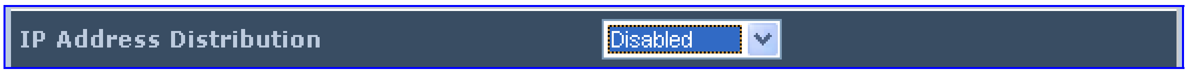
IP Address: 0 . 0 . 0 . 0

3. Specify the IP address of the DHCP server.
4. Click **OK** to save the settings.

Table 11-4: Assigning Static IP Addresses to Network Computers

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

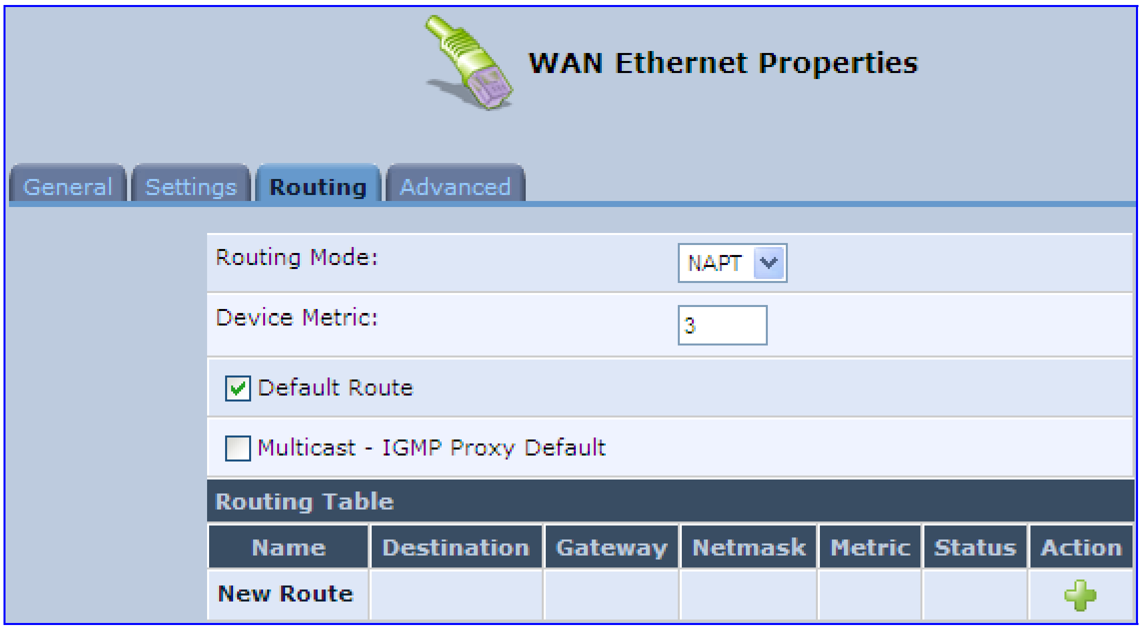
Figure 11-8: IP Address Distribution - Disable DHCP


IP Address Distribution: Disabled

11.1.3 Routing Tab

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.

Figure 11-9: Advanced Routing Properties


WAN Ethernet Properties

Routing Mode: NAPT

Device Metric: 3

[✓] Default Route

[ ] Multicast - IGMP Proxy Default

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						✚

Table 11-5: Routing Parameters

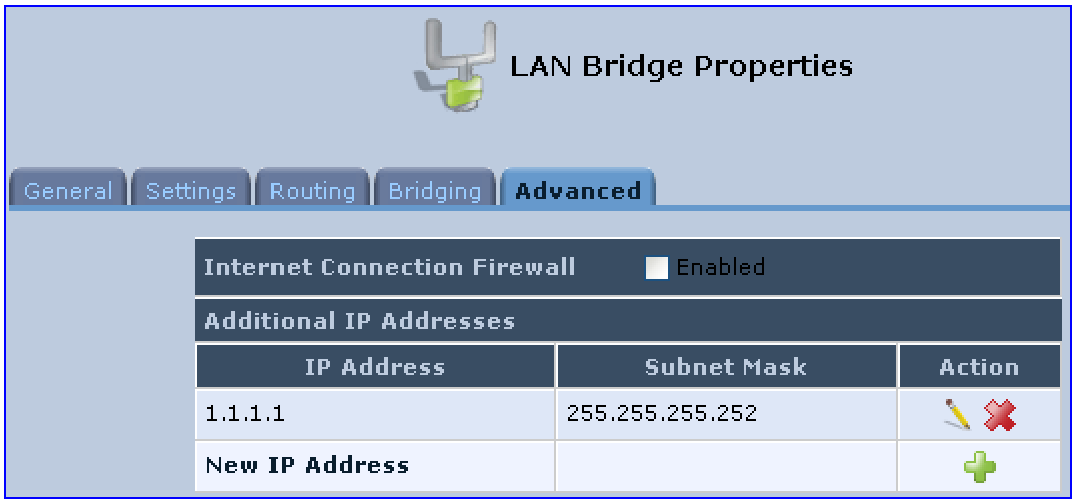
Parameter	Description
Routing	Select 'Advanced' or 'Basic' routing.
Routing Mode	Select one of the following Routing modes: ▪ **Route:** Use route mode if you want your device to function as a router between two networks. ▪ **NAT:** Network Address Translation (NAT) translates IP addresses to a valid, 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

Parameter	Description
	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.
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.

11.1.4 Advanced Tab

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 11-10: Internet Connection Firewall



Internet Connection Firewall ☐ Enabled

Additional IP Addresses

IP Address	Subnet Mask	Action
1.1.1.1	255.255.255.252	
New IP Address		

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-20x.home*.

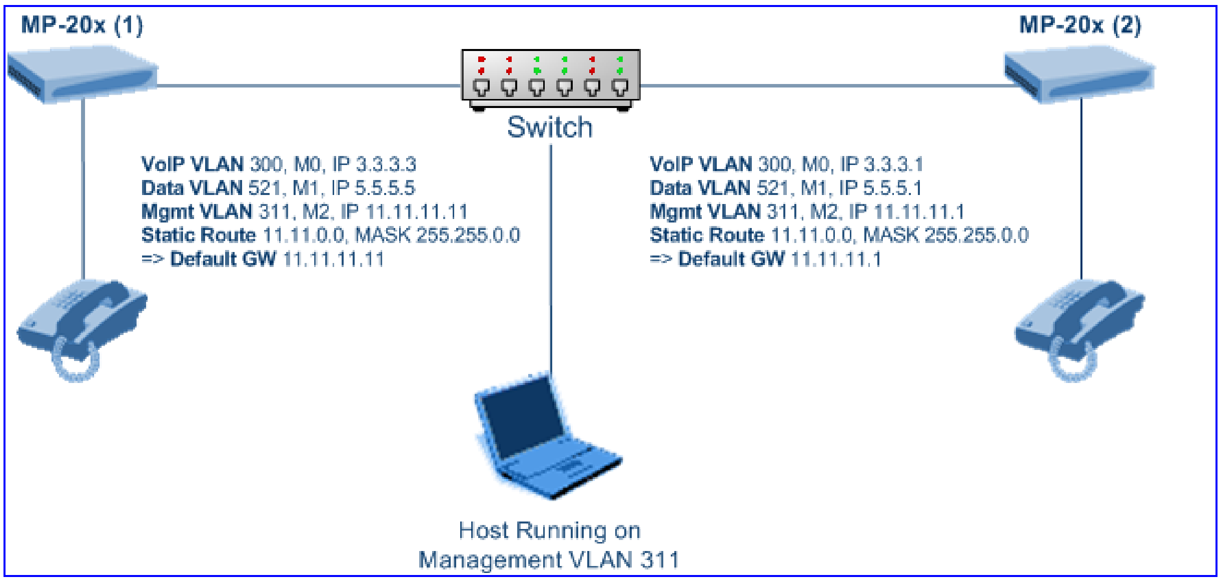
11.1.5 Example of Configuring 3 VLANs: VoIP, Data and Management

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

11.1.5.1.1 Setup

Two MP-20xs 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 11-11: Using VLAN - Setup


MP-20x (1)
MP-20x (2)
Switch
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
Host Running on
Management VLAN 311

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

1. For MP-20x 1: Open menu **Advanced** > **Remote Administration** icon, and select the 'Using Primary HTTP Port (80)' and 'Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)' check boxes.
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.

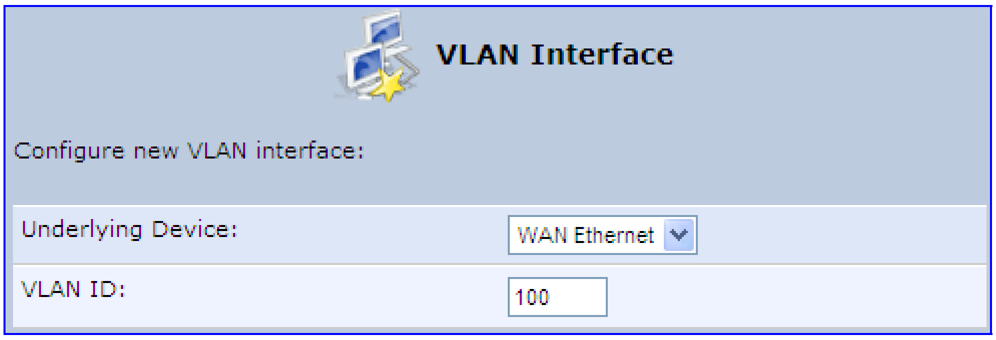
7. Repeat the same steps for MP-20x 2. Use a different IP address.
8. To access the web management for both MP-20x-1 and MP-20x-2, connect a PC that works on the same VLAN management (311).

11.1.5.1.2 Defining a VLAN, Configuring its Interface

➤ **To define an interface VLAN:**

1. Access the 'VLAN Interface' screen (menu **Network Connections** > **New Connection** > **Advanced Connection** > **VLAN Interface**.

Figure 11-12: Example of Using VLAN - VLAN Interface Screen

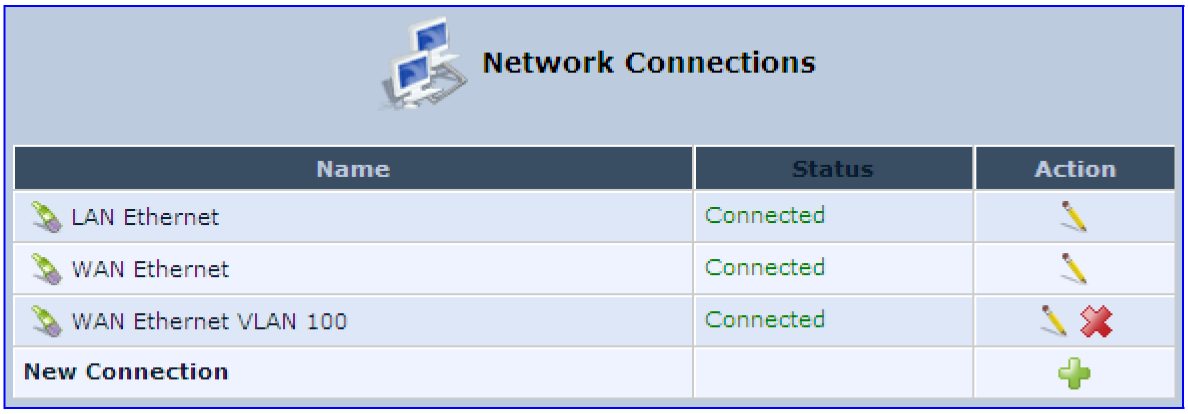

VLAN Interface

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 VLAN 100).

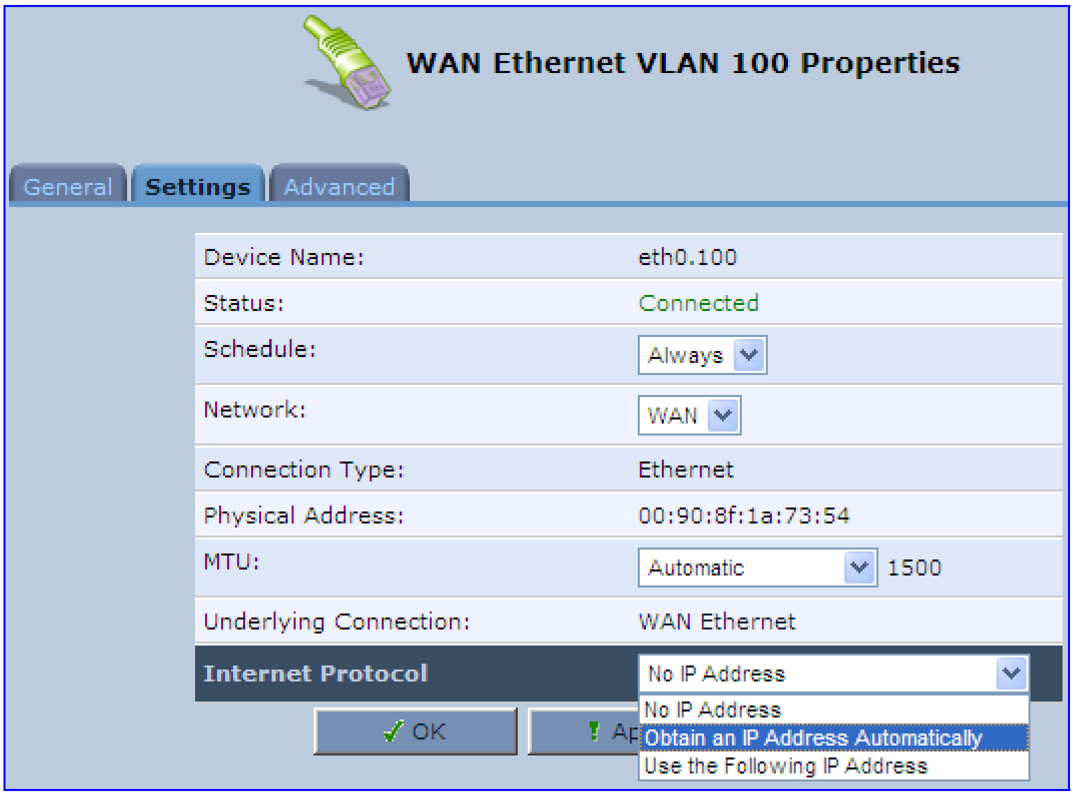
Figure 11-13: Verifying a New Interface on the WAN Side


Network Connections

Name	Status	Action
LAN Ethernet	Connected	✎
WAN Ethernet	Connected	✎
WAN Ethernet VLAN 100	Connected	✎ ✖
New Connection		✚

3. Enter the new interface by clicking the **Edit** icon, and then selecting the Settings tab; the screen shown below opens.

Figure 11-14: Configuring WAN Ethernet


WAN Ethernet VLAN 100 Properties

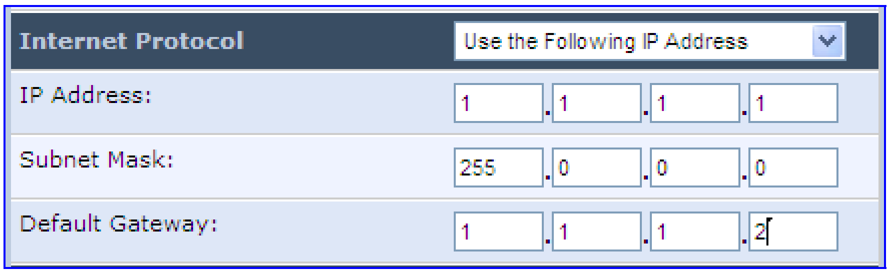
General
Settings
Advanced

Device Name:	eth0.100
Status:	Connected
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00:90:8f:1a:73:54
MTU:	Automatic 1500
Underlying Connection:	WAN Ethernet
Internet Protocol	No IP Address

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

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 11-15: 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

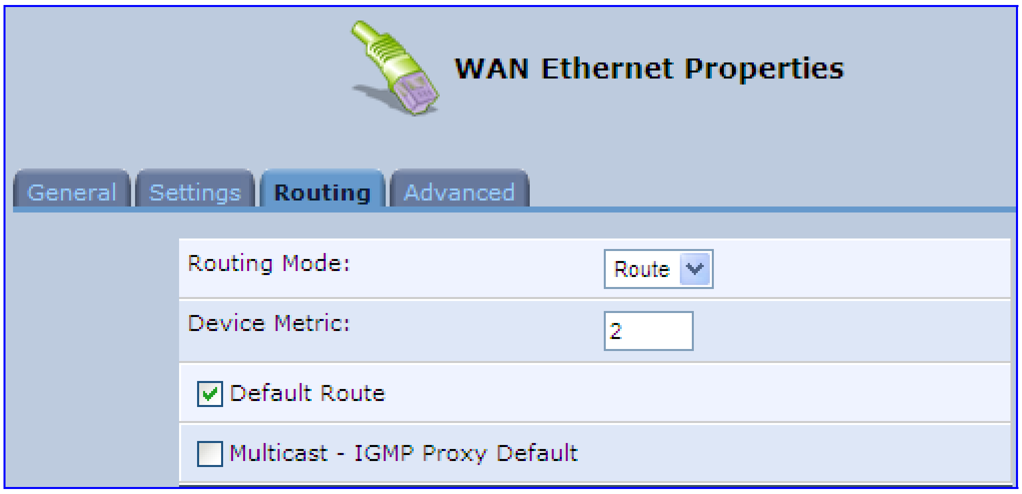
5. Define an IP address for each device and click **Apply** and **OK**.

11.1.5.1.3 Changing the Routing Mode and Adding a Static Route

➢ **To change the routing mode:**

1. (For all VoIP packets needing to be transferred within the VoIP VLAN) Open menu **Network Connections** > **WAN Ethernet** VLAN 100 > **Settings**; the figure shown below opens.

Figure 11-16: Routing


WAN Ethernet Properties

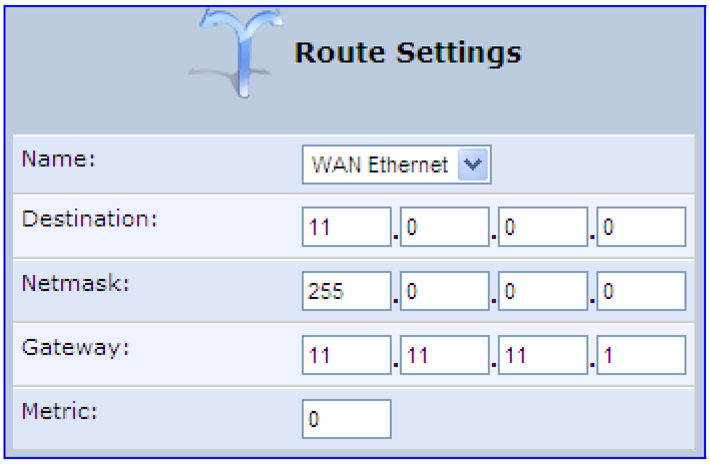
Routing Mode: Route
Device Metric: 2
☑ Default Route
☐ Multicast - IGMP Proxy Default

2. Configure parameter 'Routing Mode' (NAT or Route). Choose 'Route' and check the check box 'Default Route' to use the VoIP VLAN.
3. Configure 'Device Metric' to be the lower than the default metric (default = 3).

➢ **To add a static route:**

1. Under the Routing tab, in the Routing table, click New Route.

Figure 11-17: Route Settings


Route Settings

Name: WAN Ethernet
Destination: 11 . 0 . 0 . 0
Netmask: 255 . 0 . 0 . 0
Gateway: 11 . 11 . 11 . 1
Metric: 0

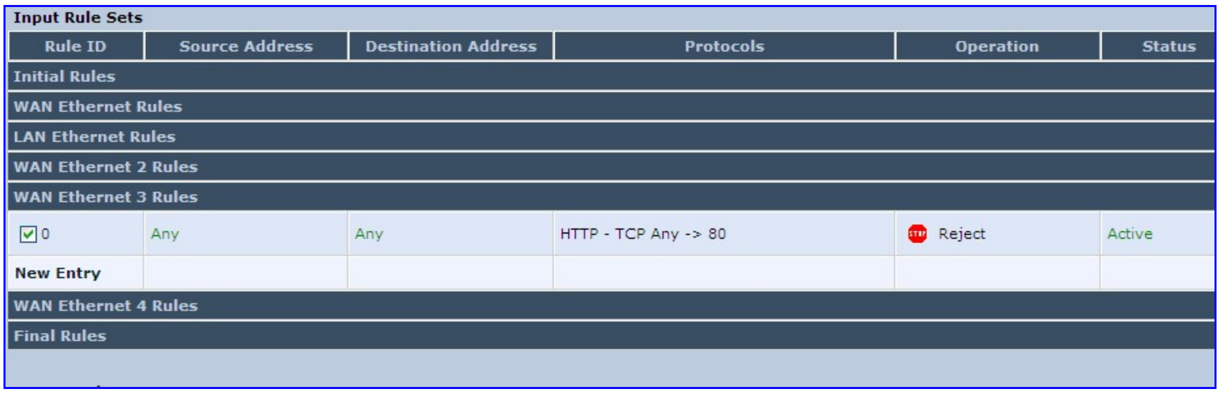
2. From the 'Name' drop-down list, choose 'WAN Ethernet'; configure the parameters Destination, Netmask and Gateway.

11.1.5.1.4 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 11-18: Input Rule Sets

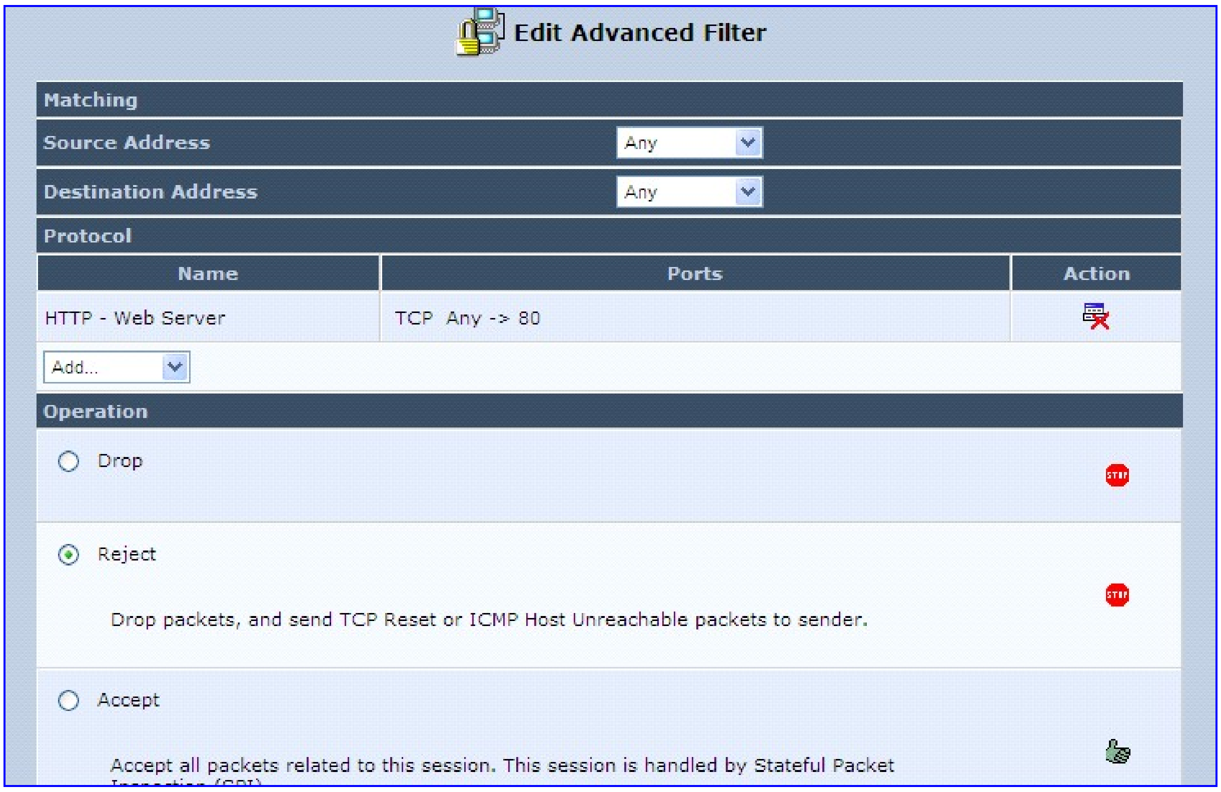


Input Rule Sets

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 and choose the filter type (Source IP, Destination IP or Protocol). In the example shown in the figure below, Port 80 (HTTP) is rejected.

Figure 11-19: Edit Advanced Filter



Edit Advanced Filter

Matching

Source Address: Any

Destination Address: Any

Protocol

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

Operation

Drop

[✓ Reject]

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

Accept

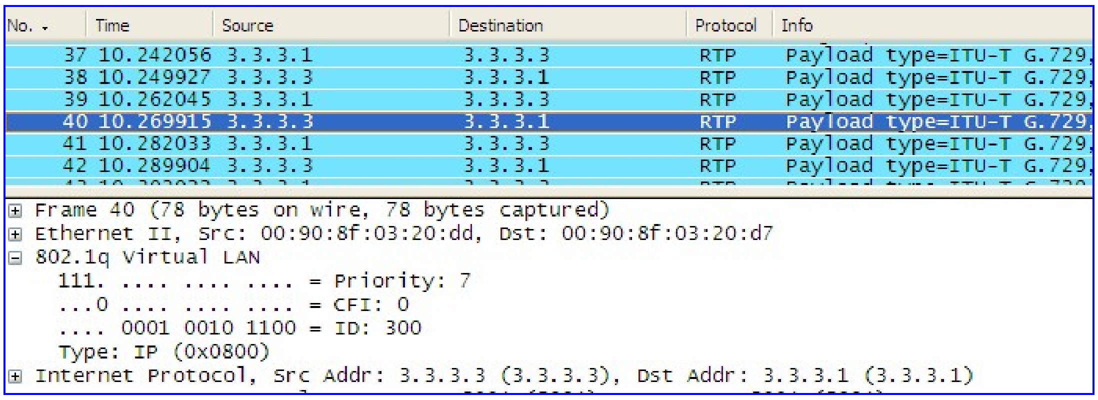
Accept all packets related to this session. This session is handled by Stateful Packet

11.1.5.1.5 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 11-20: Testing the Setup

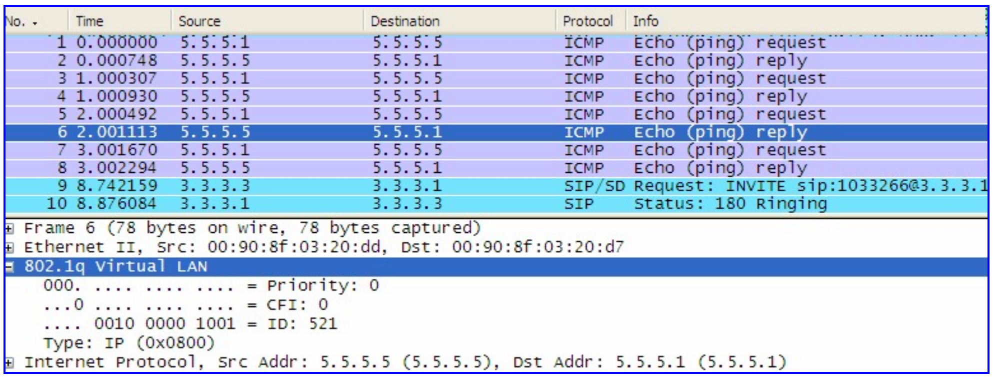


```
No. -   Time        Source     Destination   Protocol  Info
   37 10.242056  3.3.3.1     3.3.3.3       RTP       Payload type=ITU-T G.729,
   38 10.249927  3.3.3.3     3.3.3.1       RTP       Payload type=ITU-T G.729,
   39 10.262045  3.3.3.1     3.3.3.3       RTP       Payload type=ITU-T G.729,
   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 11-21: Testing the Setup

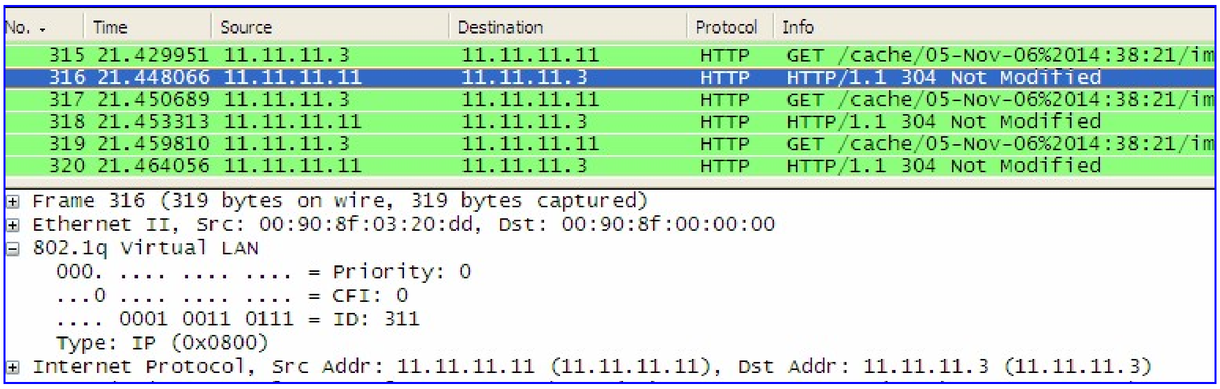


```
No. -  Time       Source    Destination  Protocol  Info
    1 0.000000   5.5.5.1   5.5.5.5      ICMP      Echo (ping) request
    2 0.000748   5.5.5.5   5.5.5.1      ICMP      Echo (ping) reply
    3 1.000307   5.5.5.1   5.5.5.5      ICMP      Echo (ping) request
    4 1.000930   5.5.5.5   5.5.5.1      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.

Figure 11-22: 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)
```

11.2 LAN-WAN Bridging

WAN bridge creates a bridge over WAN and LAN devices. In this way, PCs on the MP-20x's LAN side can get IP addresses that are known on the WAN side.

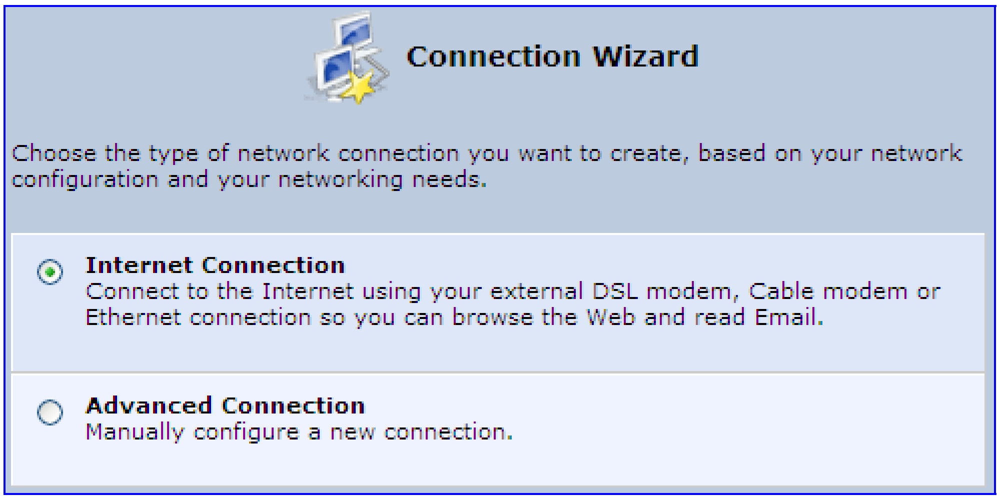
Note: Currently, the MP-202C model does not support LAN-WAN bridging.

11.2.1 Creating with the Connection Wizard

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

1. From the sidebar menu, click the **Network Connections** menu, and in the screen 'Network Connections' click the **New Connection** link; the 'Connection Wizard' screen opens.

Figure 11-23: Connection Wizard Screen



Connection Wizard

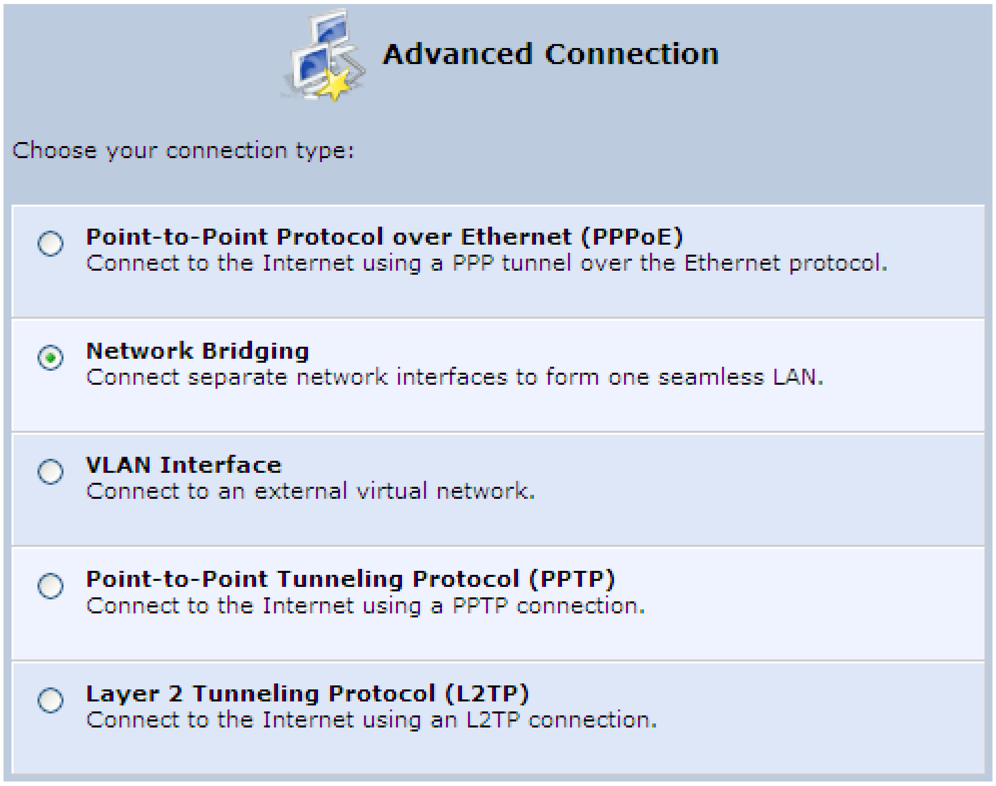
Choose the type of network connection you want to create, based on your network configuration and your networking needs.

[✓ Internet Connection]
Connect to the Internet using your external DSL modem, Cable modem or Ethernet connection so you can browse the Web and read Email.

Advanced Connection
Manually configure a new connection.

2. Select the 'Advanced Connection' option, and then click **Next**; the 'Advanced Connection' screen appears.

Figure 11-24: Advanced Connection Wizard Screen



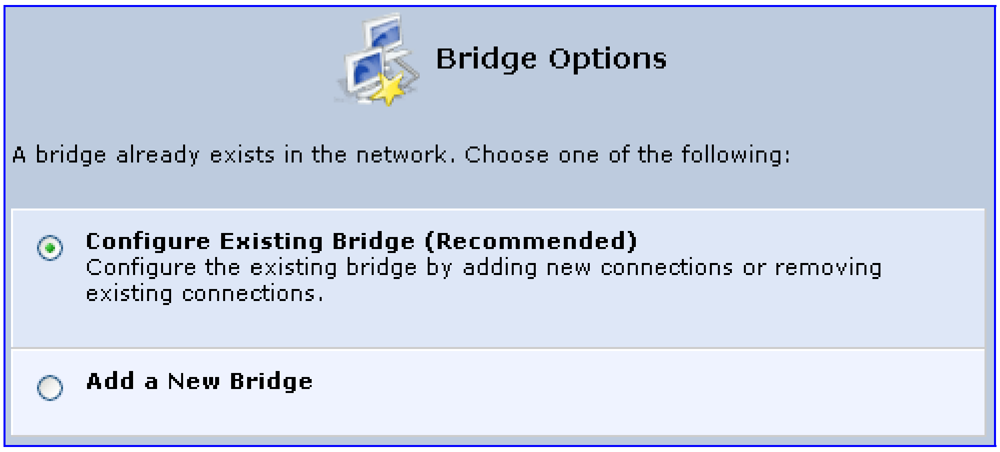
Advanced Connection

Choose your connection type:

- ○ **Point-to-Point Protocol over Ethernet (PPPoE)** Connect to the Internet using a PPP tunnel over the Ethernet protocol.
- [✓ **Network Bridging**] Connect separate network interfaces to form one seamless LAN.
- ○ **VLAN Interface** Connect to an external virtual network.
- ○ **Point-to-Point Tunneling Protocol (PPTP)** Connect to the Internet using a PPTP connection.
- ○ **Layer 2 Tunneling Protocol (L2TP)** Connect to the Internet using an L2TP connection.

3. Select the 'Network Bridging' option, and then click **Next**; the screen 'Bridge Options' opens.

Figure 11-25: Bridge Options



Bridge Options

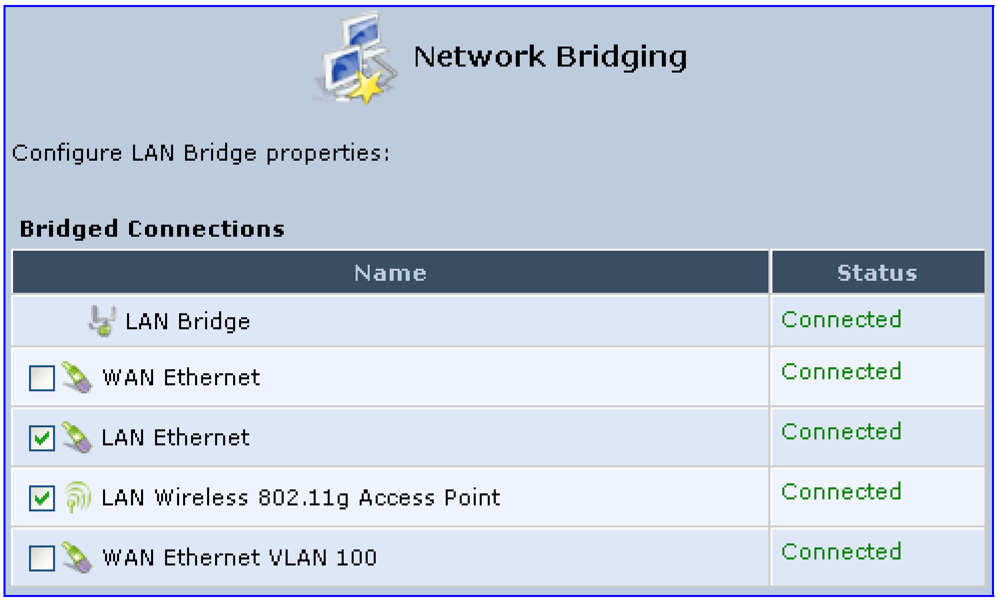
A bridge already exists in the network. Choose one of the following:

- [✓ **Configure Existing Bridge (Recommended)**] Configure the existing bridge by adding new connections or removing existing connections.
- ○ **Add a New Bridge**

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

   - **Configure Existing Bridge:** Select this option and then click **Next**; the screen 'Network Bridging' opens, allowing you to add new connections or remove existing ones, by selecting or clearing their respective check boxes.

Figure 11-26: Network Bridging



Network Bridging

Configure LAN Bridge properties:

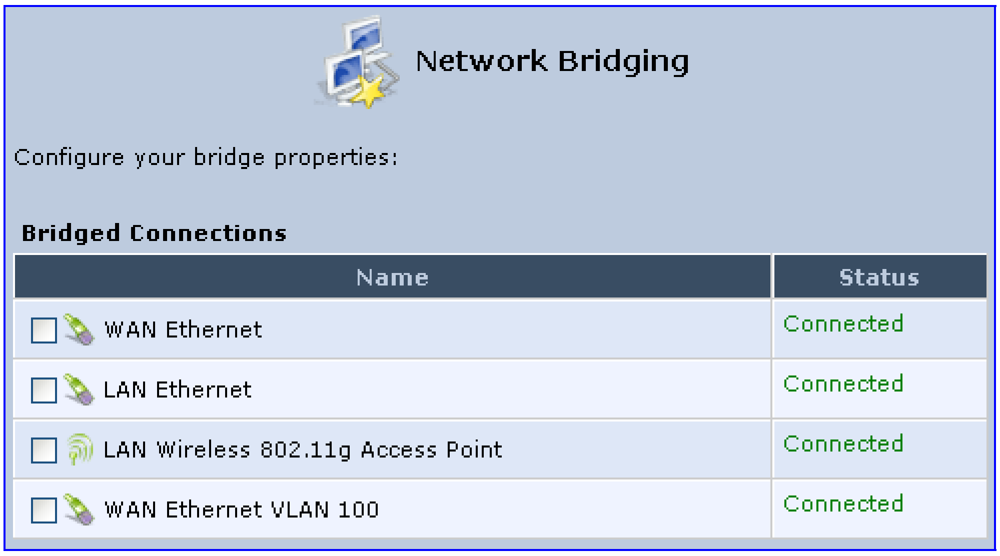
Bridged Connections

Name	Status
LAN Bridge	Connected
☐ WAN Ethernet	Connected
☑ LAN Ethernet	Connected
☑ LAN Wireless 802.11g Access Point	Connected
☐ WAN Ethernet VLAN 100	Connected

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

   - **Add a New Bridge:** Select this option and then click **Next**; a different 'Network Bridging' screen opens, allowing you to add a bridge over the unbridged connections, by selecting their respective check boxes.

Figure 11-27: WLAN-LAN - Network Bridging



Network Bridging

Configure your bridge properties:

Bridged Connections

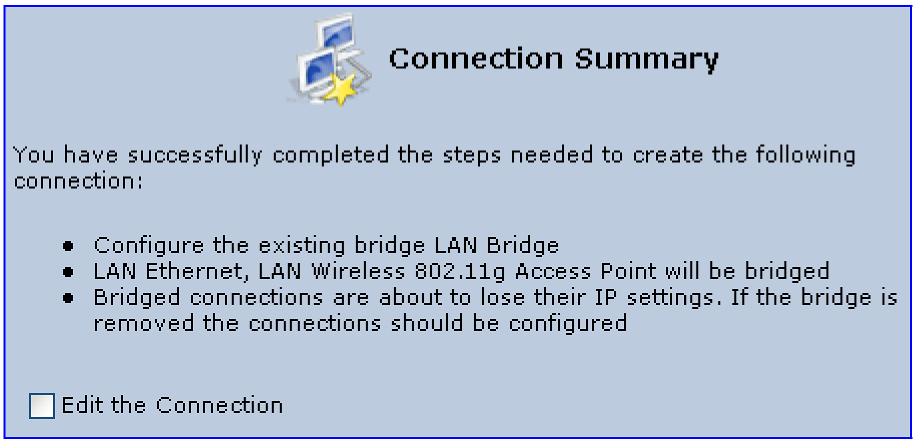
Name	Status
☐ WAN Ethernet	Connected
☐ LAN Ethernet	Connected
☐ LAN Wireless 802.11g Access Point	Connected
☐ WAN Ethernet VLAN 100	Connected

Important notes:

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

5. Click **Next**; the screen 'Connection Summary' opens, corresponding to your changes.

Figure 11-28: 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
- LAN Ethernet, 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

☐ Edit the Connection

6. Select 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.

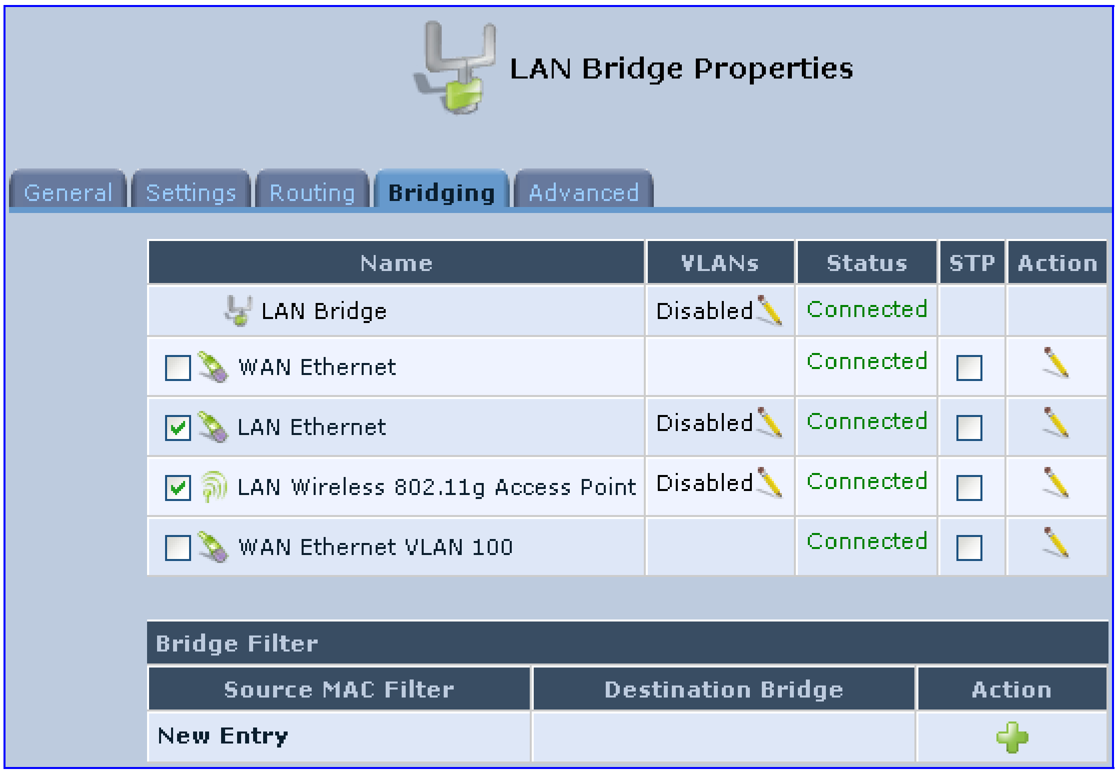
11.2.2 Settings Tab

Refer to 'Settings Tab' on page 125.

11.2.3 Bridge Tab

The **Bridging** tab 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 11-29: Bridge Settings



Name	VLANs	Status	STP	Action
LAN Bridge	Disabled	Connected		
☐ WAN Ethernet		Connected	☐	✎
☑ LAN Ethernet	Disabled	Connected	☐	✎
☑ LAN Wireless 802.11g Access Point	Disabled	Connected	☐	✎
☐ WAN Ethernet VLAN 100		Connected	☐	✎

Bridge Filter

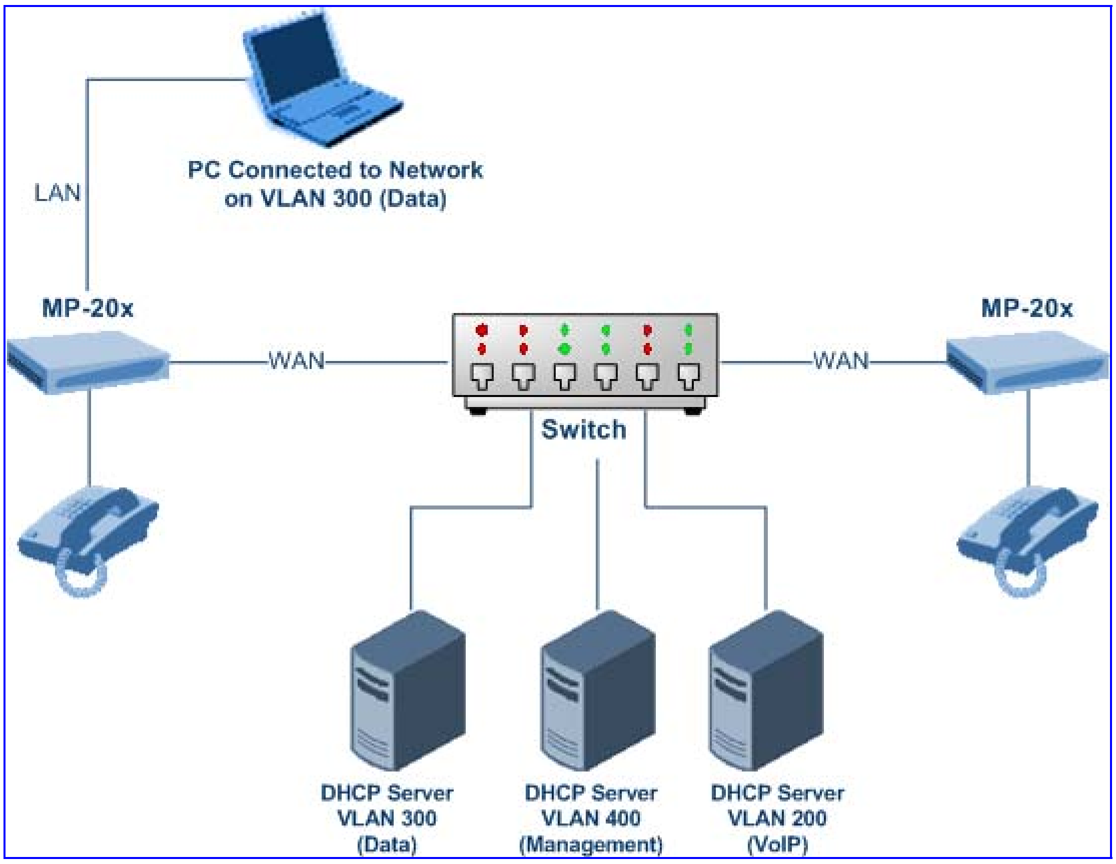
Source MAC Filter	Destination Bridge	Action
New Entry		✚

11.2.4 Examples of Configuring VLANs in Bridge Mode

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

This example explains how to configure MP-20x to use 3 separate VLANs (for VoIP, data and management) in bridge mode.

Figure 11-30: Example of Using Bridge Mode and Configuring VLANs


PC Connected to Network on VLAN 300 (Data)
LAN
MP-20x
WAN
Switch
WAN
MP-20x
DHCP Server VLAN 300 (Data)
DHCP Server VLAN 400 (Management)
DHCP Server VLAN 200 (VoIP)

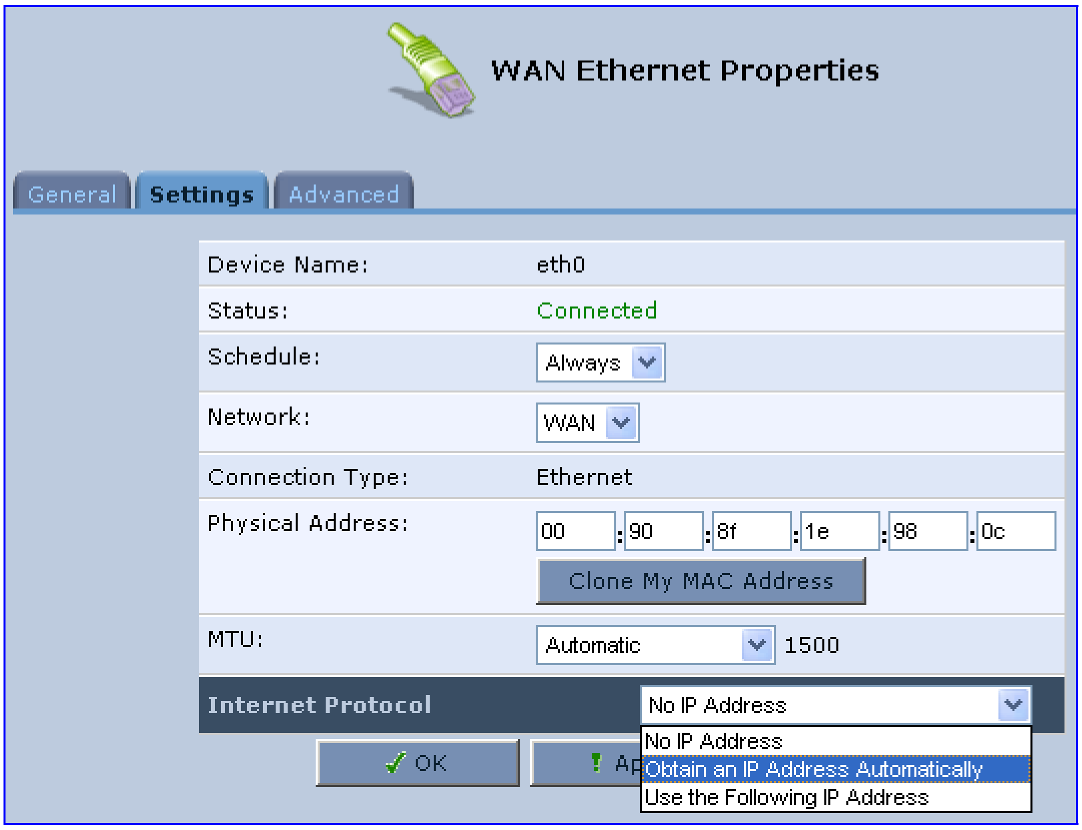
11.2.4.1.1 Setup

Two MP-20xs 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 three separate VLANs in bridge mode:**

1. (For **MP-20x "1"** and **MP-20x "2"**) Connect the PC to MP-20x "1" LAN NIC and use static IP address 192.168.2.10 for your PC.
2. In your Internet browser, browse to http://192.168.2.1.
3. Open menu **Advanced** > **Remote Administration** icon, and select the 'Using Primary HTTP Port (80)' and 'Allow Incoming ICMP Echo Requests' check boxes (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' (optionally, you can use a static IP address).
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.

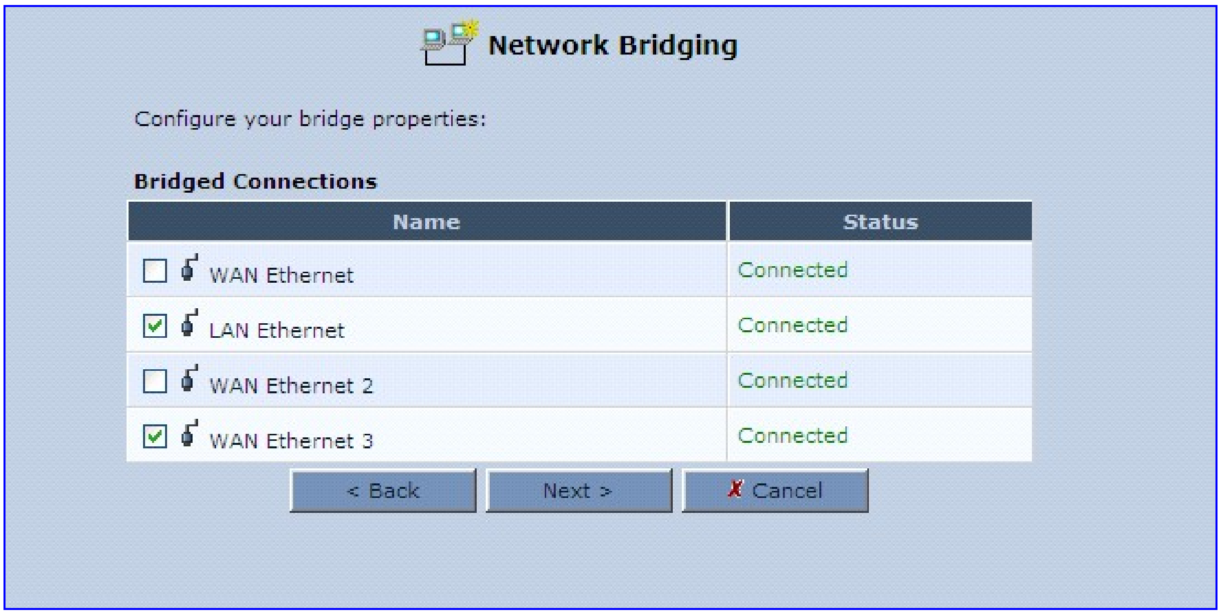
Figure 11-31: Configuring WAN Ethernet



Device Name:	eth0
Status:	Connected
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00 : 90 : 8f : 1e : 98 : 0c
MTU:	Automatic 1500
Internet Protocol	No IP Address

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'.

Figure 11-32: Network Bridging


Network Bridging

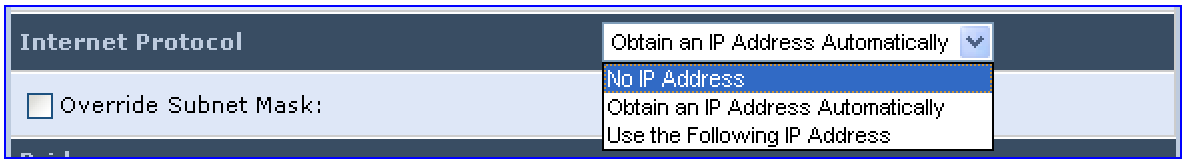
Configure your bridge properties:

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 11-33: No IP Address


Internet Protocol: Obtain an IP Address Automatically

☐ Override Subnet Mask:

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

9. Reboot MP-20x (optional).
10. Ensure that the PC is connected to the LAN port of MP-20x and then configure it to 'Obtain IP Address Automatically'; all data from the LAN port are 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.

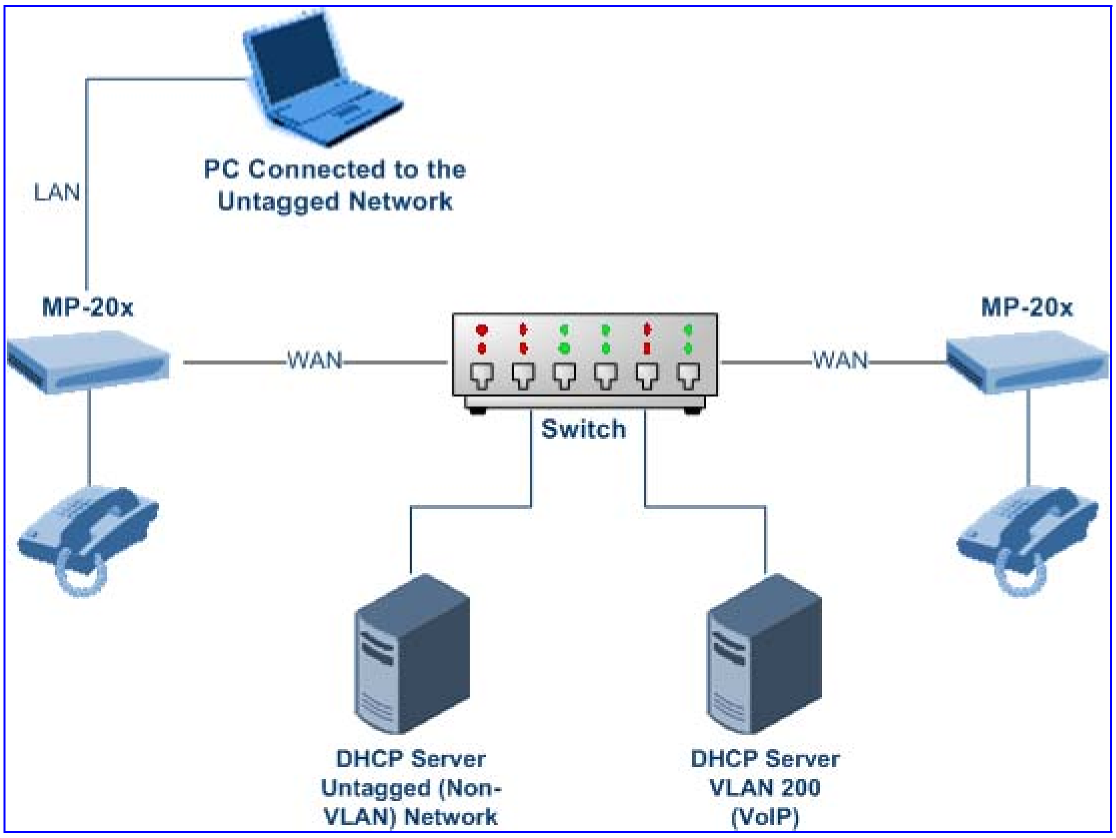
11.2.4.1.2 Testing the Setup

1. Place a VoIP call and check that the VoIP is using 802.1q/p and that the VID is 200.
2. Ping from the PC (behind **MP-20x 1**) to the network; you'll see that the data traffic is using 802.1q and that the VID is 300.
3. Connect a PC to the network in VLAN 400; verify that you can access VLAN 400 from the WAN interface.

11.2.4.2 Example 2: Configuring Tagged VoIP, Untagged Data Traffic

This example explains how to configure MP-20x to tag VoIP traffic and untag data traffic in bridge mode.

Figure 11-34: Example of Tagging Voice and Untagging Data


PC Connected to the Untagged Network
LAN
MP-20x
WAN
Switch
WAN
MP-20x
DHCP Server Untagged (Non-VLAN) Network
DHCP Server VLAN 200 (VoIP)

Setup

Two MP-20xs 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.

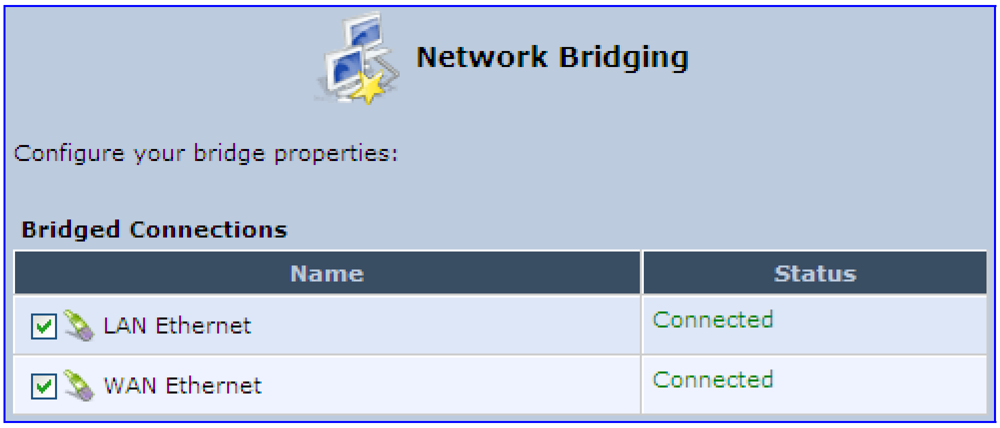
The procedure below describes the provedure for **MP-20x (1) and MP-20x (2).**

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

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' (Network Connections menu > New Connection link > Advanced Connection option > Network Bridging option), check LAN Ethernet and WAN Ethernet.

Figure 11-35: WAN/LAN Bridge



Network Bridging

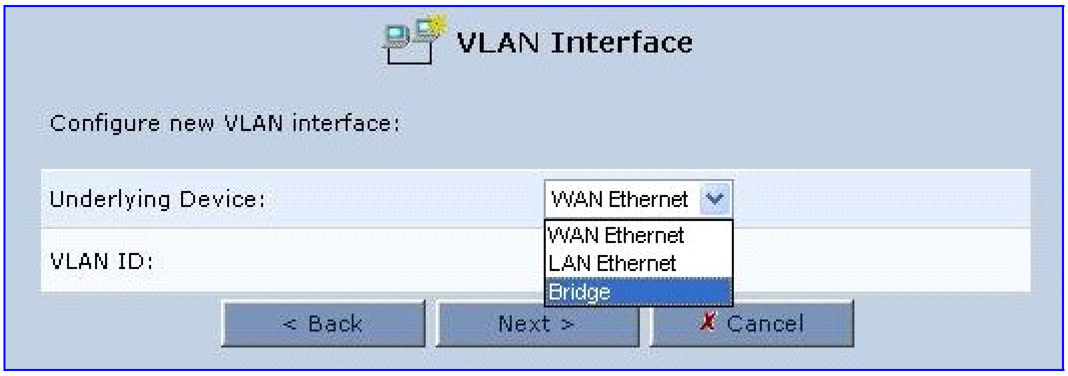
Configure your bridge properties:

Bridged Connections

Name	Status
✓ LAN Ethernet	Connected
✓ WAN Ethernet	Connected

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

Figure 11-36: VLAN Interface Screen



VLAN Interface

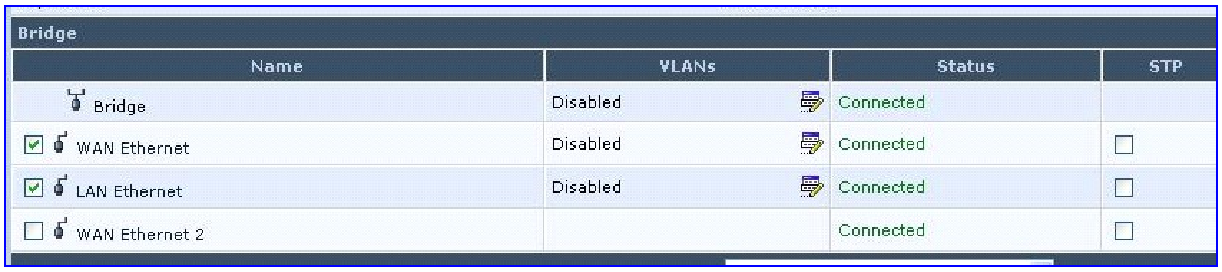
Configure new VLAN interface:

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).

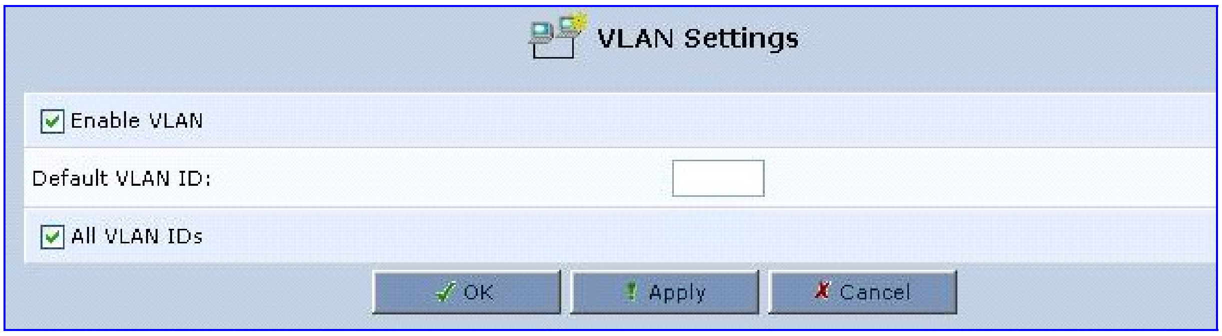
Figure 11-37: Bridge Section of the Screen



Bridge

Name	VLANs	Status	STP
Bridge	Disabled	Connected	
✓ WAN Ethernet	Disabled	Connected	☐
✓ LAN Ethernet	Disabled	Connected	☐
☐ WAN Ethernet 2		Connected	☐

Figure 11-38: VLAN Settings


VLAN Settings

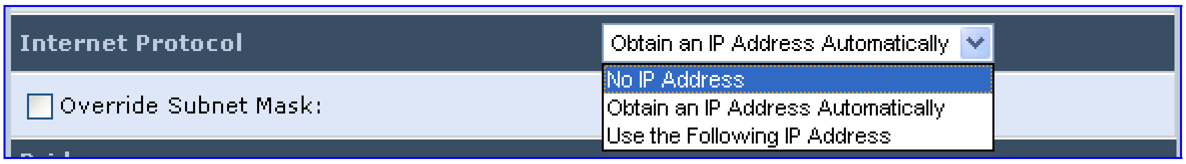
☑ Enable VLAN

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 11-39: No IP Address

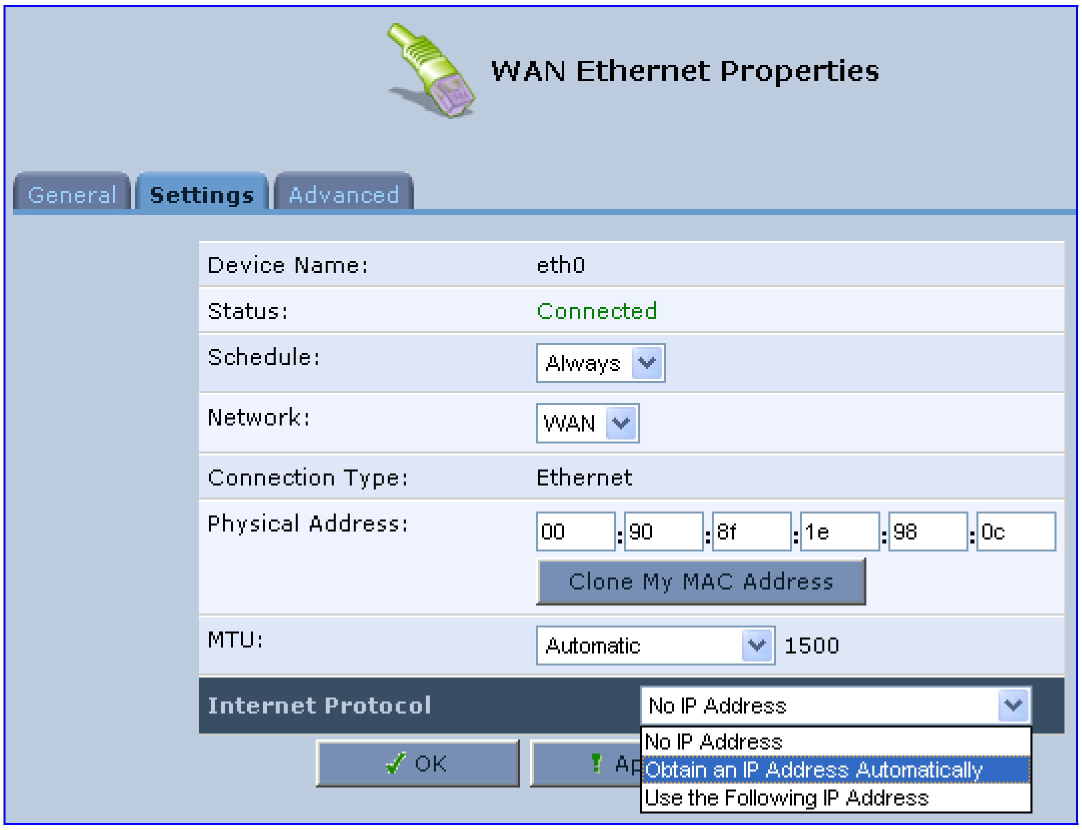

Internet Protocol: Obtain an IP Address Automatically

☐ Override Subnet Mask:

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

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 11-40: Configuring WAN Ethernet


WAN Ethernet Properties

General
Settings
Advanced

Device Name: eth0

Status: Connected

Schedule: Always

Network: WAN

Connection Type: Ethernet

Physical Address: 00 : 90 : 8f : 1e : 98 : 0c

MTU: Automatic 1500

Internet Protocol: No IP Address

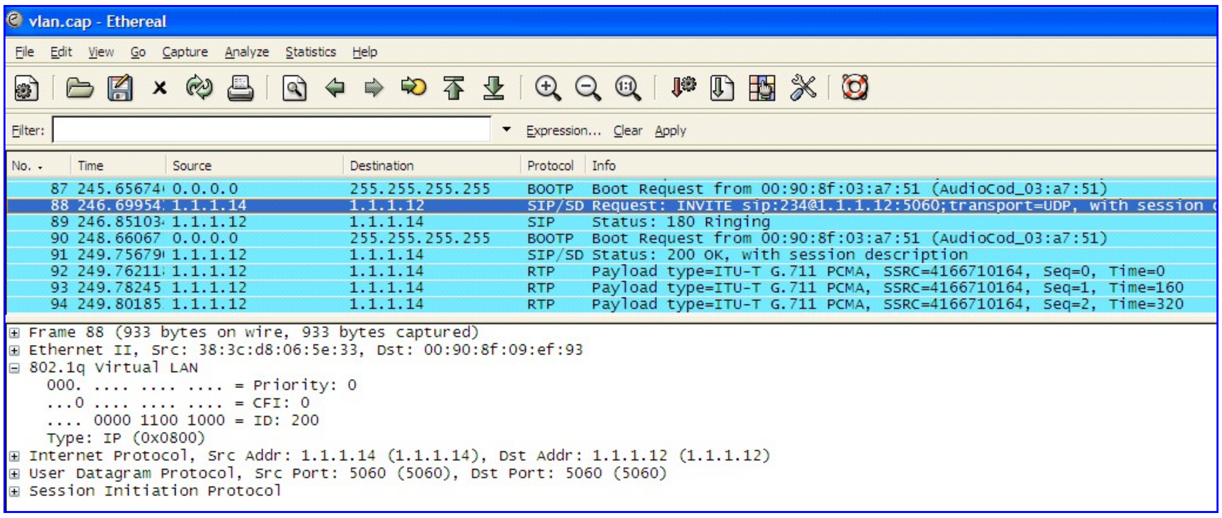
Clone My MAC Address
No IP Address
Obtain an IP Address Automatically
Use the Following IP Address
OK
Ap

9. Set your PC to use DHCP address.

Testing the Setup

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

Figure 11-41: Testing the Setup

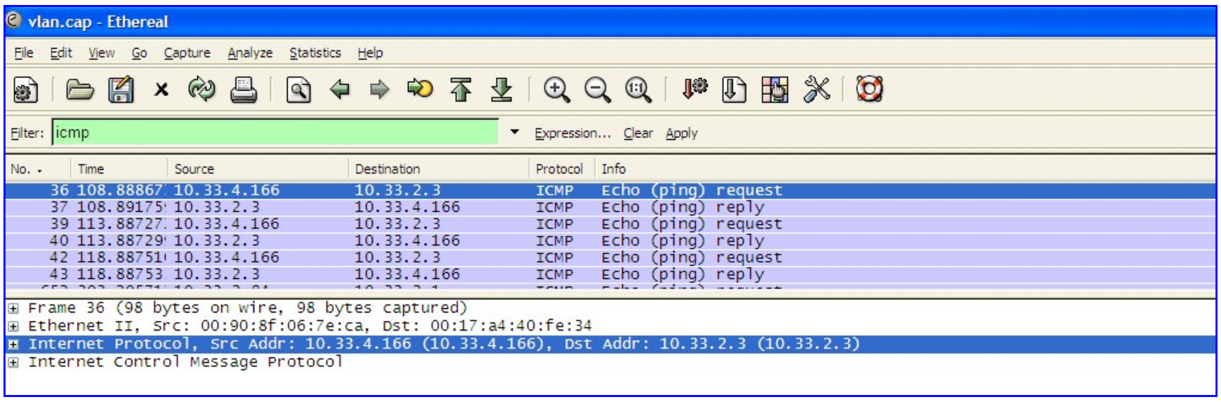

vlan.cap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
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 MP-20x) and verify that the data traffic (ICMP) is untagged (refer to the screen below).

Figure 11-42: Testing the Setup


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

```
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
```

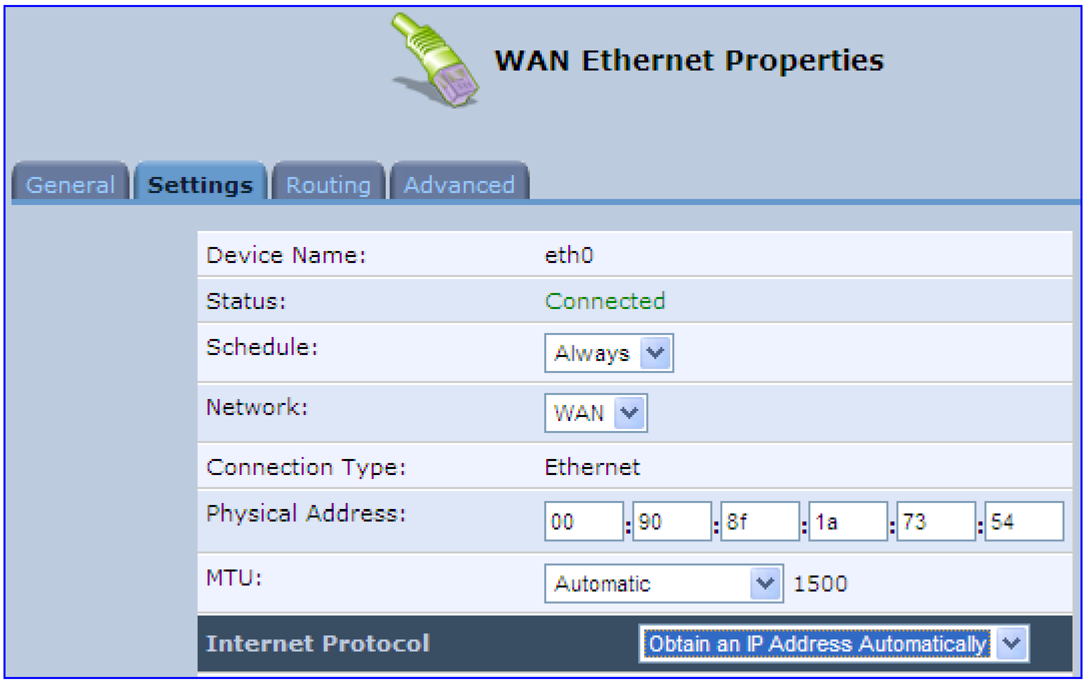
```
⊞ Frame 36 (98 bytes on wire, 98 bytes captured)
⊞ Ethernet II, Src: 00:90:8f:06:7e:ca, Dst: 00:17:a4:40:fe:34
⊞ Internet Protocol, Src Addr: 10.33.4.166 (10.33.4.166), Dst Addr: 10.33.2.3 (10.33.2.3)
⊞ Internet Control Message Protocol
```

11.2.4.3 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' (optionally, you can use a static IP address).

Figure 11-43: Configuring WAN Ethernet

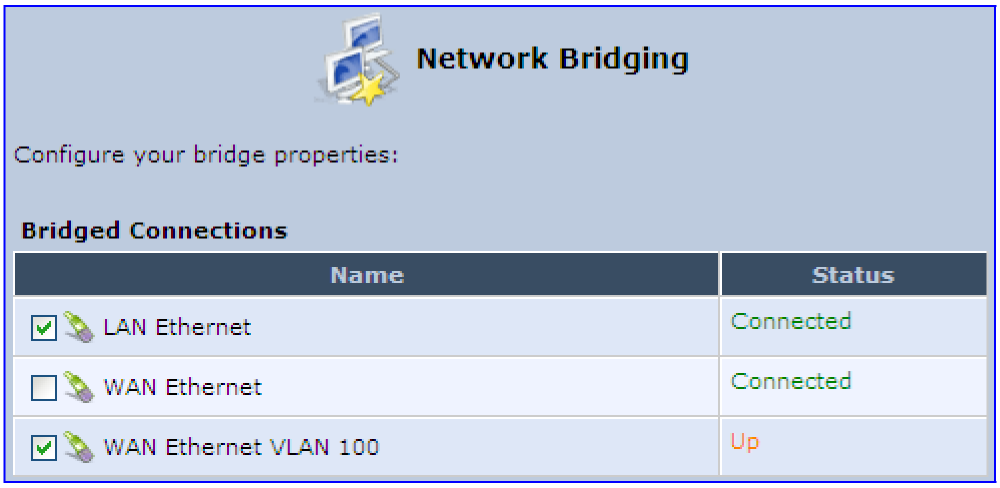


WAN Ethernet Properties

Device Name:	eth0
Status:	Connected
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00 : 90 : 8f : 1a : 73 : 54
MTU:	Automatic 1500
Internet Protocol	Obtain an IP Address Automatically

2. Define a new network bridge. Define it by selecting the check boxes of LAN Ethernet and the new VLAN Interface that you defined.

Figure 11-44: VoIP and Data on same VLAN



Network Bridging

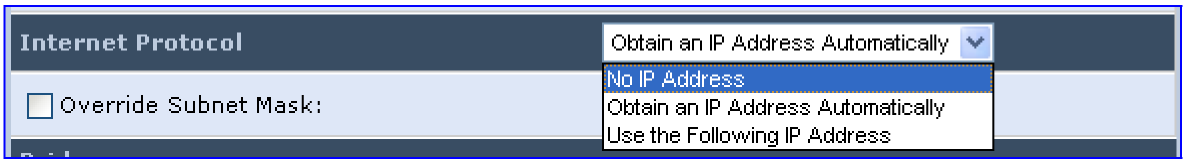
Configure your bridge properties:

Bridged Connections

Name	Status
☑ LAN Ethernet	Connected
☐ WAN Ethernet	Connected
☑ WAN Ethernet VLAN 100	Up

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

Figure 11-45: No IP Address



Internet Protocol: Obtain an IP Address Automatically

☐ Override Subnet Mask:

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

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

Reader's Notes

12 Remote MP-20x Telephone Adapter Management

MP-20x was designed to be mass-deployed by carriers and service providers. One of the keys to guarantee end-user satisfaction and true toll-quality service in mass field deployment is comprehensive remote configuration and management capabilities:

- Automatic and remote configuration updates
- Automatic and remote firmware updates
- Remote diagnosis of problems reported by the user
- Remote collection of statistical information regarding the quality of the service
- Remote notifications of problems in the service

12.1 Overview

12.1.1 Remote Configuration

By default, MP-20x is provided with factory default settings, which are common to all MP-20x devices (except for the MAC address). The factory settings allow the user to connect to MP-20x's embedded Web server from the LAN interface.

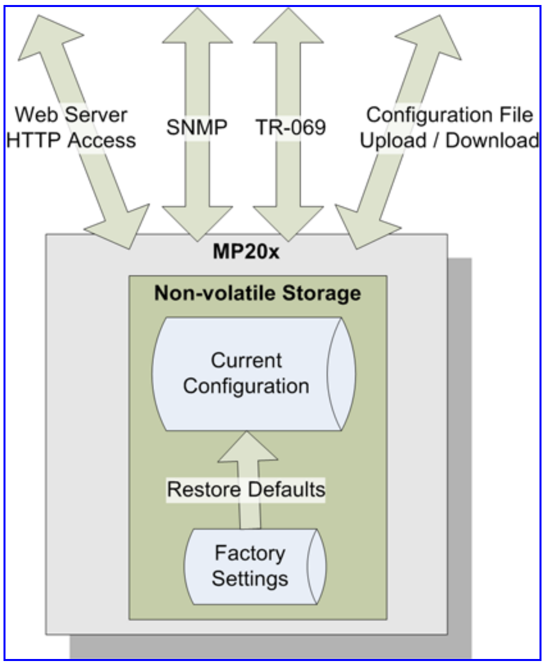
By default, the WAN interface is configured for DHCP (i.e., automatically obtains its IP address from a DHCP server). In the case of PPPoE or other Internet dialers, this default configuration does not allow MP-20x to connect to the Internet. The default configuration does not include any VoIP service provider settings (such as a SIP proxy).

In some cases, AudioCodes can ship MP-20x devices that are pre-configured with some customer-specific parameters. This set of parameters is usually defined as the new "factory settings" for this specific customer.

MP-20x's factory default settings and the current configuration running on MP-20x are stored on MP-20x's non-volatile flash memory. The current configuration can be remotely updated using several configuration interfaces:

- HTTP-based Web server
- SNMP
- TR-069
- Configuration file upload/download

Figure 12-1: Remote Management Interfaces



All configuration interfaces access the same internal configuration repository. The configuration file represents the complete set of MP-20x configuration parameters. Specific configuration interfaces (e.g. SNMP and TR-069) might support access only to a sub-set of these configuration parameters.

At any time, the factory settings can be restored using the Web interface or by pressing on the Restore Defaults push-button while MP-20x is being powered up.

The table below lists the main MP-20x configuration parameter groups:

Table 12-1: Main Configuration Parameter Groups

Group	Description
VoIP	Parameters relating to the VoIP functionality (e.g. analog interface, SIP signaling, voice and fax, media streaming)
WAN Interface	The main WAN Internet connection (this group is also referred to as the "Quick Setup").
Network Connections	Configuration of all network connections (LAN and WAN), including advanced connections such as VLANs.
Security	Parameters relating to the internal firewall.
QoS	Configuration of Quality of Service parameters such as priorities and traffic shaping.
System / Advanced	Configuration of system parameters such as Remote Update and Remote Access and advanced parameters such as Dynamic DNS, UPnP.

A typical set of parameters that a service provider may want to configure include the following:

- Remote access and/or automatic firmware and configuration update parameters
- VoIP configuration: SIP proxy, line settings (User IP, Password)
- QoS parameters (e.g. traffic shaping)

12.1.2 Remote Management

12.1.2.1 Firmware Upgrade

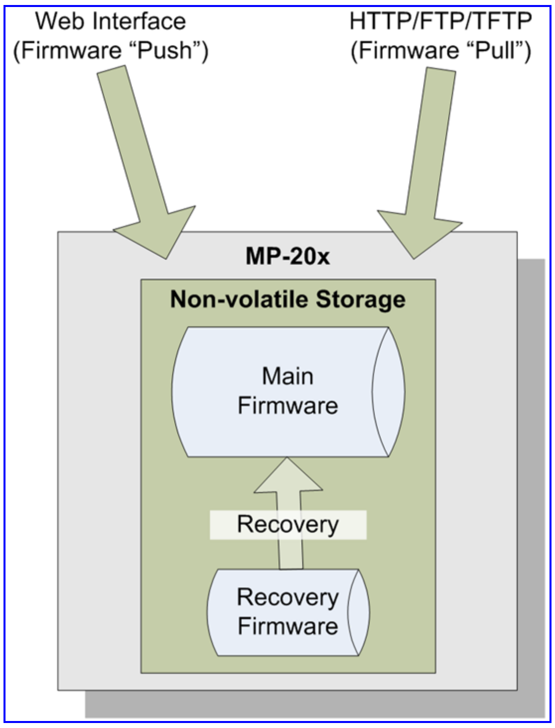
Service providers require the ability to update MP-20x's firmware in the field (e.g. in case of maintenance releases or releases that support new required features). The process is required to be automatic, allowing mass update, and robust and fail-safe.

MP-20x's firmware is stored in the non-volatile flash memory. MP-20x's flash memory is capable of storing a recovery firmware that ensures a fail-safe operation (even if the user unplugs the power during the firmware burning process).

MP-20x's firmware can be upgraded using one of the following mechanisms:

- The new firmware can be "pushed" (uploaded) to MP-20x, using the embedded Web server
- The new firmware can be "pulled" (downloaded) by MP-20x from a remote HTTP, FTP, or TFTP server

Figure 12-2: Firmware Upgrade Mechanism



The remote firmware download process can be triggered by one of the following:

- MP-20x checks for a new firmware upon MP-20x restart
- MP-20x periodically checks for a new firmware
- Manual trigger using CLI, TR-069, SNMP, or Web

Note: Unless forced, MP-20x downloads and upgrades to the new firmware only if its version number is higher than the firmware version currently running on MP-20x. The version number is not taken from the image file name, but from the header of the image file.

12.1.2.2 Status and Performance Monitoring

The ability to remotely monitor the status of MP-20x is critical to the service provider, who wants to support users without having to send a technician on site (avoiding the "truck roll"). The service provider may want to know the current status of MP-20x (e.g. is it registered to the SIP proxy, is the phone off-hook) or some statistical information (e.g. average packet loss during a call).

MP-20x maintains a set of status and performance information internally. This information (or parts of it) can be retrieved via the different management interfaces (e.g. Web, SNMP, or TR-069).

The table below describes the status and performance monitoring (statistical) information available in MP-20x, divided into the main groups.

Table 12-2: Status and Performance Monitoring Parameters

Group	Description
VoIP	▪ Current status information per line: - Phone state - Registration status - Source, codec and type of current call - Packet loss, jitter and delay of current call
Network Connections	▪ Current status information per interface: - Connection status - Allocated IP address - Received and transmitted packets
System	▪ Software version information ▪ Hardware version information ▪ System Up time

12.1.2.3 Alarms, Notifications and Logging

Instead of periodically polling MP-20x to obtain its current status, the service provider may want MP-20x to notify abnormal events or to send regular reports to a logging server. Both options are supported by MP-20x. The table below shows the relevant interfaces for alarms and notifications.

Table 12-3: Notifications and Logged Events

Group	Notifications and Logged Events
VoIP	▪ **Notifications:** Registration error or timeout ▪ **Logged Events:** - End of call (Call Detail Record logging) - SIP messages logging (optional - for debugging)
Network Connections	▪ **Notifications:** Connection up / down
Security	▪ **Logged Events:** Security log (configurable)
System	▪ **Notifications:** - System restart - Firmware / configuration update ▪ **Logged Events:** Debug-level logging (optional)

Note that the terms Alarm and Notification represent the same thing. The difference between alarm/notification and logging is that an alarm is normally used to represent an abnormal event (e.g. registration error), while logged events can represent either regular events (e.g. end of call) or abnormal events.

The table below shows the event severity levels defined in MP-20x. Typically, events with severity of Error or Emergency are notified in addition to being logged.

Table 12-4: Severity of Logged Events

Severity	Decsription
Debug	Debug-level messages.
Notice	Normal but significant condition. Notices requiring attention at a later time. Non-error conditions that might require special handling.
Error	Recoverable / temporary error condition.
Emergency	System is unusable. The most severe messages that prevent continuation of operation, such as immediate system shutdown.

12.2 Remote Configuration and Management Interfaces

The following interfaces are available on MP-20x for remote configuration and management:

- Web server (GUI) over HTTP/HTTPS
- TR-069 and TR-104
- SNMP
- Syslog
- Firmware or configuration file download via HTTP/HTTPS/FTP/ TFTP
- CLI over Telnet/SSH

The table below lists the possible operations over these different interfaces:

Table 12-5: Operations per Configuration/Management Interface

Operation	Web GUI	TR-069	SNMP	Syslog	File D/L	CLI
Configuration Update	Yes	Yes	Yes	No	Yes	Yes
Firmware Upgrade	Yes	Yes	Yes	No	Yes	Yes
Status Monitoring	Yes	Yes	Yes	No	No	Yes
Debugging and Diagnostics	Yes	No	No	Yes	No	Yes

Service providers can choose to combine several management interfaces, for example, Automatic file download for configuration and firmware updates plus SNMP for alarms.

12.2.1 Embedded Web Server

MP-20x provides an embedded Web server with a rich Graphical User Interface (GUI). The Web server can be accessed from the local LAN interface (e.g. by the home user) or from the WAN interface (e.g. by the service provider support personnel). The Web GUI provides easy and intuitive configuration of all MP-20x parameters (i.e., VoIP, network interfaces, security, QoS and advanced system settings). In addition, the Web GUI provides status monitoring pages, diagnostic pages and enabled firmware upgrade.

Typically, service providers do not want to configure each MP-20x manually and therefore, they do not use the Web server in live deployments. However, the Web server is still useful for:

- Trying different configurations in the lab during the integration phases
- Creating mass-configuration template files
- Debugging special customer problems (by accessing the Web server from the WAN interface)

Since the Web server allows all configuration and management operations, it is important to protect it. The following security measures are available:

- The Web server is user and password protected. Several users can be defined. A special user with limited-access (only to the 'Quick Setup' screen) can be defined.
- The access to the Web server can be blocked from the WAN and/or LAN interfaces.
- Access to the Web server can be limited to specific IP addresses.
- Secured HTTP (HTTPS) is supported. It is possible to enable HTTPS-only, if required.
- The HTTP and/or HTTPS port can be modified (from the default 80 and 8080).

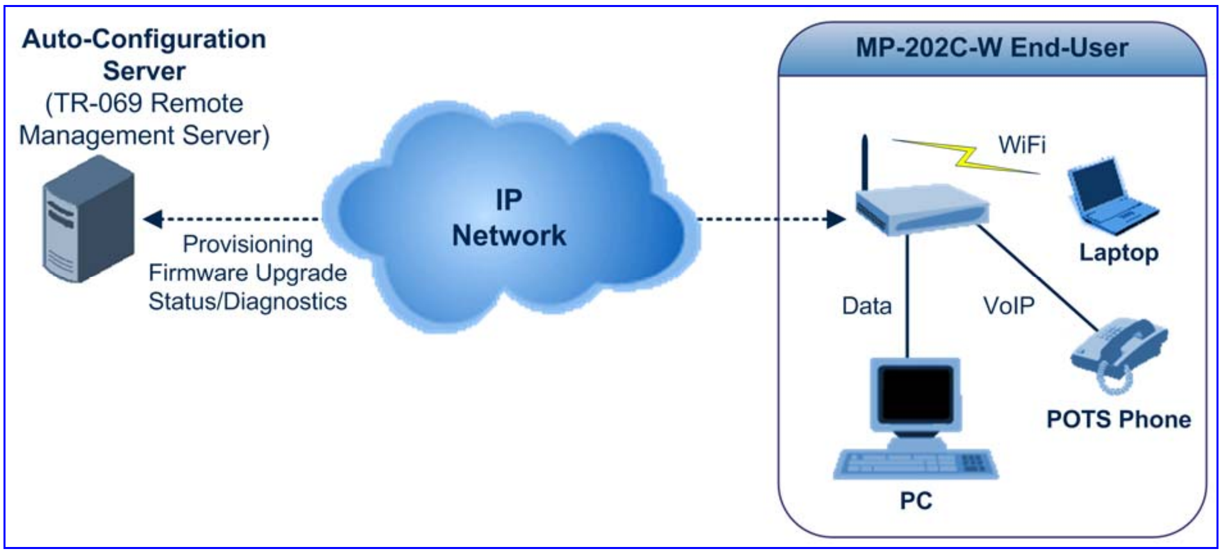
12.2.2 TR-069 and TR-104 CPE WAN Management Protocol

TR-069 is a WAN management protocol intended for communication between Customer Premise Equipment (CPE) or residential devices (such as MP-20x), and an Auto-Configuration Server (ACS), residing on the service provider's side. 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 theMP-20x. Such a protocol is useful, for example, for remotely and securely controlling MP-20x by the CPE provider. The standard is published by the DSL Forum. TR-069 runs over SOAP/HTTP and enables device configuration, management (including firmware upgrade), and status monitoring. TR-104 is an extension of TR-069 for VoIP configuration and monitoring.

The TR standards are published by the DSL forum:

- **TR-069:** http://www.broadband-forum.org/technical/download/TR-069.pdf
- **TR-104:** http://www.broadband-forum.org/technical/download/TR-104.pdf

Figure 12-3: 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.

Notes:

- MP-20x was tested for interoperability with two ACS vendors – Motive and FriendlyTR69. Working with other ACS types may require specific interoperability effort.
- The parameter values in the subsequent tables are sample values only taken from an ACS.

12.2.2.1 Configuring MP-20x via TR-069 and TR-104

TR-069 allows basic configuration of MP-20x. The configuration is defined in a hierarchical tree-like structure according to the TR-069 standard.

12.2.2.1.1 Configuring the WAN Interface

Table 12-6: InternetGatewayDevice.WANDevice.i.WANConnectionDevice.i.WANIPConnection.i

TR-069/TR-104 Parameter	Configuration File Parameter	Description
AddressingType	**mt_cwmp_param_wan_conn_ip_addressing_type_get/set**	The method used to assign an address to the WAN side interface of the CPE for this connection: ▪ "DHCP" ▪ "Static"
ConnectionStatus	**mt_cwmp_param_wan_conn_ip_status_get**	Current status of the connection: ▪ "Unconfigured" ▪ "Connecting" ▪ "Connected" ▪ "PendingDisconnect" ▪ "Disconneting" ▪ "Disconnected"
ConnectionType	**mt_cwmp_param_wan_conn_ppp_type_get**	Specifies the connection type of the connection instance: ▪ "Unconfigured" ▪ "IP_Routed" ▪ "DHCP_Spoofed" ▪ "PPPoE_Bridged" ▪ "PPPoE_Relay" ▪ "PPTP_Relay" ▪ "L2TP_Relay"
DefaultGateway	**mt_cwmp_param_wan_conn_ip_default_gateway_get/set**	The IP address of the default gateway for this connection. This parameter is configurable only if the AddressingType is Static.
DNSEnabled	**mt_cwmp_param_wan_conn_ip_dns_enabled_get/set**	Whether or not the device should attempt to query a DNS server across this connection.
DNSOverrideAllowed	**mt_cwmp_param_wan_conn_ip_dnsoverrideallowed_get/set**	Whether or not a manually set, non-empty DNS address can be overridden by a DNS entry received from the WAN.
DNSServers	**mt_cwmp_param_wan_conn_xxx_dnsservers_get/set(i)**	Comma-separated list of DNS server IP addresses for this connection. Support for more than three DNS Servers is optional.
Enable	**mt_cwmp_param_wan_conn_xxx_enable_get/set(1)**	Enables or disables the connection instance. On creation of a WANIPConnection instance, it is initially disabled.

TR-069/TR-104 Parameter	Configuration File Parameter	Description
ExternalIPAddress	**mt_cwmp_param_wan_conn_xxx_externalip_get(i)**	The external IP address used by NAT for this connection. This parameter is configurable only if the AddressingType is Static.
MaxMTUSize	**mt_cwmp_param_wan_conn_ip_max_mtu_size_get/set(i)**	The maximum allowed size of an Ethernet frame from LAN-side devices.
Name	**mt_cwmp_param_wan_conn_xxx_name_get/set(i)**	User-readable name of this connection.
NATEnabled	**mt_cwmp_param_wan_conn_xxx_nat_enabled_get/set(i)**	Indicates if NAT is enabled for this connection.
PortMappingNumberOfEntries	**-**	Total number of port mapping entries.
PossibleConnectionTypes	**-**	A comma-separated list indicating the types of connections possible for this connection instance. Each element of the list is an enumeration of: ▪ "Unconfigured" ▪ "IP_Routed" ▪ "IP_Bridged"
RouteProtocolRx	**mt_cwmp_param_wan_conn_xxx_route_protocol_rx_get/set**	Defines the Rx protocol to be used: ▪ "Off" ▪ "RIPv1" (Optional) ▪ "RIPv2" (Optional) ▪ "OSPF" (Optional)
RSIPAvailable	**mt_cwmp_param_wan_conn_xxx_rsip_available_get(i)**	Indicates if Realm-specific IP (RSIP) is available as a feature on MP-20x.
ShapingRate	**-**	Rate to shape this connection's egress traffic to. If less than or equal to 100, in percentages of the rate of the highest rate-constrained layer over which the packet travels on egress. The rate is limited over the window period specified by ShapeWindow. If greater than 100, in bits per second. A value of -1 indicates no shaping.
SubnetMask	**lan_host_config_management_get/set** **rg_conf dhcps/ netmask**	Subnet mask of the WAN interface. This parameter is configurable only if the AddressingType is Static.
SpecVersion	""	Currently, 1.0 is the only available version.
Uptime	**-**	The time in seconds that this connection has been up.

12.2.2.1.2 Configuring the LAN Interface

Table 12-7: InternetGatewayDevice.LANDevice.i.LANEthernetInterfaceConfig

TR-069/TR-104 Parameter	Configuration File Parameter	Description
Enable	**device_eic_enable_get/set**	Enables or disables this interface.
MACAddress	**device_mac_address_get**	The physical address of the interface.
MaxBitRate	**device_max_bit_rate_get**	The maximum upstream and downstream bit rate available for this connection: ▪ "10" ▪ "100" ▪ "1000" ▪ "Auto"
Status	**device_status_get**	The status of the interface: ▪ "Up" ▪ "NoLink" ▪ "Error" ▪ "Disabled"

Table 12-8: InternetGatewayDevice.LANDevice.i.LANHostConfigManagement

TR-069/TR-104 Parameter	Configuration File Parameter	Description
AllowedMACAddresses	**allowed_mac_addresses_get/set**	Represents a comma-separated list of hardware addresses that are allowed to connect to this connection if MACAddressControlEnabled is 1 for a given interface.
DHCPLeaseTime	**dhcp_lease_time_get/set**	Specifies the lease time in seconds of client assigned addresses. A value of -1 indicates an infinite lease.
DHCPRelay	**dhcp_relay_get/set**	Determines if the DHCP server performs the role of a server (0) or a relay (1) on the LAN interface.
DHCPServerEnable	**lan_host_config_management_get/set** **rg_conf dhcps/enable**	Enables or disables the DHCP server on the LAN interface.
DNSServers	**dhcps_dns_servers_get/set**	Comma-separated list of DNS servers offered to DHCP clients. Support for more than three DNS Servers is optional.
DomainName	**domain_name_get/set**	Sets the domain name for clients on the LAN interface.

TR-069/TR-104 Parameter	Configuration File Parameter	Description
IPRouters	**ip_routers_get/set**	Comma-separated list of IP addresses of routers on this subnet. Also known as default gateway. Support for more than one Router address is optional.
MaxAddress	**lan_host_config_management_get/set** **rg_conf dhcps/end_ip**	Specifies the last address in the pool to be assigned by the DHCP server on the LAN interface.
MinAddress	**lan_host_config_management_get/set** **rg_conf dhcps/start_ip**	Specifies the first address in the pool to be assigned by the DHCP server on the LAN interface.
SubnetMask	**lan_host_config_management_get/set** **rg_conf dhcps/ netmask**	Specifies the client's network subnet mask.

12.2.2.1.3 Configuring VoIP via TR-104

Table 12-9: InternetGatewayDevice.Services.VoiceService.i.Capabilities

TR-069/TR-104 Parameter	Configuration File Parameter	Description
ButtonMap	-	Support for a configurable button map. A true value indicates support for a configurable button map via the VoiceService.{i}.VoiceProfile.{i}.ButtonMap object.
DSCPCoupled	-	A true value indicates that the CPE is constrained such that transmitted call control packets use the same DSCP marking as transmitted RTP packets. If the value is true, the CPE must not support the DSCPMark parameter for call control.
EthernetTaggingCoupled	-	A true value indicates that the CPE is constrained such that transmitted call control packets use the same Ethernet tagging (VLAN ID Ethernet Priority) as transmitted RTP packets. If the value is true, the CPE must not support the VLANIDMark or EthernetPriorityMark parameters within a call control object (e.g., SIP, MGCP, or H323).

TR-069/TR-104 Parameter	Configuration File Parameter	Description
FaxPassThrough	-	Support for fax pass-through. A true value indicates support for the parameter VoiceService.{i}.VoiceProfile.{i}.FaxPassThrough. (True if voip/audio/fax/fax_transport_mode equals Bypass)
FaxT38	-	Support for T.38 fax. A true value indicates support for the object VoiceService.{i}.VoiceProfile.{i}.FaxT38.
MaxLineCount	**voip/num_of_fxs_lines**	Maximum number of lines supported across all profiles.
MaxProfileCount	-	Maximum number of distinct voice profiles supported.
MaxSessionCount	-	Maximum number of voice sessions supported across all lines and profiles. (This might differ from MaxLineCount if each line can support more than one session for CPE provided conference calling. This value can be less than the product of MaxLineCount and MaxSessionsPerLine.)
MaxSessionsPerLine	-	Maximum number of voice sessions supported for any given line across all profiles. A value greater than one indicates support for CPE provided conference calling.
ModemPassThrough	-	Support for modem pass-through. A true value indicates support for the parameter VoiceService.{i}.VoiceProfile.{i}.ModemPassThrough.
NumberingPlan	-	Support for a configurable numbering plan. A true value indicates support for a configurable numbering plan via the VoiceService.{i}.VoiceProfile.{i}.NumberingPlan object.
PSTNSoftSwitchOver	-	A true value indicates MP-20x is capable of supporting the PSO_Activate Facility Action, which allows a call to be switched to a PSTN FXO. **Note:** Currently, this parameter is not supported.
Regions	**pkg\mgt\lib\mgt_regional_settings.c slic_dsp_general_and_regional_settings_params_array**	Comma-separated list of geographic regions supported by MP-20x. Each item in the list must be an alpha-2 (two-character alphabetic) country code as specified by ISO 3166. An empty list indicates that MP-20x does not support region-based customization. **Note:** This format is currently not supported.

TR-069/TR-104 Parameter	Configuration File Parameter	Description
RingGeneration	-	Support for ring generation. A true value indicates support for control of ring generation via the VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Ringer object. A true value also indicates that the RingDescriptionsEditable, PatternBasedRingGeneration and FileBasedRingGeneration parameters in this object are present.
RTCP	-	Support for RTCP.
RTPRedundancy	-	Support for RTP payload redundancy as defined in RFC 2198. A true value indicates support for VoiceService.{i}.VoiceProfile.{i}.RTP.Redundancy.
SignalingProtocols	**voip/signalling/protocol**	Signal protocol: ▪ "SIP" ▪ "MGCP" Each entry can be appended with a version indicator in the form "/X.Y". For example: "SIP/2.0". **Note:** Only one protocol is supported at a time.
SRTP	-	Support for SRTP. **Note:** Currently, SRTP is not supported.
ToneGeneration	-	Support for tone generation. A true value indicates support for the object VoiceService.{i}.VoiceProfile.{i}.Tone. A true value also indicates that the ToneDescriptionsEditable, PatternBasedToneGeneration and FileBasedToneGeneration parameters in this object are present.
VoicePortTests	-	Support for remotely accessible voice-port tests. A true value indicates support for the VoiceService.{i}.PhyInterface.{i}.Tests object.

Table 12-10: InternetGatewayDevice.Services.VoiceService.i.Capabilities.Codecs

TR-069/TR-104 Parameter	Configuration File Parameter	Description
Codec	**voip/codec/i/name**	Identifier of the type of codec.
EntryID	**voip/codec/i/**	Unique identifier for each entry in the table.
PacketizationPeriod	**voip/codec/i/ptime**	Comma-separated list of supported packetization periods (in milliseconds), or continuous ranges of packetization periods. Ranges are indicated as a hyphen-separated pair of unsigned integers. For example: ▪ “20” indicates a single discrete value. ▪ “10, 20, 30” indicates a set of discrete values. ▪ “5-40” indicates a continuous inclusive range. ▪ “5-10, 20, 30” indicates a continuous range in addition to a set of discrete values. A range must only be indicated if all values within the range are supported. **Note:** Currently, only a single ptime per codec is supported.

Table 12-11: InternetGatewayDevice.Services.VoiceService.i.VoiceProfile

TR-069/TR-104 Parameter	Configuration File Parameter	Description
DTMFMethod	**voip/out_of_band_dtmf**	Method by which DTMF digits must be passed: ▪ “InBand” ▪ “RFC2833” ▪ “SIPInfo

TR-069/TR-104 Parameter	Configuration File Parameter	Description
Enable	-	Enables or disables all lines in this profile, or places it into a quiescent state: ▪ "Disabled" ▪ "Quiescent" ▪ "Enabled" On creation, a profile must be in the Disabled state. In the Quiescent state, in-progress sessions remain intact, but no new sessions are allowed. Support for the Quiescent state in a MP-20x is optional. If this parameter is set to "Quiescent" in a MP-20x that does not support the Quiescent state, it must treat it the same as the Disabled state.
Name	-	String to easily identify the profile instance. **Note:** Currently, this is not supported.
NumberOfLines	**voip/num_of_fxs_lines**	Number of instances of Line within this VoiceProfile.

Table 12-12: InternetGatewayDevice.Services.VoiceService.i.VoiceProfile.i.SIP

TR-069/TR-104 Parameter	Configuration File Parameter	Description
OutboundProxy	**voip/ signalling/sip/sip_outbound_proxy/addr**	Host name or IP address of the outbound proxy. If a non-empty value is specified, the SIP endpoint must send all SIP traffic (requests and responses) to the host indicated by this parameter and the port indicated by the OutboundProxyPort parameter. This must be done regardless of the routes discovered using normal SIP operations, including use of Route headers initialized from Service-Route and Record-Route headers previously received. The OutboundProxy value is not used to generate the URI placed into the Route header of any requests.
OutboundProxyPort	**voip/ signalling/sip/sip_outbound_proxy/proxy**	Destination port for connecting to the outbound proxy. This parameter must be ignored unless the value of the OutboundProxy parameter in this object is non-empty.
ProxyServer	**voip/signalling/sip/proxy_address** **or** **voip/signalling/sip/sip_registrar/addr**	Host name or IP address of the SIP proxy server.

TR-069/TR-104 Parameter	Configuration File Parameter	Description
ProxyServerPort	**voip/signalling/sip/proxy_port or voip/signalling/sip/sip_registrar/port**	Destination port for connecting to the SIP server.
ProxyServerTransport	**voip/signalling/sip/transport_protocol**	Transport protocol for connecting to the SIP server. Must be chosen from among the transports supported.
RegisterExpires	**voip/signalling/sip/proxy_timeout**	Register request Expires header value (in seconds).
RegistrarServerTransport	**voip/signalling/sip/transport_protocol**	Transport protocol for connecting to the SIP server. Must be chosen from among the transports supported.
UserAgentPort	**voip/signalling/sip/port**	Port for incoming call control signaling.
UserAgentTransport	**voip/signalling/sip/transport_protocol**	Transport protocol for incoming call control signaling.

12.2.2.1.4 Upgrading Firmware via TR-069

TR-069 contains a built-in mechanism for MP-20x firmware upgrade.

12.2.2.2 Monitoring MP-20x Status via TR-069 and TR-104

The service provider can monitor the status of MP-20x via TR-069 and TR-104.

12.2.2.2.1 Device Information

Table 12-13: InternetGatewayDevice.DeviceInfo

TR-069/TR-104 Parameter	Configuration File Parameter	Description
Description	**manufacturer/description**	A full description of MP-20x (string).
DeviceLog	“”	Vendor-specific log(s).
HardwareVersion	**Manufacturer/hardware/version**	A string identifying the particular MP-20x model and version.
Manufacturer	**manufacturer/vendor_name**	A string identifying the manufacturer of MP-20x, i.e., AudioCodes.
ManufacturerOUI	**manufacturer/vendor_oui**	Organizationally unique identifier of the device manufacturer. Represented as a six hexadecimal-digit value using all upper-case letters and including any leading zeros.
ModelName	**manufacturer/model_number**	A string identifying the model name of MP-20x.

TR-069/TR-104 Parameter	Configuration File Parameter	Description
ProductClass	**manufacturer/product_class**	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 SerialNumber parameter is unique.
ProvisioningCode	**cwmp/provisioning_code**	Identifier of the primary service provider and other provisioning information, which may be used by the Server to determine service provider-specific customization and provisioning parameters. If non-empty, this argument must be in the form of a hierarchical descriptor with one or more nodes specified. Each node in the hierarchy is represented as a 4-character sub-string, containing only numerals or upper-case letters. If there is more than one node indicated, each node is separated by a "." (dot). For example, “TLCO” and “TLCO.GRP2”.
SerialNumber	**Manufacturer/hardware/serial_num**	Serial number of MP-20x.
SoftwareVersion	**system/external_version**	A string identifying the software version currently installed in MP-20x. To allow version comparisons, this element must be in the form of dot-delimited integers, where each successive integer represents a more minor category of variation. For example, 3.0.21 where the components mean Major.Minor.Build.
UpTime	-	Time in seconds since MP-20x was last reset.

12.2.2.2.2 WAN Status

Table 12-14: InternetGatewayDevice.WANDevice.i.WANConnectionDevice.i. WANIPConnection.i.Stats

TR-069/TR-104 Parameter	Configuration File Parameter	Description
EthernetBytesReceived	**mt_cwmp_param_wan_conn_ip_stats_get (STAT_RX_BYTES)**	Total number of bytes received over all connections within the same WANConnectionDevice that share a common MAC address since MP-20x was last reset.
EthernetBytesSent	**mt_cwmp_param_wan_conn_ppp_stats_get (STAT_TX_BYTES)**	Total number of bytes sent over all connections within the same WANConnectionDevice that share a common MAC address since MP-20x was last reset.
EthernetPacketsReceived	**mt_cwmp_param_wan_conn_ppp_stats_get (STAT_RX_PACKETS)**	Total number of Ethernet packets received over all connections within the same WANConnectionDevice that share a common MAC address since MP-20x was last reset.
EthernetPacketsSent	**mt_cwmp_param_wan_conn_ppp_stats_get**	Total number of Ethernet packets sent over all connections within the same WANConnectionDevice that share a common MAC address since MP-20x was last reset.

12.2.2.2.3 LAN Status

Table 12-15: InternetGatewayDevice.LANDevice.i.LANEthernetInterfaceConfig.i.Stats

TR-069/TR-104 Parameter	Configuration File Parameter	Description
BytesReceived	**mt_voip_get_state (line, state)**	Total number of bytes received over the interface since MP-20x was last reset.
BytesSent	**mt_voip_get_state(line, state)**	Total number of bytes sent over the interface since MP-20x was last reset.
PacketsReceived	**mt_voip_get_state(line, state)**	Total number of packets received over the interface since MP-20x was last reset.
PacketsSent	**mt_voip_get_state(line, state)**	Total number of packets sent over the interface since MP-20x was last reset.

12.2.2.2.4 VoIP Status via TR-104

Table 12-16: InternetGatewayDevice.Services.VoiceService.i.VoiceProfile.i.Line.i.Stats

TR-069/TR-104 Parameter	Configuration File Parameter	Description
ResetStatistics	-	When set to one, it resets the statistics for this voice line. Always False when read.
PacketsSent	**mt_voip_get_state(line, state)**	Total number of RTP packets sent for this line.
PacketsReceived	**mt_voip_get_state(line, state)**	Total number of RTP packets received for this line.
BytesSent	**mt_voip_get_state(line, state)**	Total number of RTP payload bytes sent for this line.
BytesReceived	**mt_voip_get_state(line, state)**	Total number of RTP payload bytes received for this line.
PacketsLost	**mt_voip_get_state(line, state)**	Total number of RTP packets that have been lost for this line.
Overruns	-	Total number of times the receive jitter buffer has overrun for this line.
Underruns	-	Total number of times the receive jitter buffer has underrun for this line.
IncomingCallsReceived	-	Total incoming calls received.
IncomingCallsAnswered	-	Total incoming calls answered by the local user.
IncomingCallsConnected	-	Total incoming calls that successfully completed call setup signaling.
IncomingCallsFailed	-	Total incoming calls that failed to successfully complete call setup signaling.
OutgoingCallsAttempted	-	Total outgoing calls attempted.
OutgoingCallsAnswered	-	Total outgoing calls answered by the called party.
OutgoingCallsConnected	-	Total outgoing calls that successfully completed call setup signaling.
OutgoingCallsFailed	-	Total outgoing calls that failed to successfully complete call setup signaling.
CallsDropped	-	Total calls that were successfully connected (incoming or outgoing), but dropped unexpectedly while in progress without explicit user termination.
TotalCallTime	-	Cumulative call duration (in seconds).

TR-069/TR-104 Parameter	Configuration File Parameter	Description
ServerDownTime	-	The number of seconds MP-20x is unable to maintain a connection to the server. Applies only to SIP.
ReceivePacketLossRate	**mt_voip_get_state(line, state)**	Current receive packet loss rate (in percentage).
FarEndPacketLossRate	-	Current far-end receive packet lost rate (in percentage).
ReceiveInterarrivalJitter	-	Current receive interarrival jitter (in microseconds).
FarEndInterarrivalJitter	-	Current Interarrival jitter (in microseconds) as reported from the far-end device via RTCP.
RoundTripDelay	**mt_voip_get_state**	Current round-trip delay (in microseconds).
AverageReceiveInterarrivalJitter	-	Average receive interarrival jitter (in microseconds) since the beginning of the current call.
AverageFarEndInterarrivalJitter	-	Average far-end interarrival jitter (in microseconds) since the beginning of the current call.
AverageRoundTripDelay	-	Average round-trip delay (in microseconds) since the beginning of the current call. This is the average of the RoundTripDelay statistics accumulated each time the delay is calculated.

12.2.2.3 Security Concerns and Measures

The CPE WAN Management Protocol is designed to allow a high degree of security in the interactions that use it. The CPE WAN Management Protocol is designed to prevent tampering with the transactions that take place between a CPE and ACS, provide confidentiality for these transactions, and allow various levels of authentication.

The following security mechanisms are incorporated in this protocol:

- The protocol supports the use of SSL/TLS for communications transport between CPE and ACS. This provides transaction confidentiality, data integrity, and allows certificate-based authentication between the CPE and ACS.
- The HTTP layer provides an alternative means of CPE authentication based on shared secrets.

12.2.3 SNMP

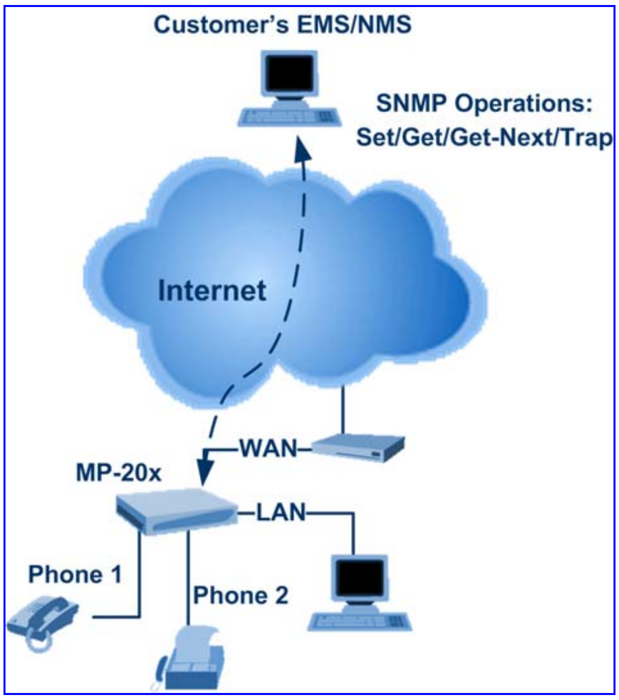
Simple Network Management Protocol (SNMP) is used in network management systems to configure and monitor network-attached devices. SNMP is an IETF standard defined by RFC 1157, 1441 and additional RFCs for specific Management Information Base (MIBs).

MP-20x contains an embedded SNMP agent and supports SNMPv1, SNMPv2 and partially supports SNMPv3. For monitoring of the network interfaces, the standard SNMP MIB-II (RFC 1213) is supported. For more options, a proprietary MIB, AC-MP20X-MIB includes the following sections:

- **acMP20xConfig:** for changing MP-20x's configuration
- **acMP20xStatus:** for monitoring MP-20x's status
- **acMP20xAlarms:** for receiving notifications (alarms) from MP-20x

The figure below shows the SNMP network architecture:

Figure 12-4: SNMP Network Architecture



12.2.3.1 Configuring MP-20x via SNMP

The acMP20xConfig MIB section is structured in a similar hierarchy as MP-20x's Web GUI. Each parameter in the MIB has a matching parameter in the Web GUI and a matching parameter in the gateway's configuration file. The MIB file defines the valid range and the default value for each parameter. Typically, the customer integrates the MP20x MIB into the customer's Network Management System (NMS) to automate the configuration process.

Note: A special MIB object is defined to allow MP-20x firmware upgrade triggered by SNMP. The object acMP20xRemoteUpdate triggers a remote upgrade from the SNMP-configured URL.

12.2.3.2 Monitoring the MP-20x via SNMP

SMNP can be used to monitor the status of MP-20x. VoIP-related monitoring is performed via the proprietary MIB acMP20x. Other parameters are available in the standard MIB-II.

12.2.3.2.1 VoIP Monitoring

The acMp20xStatus section allows the service provider to get the current MP-20x status. The list below shows the available objects.

```
acMP20xStatus
    acMP20xStatusVoIP
          acMP20xStatusVoIPLinesTable
acMP20xLinePhoneState – on-hook / off-hook / ringing
acMP20xLineRegistrationState – not registered / registered /
registration error
                acMP20xLineCallsTable
                      acMP20xCallOrigine – Incoming / outgoing
                      acMP20xCallRemoteNumber – Remote phone
number
                      acMP20xCallRemoteID – Remote SIP ID
                      acMP20xCallDuration – Call duration in ms
                      acMP20xCallType – Voice/Fax/Modem
                      acMP20xCallEncoder – Tx codec type
                      acMP20xCallDecoder – Rx codec type
                      acMP20xCallPacketsSent – Number of RTP
                      packets sent
                      acMP20xCallPacketsReceived – Number of RTP
packets sent
                      acMP20xCallBytesSent – Number of payload
bytes sent
                      acMP20xCallBytesReceived – Number of payload
bytes received
                      acMP20xCallPacketsLost – Number of packets
lost
                      acMP20xCallLostPercentage – Packet loss
percentage
                      acMP20xCallJitter – Average call jitter in ms
                      acMP20xCallRoundTripDelay – Average call
round-trip delay in ms
```

12.2.3.2.2 Network Interfaces and System Monitoring

Status monitoring of the system and network interfaces can be done via the standard MIB-II (iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1)). The following table shows some of the information elements available via MIB-II:

Table 12-17: Table 3-13: Information Elements Available via MIB-II

Section	Available Information
system	▪ Description ▪ Version Information ▪ Up-time
interfaces	**Information per network interface:** ▪ Description ▪ Type ▪ Speed ▪ MAC address ▪ Traffic statistics ▪ Errors
ip	Assigned IP addresses and IP-related parameters
icmp, udp, tcp	Transport-protocol specific statistical information
ifMIB	Information about network interfaces per RFC 2233

12.2.3.3 Security Concerns and Measures

Since SNMP allows write-access to configuration parameters, it is important to protect this interface. The following security measures are available:

- A community string (password) can be defined for read-only access and for read/write access.
- It is possible to limit access to SNMP to a trusted peer (single IP address or a range of addresses).
- SNMPv3 provides an significant security improvement over SNMPv1/2. Version 2.8.0 will support SNMPv3 and will allow the service provider to configure SNMPv3 security parameters.
- SNMP traffic can be allowed over an IPSec secured connection – check availability with AudioCodes.

12.2.4 Syslog

Syslog is a standard protocol for reporting and logging of messages over IP network and is defined by RFC 3164. MP-20x enables the service provider to configure a Syslog server and a severity level above which errors are sent to the server. Typically, only error-level messages should be sent to the Syslog server (in order not to flood it with irrelevant debug-level information). For debugging, it is possible to temporarily allow logging for debug-level messages (e.g. for SIP messages).

Many free Syslog servers exist, including Kiwi Syslog Daemon' (http://www.kiwisyslog.co'm http://www.kiwisyslog.com).

Note: Since Syslog is used only to output messages from MP-20x, it does not contain any security concerns.

12.2.5 Automatic File Download

A practical, straight-forward and easy to implement method for mass configuration and firmware update is automatic file download from a remote file server (via HTTP, FTP, or TFTP). This method is used by many service providers.

12.2.5.1 Firmware File Download

MP-20x's firmware files contain information about the target product type and the firmware version information.

12.2.5.2 Configuration File Download

MP-20x supports two configuration file formats, a ***.conf** file and an ***.ini** file. Both files define the same parameters, but in a different format; the *.conf file has a hierarchical tree-like structure and the *.ini file is "flat" (defining the full path for each parameter).

As with the firmware file, the configuration file can be “pushed” to MP-20x via the Web server or “pulled” by MP-20x from a remote server. This section refers only to the second option.

When MP-20x downloads a file from a remote server, it performs the following actions:

- Decrypts the file, if it is encrypted.
- Checks that the file version is later than the current configuration file version (if it is not later, the new configuration is not used).

- Checks the software version with which the configuration file was created (if the file was created with a later software version, it is not used).
- Merges the configuration file with the current configuration:
  - Parameters that appear in the new file are modified or added
  - Parameters that do not appear in the new file remain in their existing value

Notes:

- It is recommended that the configuration file (that is downloaded from the network), contains only the small subset of parameters that the service provider needs to update remotely.
- To create the configuration file, it is recommended to use a MP-20x that is restored to factory settings, modify the required parameters using the Web GUI, and then upload the configuration file from MP-20x with the option to get only the modified configuration fields enabled.

12.2.5.3 Security Concerns and Measures

The main security hazard in automatic file download is that a hacker can force MP-20x to download a file from the hacker's server instead of the service provider’s legitimate server. Another concern is exposing information such as the SIP proxy IP address and user and password information in the configuration file (if the hacker is sniffing the network).

The following security measures are available to prevent this:

- The configuration file can be encrypted using 3DES with pre-configured key. This prevents the user from learning the format of the file and obtaining information from it.
- HTTPS can be used to further encrypt the transport.
- HTTPS certificates can be used to allow MP-20x to authenticate the server and also to prevent the user from acquiring the file from the server.

12.2.6 Telnet CLI

MP-20x features a Command Line Interface (CLI) over Telnet. The CLI enables the service provider to manage MP-20x (e.g. reboot, force a firmware upgrade), to obtain information about the status of the device (e.g. VoIP calls, network interfaces, version information), to change the configuration and to perform different debugging tasks (e.g. enable debug logging, enable packet recording).

Typically, the CLI interface is only used for debugging and diagnostics, since it does not allow mass configuration and monitoring.

Since the CLI allows all configuration and management operations, it is important to protect it. The following security measures are available:

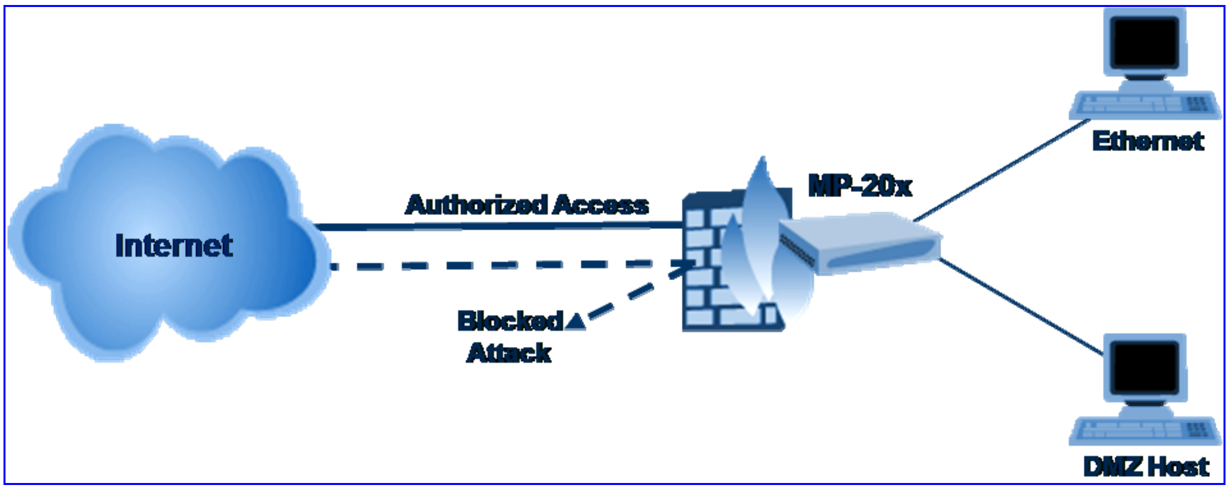
- The CLI is user and password protected (same as the Web).
- Telnet access can be blocked from the WAN and/or LAN interfaces.
- It is possible to limit Telnet access to specific IP addresses.
- Future versions will support SSH.

13 Security

MP-20x'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.

Figure 13-1: Firewall in Action



MP-20x 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.

MP-20x 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:

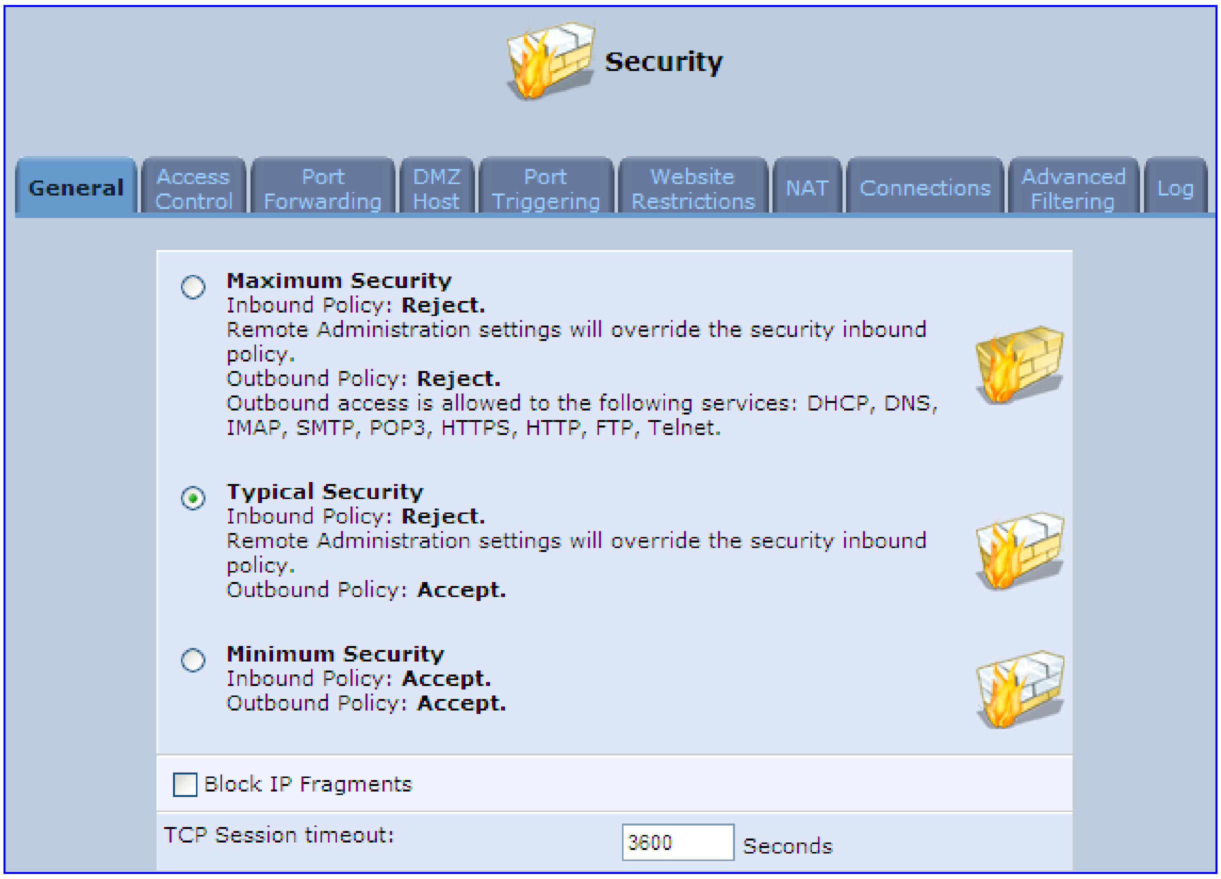
- The 'General' screen allows you to choose the security level for the firewall (refer to' General Security Level Settings' on page 178).
- The 'Access Control' screen can be used to restrict access from the home network to the Internet (refer to 'Local Servers (Port Forwarding)' on page 182).
- The '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 182).
- 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 186).
- 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 243).

- 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 189).
- 'Advanced Filtering' allows you to implicitly control the firewall setting and rules (refer to 'Advanced Filtering' on page 196).
- 'Security Log' allows you to view and configure the firewall Log (refer to Security Log).

13.1 General Security Level Settings

Use the 'Security Settings' screen to configure the Telephone Adapter's basic security settings.

Figure 13-2: 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: DHCP, DNS, IMAP, SMTP, POP3, HTTPS, HTTP, FTP, Telnet.

[✓] **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

TCP Session timeout: 3600 Seconds

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 MP-20x) or rejected (barred from passing through MP-20x) 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") are also 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 MP-20x, the firewall identifies 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 allows this request to pass out onto the Internet (refer to 'WAN PPPoE' on page 110 for more on setting access controls). When the Web page is returned from the Web server the firewall associates it with this session and allows 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 MP-20x: Minimum, Typical, and Maximum (the default setting). The table below summarizes the behavior of MP-20x for each of the three security levels.

Table 13-1: 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 180'.

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 are not blocked outbound, even at Maximum Security Level.

➢ To configure MP-20x'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' check box 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 some UDP-based services make legitimate use of IP fragments. You need to allow IP fragments to pass into the home network to make use of these select services.

3. In the 'TCP Session timeout' field, enter the time-to-live (TTL) in units of hours for TCP sessions. The valid range is 1 to 120 hours (default is an hour).

4. Click **OK** to save the changes.

13.2 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.

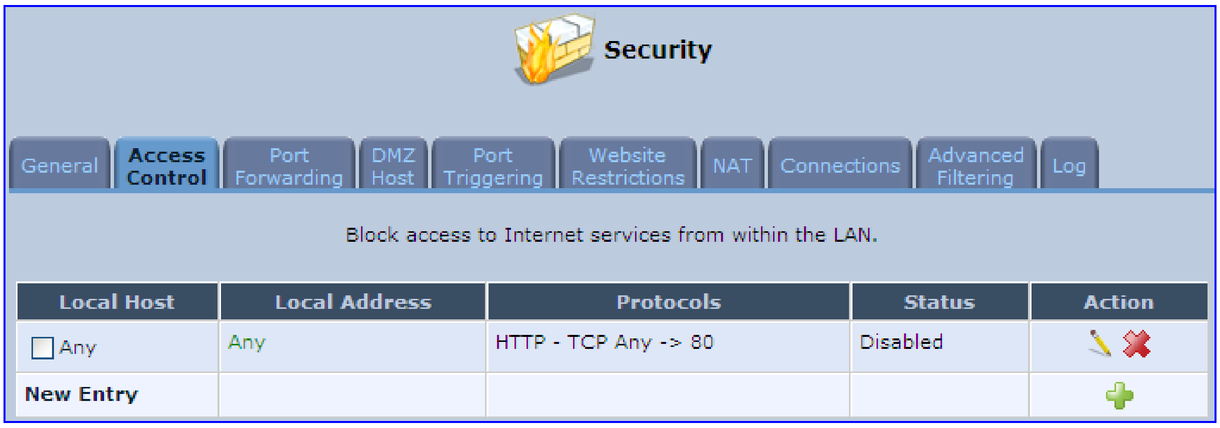
Access Control defines restrictions on the types of requests that may pass from the home network out to the Internet, and thus may block traffic flowing in both directions. In the e-mail example given above, you may prevent computers in the home network from receiving e-mail by blocking their *outgoing* 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. From the sidebar menu, click the **Security** menu, and in the screen 'Security', click the **Access Control** tab; the screen 'Access Control' opens.

Figure 13-3: Access Control

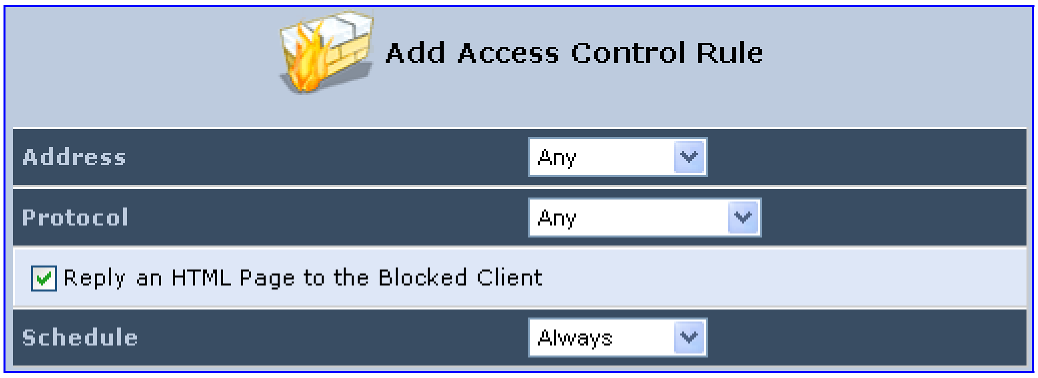


Block access to Internet services from within the LAN.

Local Host	Local Address	Protocols	Status	Action
☐ Any	Any	HTTP - TCP Any -> 80	Disabled	
New Entry				

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

Figure 13-4: Add Access Control Rule



Add Access Control Rule

Address	Any
Protocol	Any
✓ Reply an HTML Page to the Blocked Client	
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 specific computer address in your LAN. If you choose the 'Specify Address' option, the screen refreshes, 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 specific 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 takes 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 the **Edit** icon 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 takes 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 **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.

13.3 Port Forwarding

By default, MP-20x 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 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 MP-20x. You must select the application's protocol and the local IP address of the computer using or providing the service. If required, you can add new protocols in addition to the most common ones provided by MP-20x.

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 MP-20x 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 provides 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 hosts the Web server. When an Internet user points her browser to the external IP address of MP-20x, 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 MP-20x 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 is now forwarded to the PC running the Web server on port 8080.

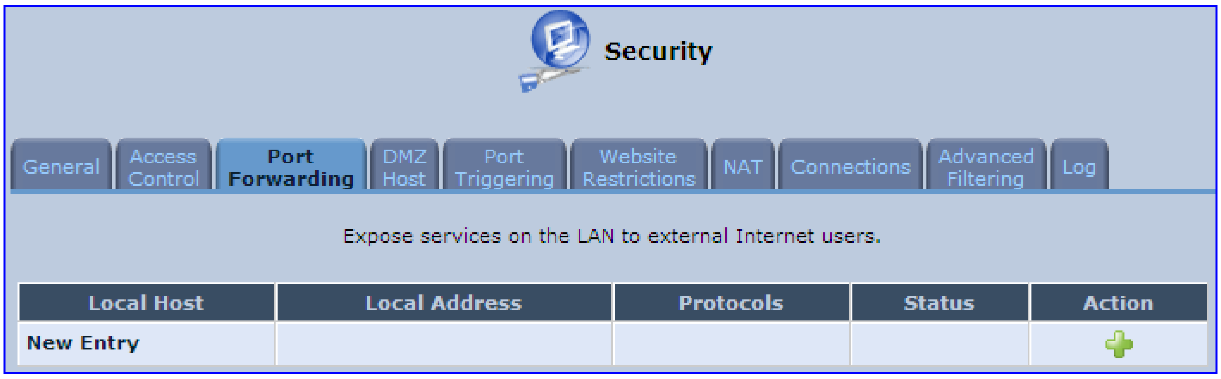
When setting a port forwarding service, you must ensure that the port is not already in use by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP - the port used by MP-20x's VoIP application (5060) is the same port on which port forwarding is 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. From the sidebar menu, click the **Security** menu, and in the screen 'Security', click the **Port Forwarding** tab; the screen 'Port Forwarding' opens.

Figure 13-5: Port Forwarding Screen

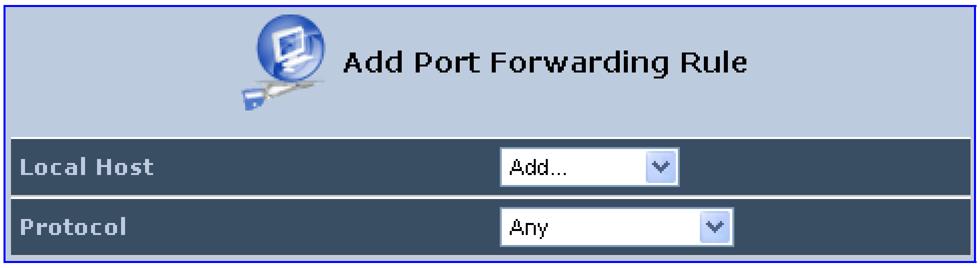


Expose services on the LAN to external Internet users.

Local Host	Local Address	Protocols	Status	Action
New Entry				✚

2. Click the link **New Entry**; the screen 'Add Port Forwarding Rule' opens.

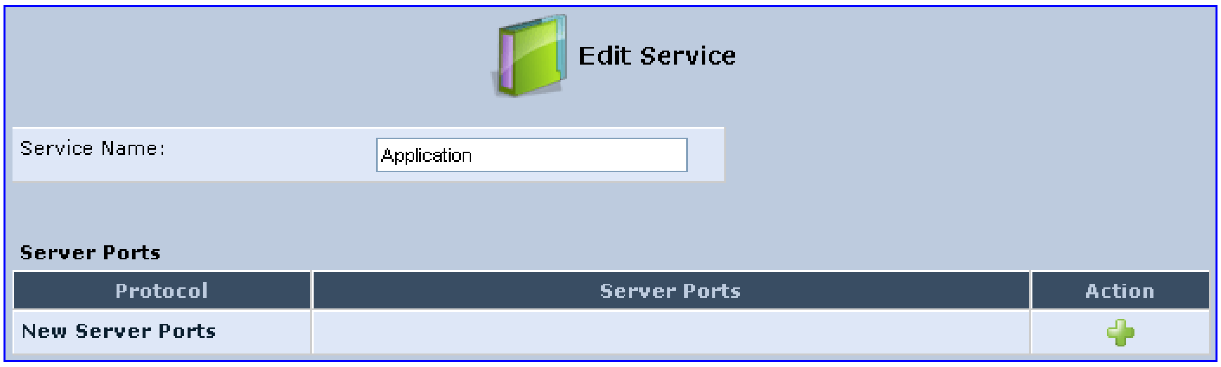
Figure 13-6: Add Port Forwarding Rule



Local Host	Add...
Protocol	Any

3. Enter the IP address or the host name of the computer that provides the service (the 'server'). Note that only one LAN computer can be assigned to provide a specific service or application.
4. The Protocol drop-down list lets you select or specify the type of protocol used.
5. In addition to the list of popular protocols it provides, you may also choose any or a specific protocol. If you choose the option 'User Defined', the screen refreshes and the following appears:

Figure 13-7: Add a Specific Protocol



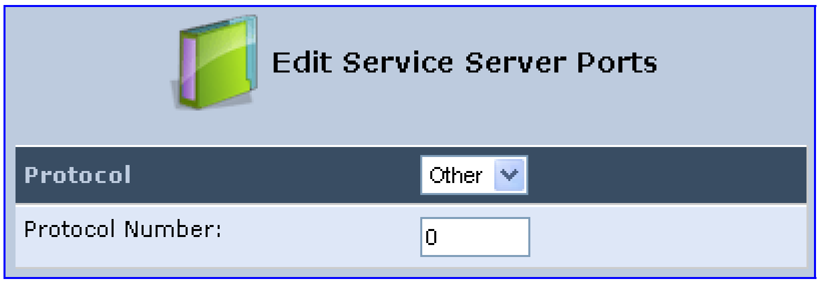
Service Name: Application

Server Ports

Protocol	Server Ports	Action
New Server Ports		✚

a. Enter a 'Service Name' and then click 'New Server Ports'. Select a protocol and then enter the protocol number.

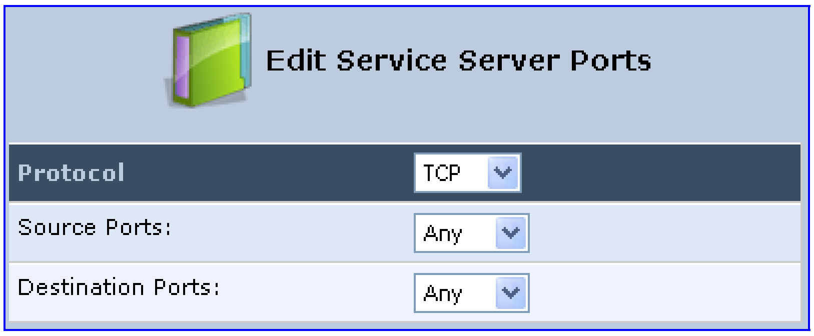
Figure 13-8: Add a Specific Protocol


Edit Service Server Ports

Protocol	Other
Protocol Number:	0

6. If you specify a listed protocol, you can select the port to forward the packets. By default, MP-20x 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 13-9: Add Specific Ports

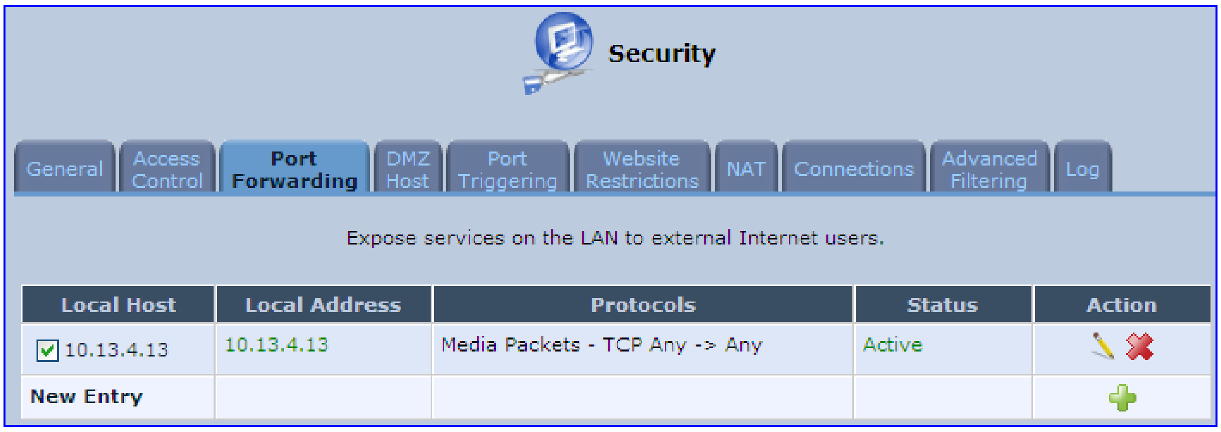

Edit Service Server Ports

Protocol	TCP
Source Ports:	Any
Destination Ports:	Any

7. To define the time period during which this rule takes effect, select The in the drop-down list 'Schedule' between 'Always' or a specific schedule. If you choose the option 'User Defined', the screen refreshes and the 'Edit Scheduler Rule' screen appears.

8. Click **OK** to save your changes; the screen 'Port Forwarding' displays a summary of the rule that you just added.

Figure 13-10: Port Forwarding Rule



Expose services on the LAN to external Internet users.

Local Host	Local Address	Protocols	Status	Action
✓ 10.13.4.13	10.13.4.13	Media Packets - TCP Any -> Any	Active	
New Entry				

9. Edit the port forwarding rule by modifying its entry under column 'Local Host' in the screen 'Port Forwarding'. To modify an entry, click the **Edit** icon for the rule; the screen 'Edit Port Forwarding Rule' opens. This screen allows you to edit all the parameters that you configured when creating the port forwarding rule.
10. Click **OK** to save your changes and return to the screen 'Port Forwarding'.
11. 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.

13.4 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.

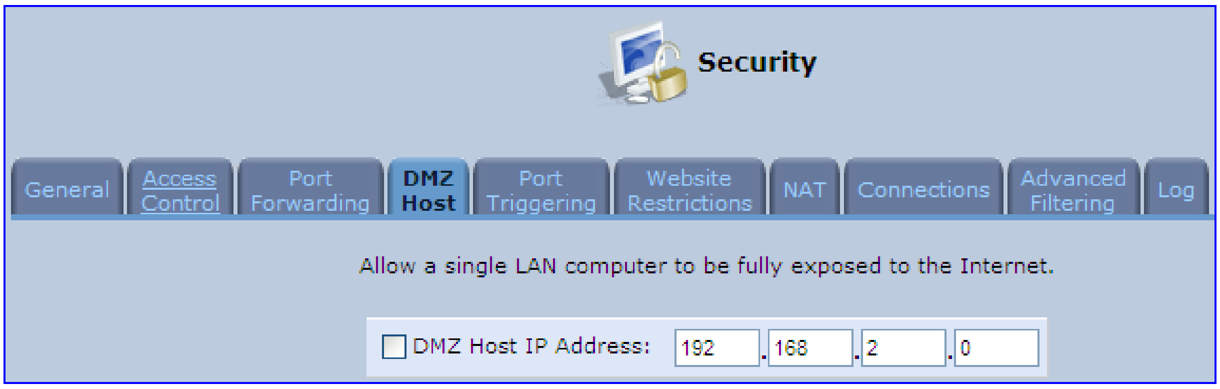
Warning: A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

An incoming request for access to a service in the home network, such as a Web-server, is fielded by MP-20x. MP-20x forwards 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 receives the request instead.

➢ **To designate a local computer as a DMZ Host:**

1. From the sidebar menu, click the **Security** menu, and in the screen 'Security', click the **DMZ Host** tab; the screen 'DMZ Host' opens.

Figure 13-11: DMZ Host



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

☐ DMZ Host IP Address: 192 . 168 . 2 . 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 does not 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 may want to enable it again in the future.

- To disable the DMZ host so that it is not 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.

13.5 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 222. The gaming server responds by connecting the user using UDP on port 333 when starting gaming sessions. In such a case you must use port triggering, since this scenario conflicts with the following default firewall settings:

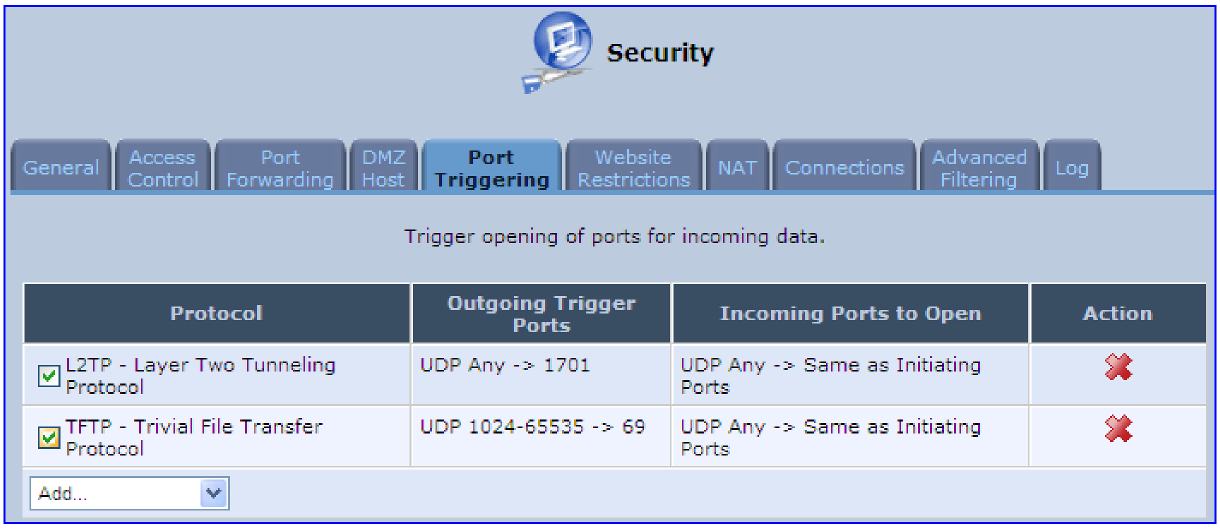
- The firewall blocks inbound traffic, by default.
- The server replies to MP-20x's IP, and the connection is not sent back to your host, since it is not part of a session.

To solve this, you need to define a Port Triggering entry, which allows inbound traffic on UDP port 333, only after a LAN host generated traffic to UDP port 222. 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 222.

➢ To view port triggering settings:

1. From the sidebar menu, click the **Security** menu, and in the screen 'Security', click the **Port Triggering** tab; the screen 'Port Triggering' opens. The screen lists all port triggering entries.

Figure 13-12: Port Triggering



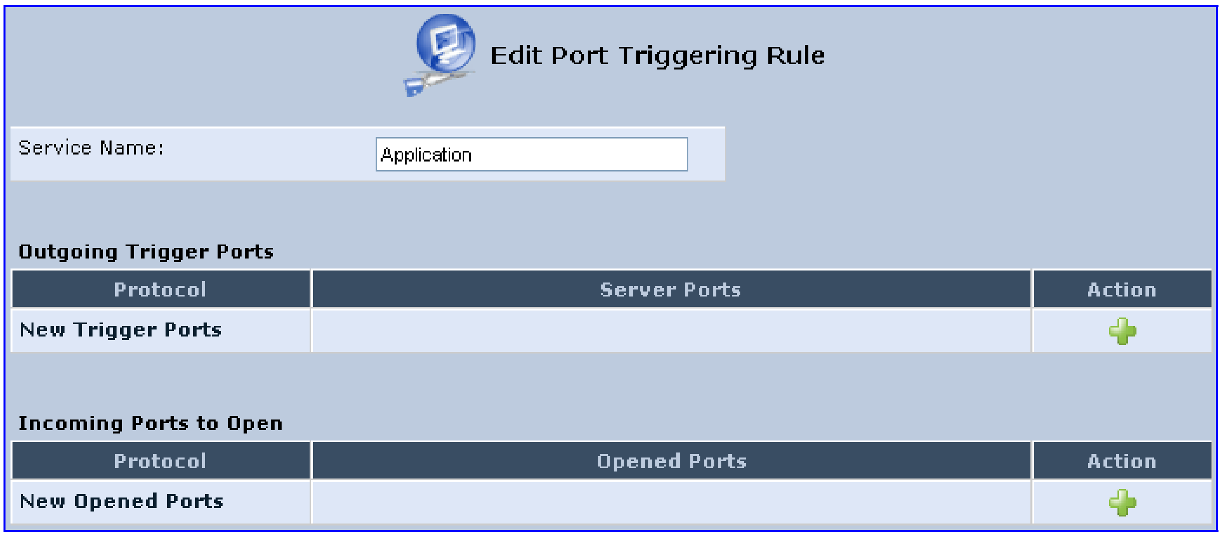
Trigger opening of ports for incoming data.

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

➢ To add an entry for the gaming example above:

1. From the drop-down list, select 'User Defined' to add an entry; the screen 'Edit Service' opens.

Figure 13-13: Adding Port Triggering Rules



Service Name: Application

Outgoing Trigger Ports

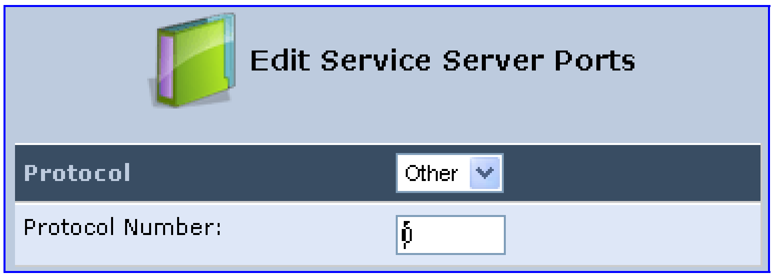
Protocol	Server Ports	Action
New Trigger Ports		✚

Incoming Ports to Open

Protocol	Opened Ports	Action
New Opened Ports		✚

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

Figure 13-14: Edit Service Server Ports

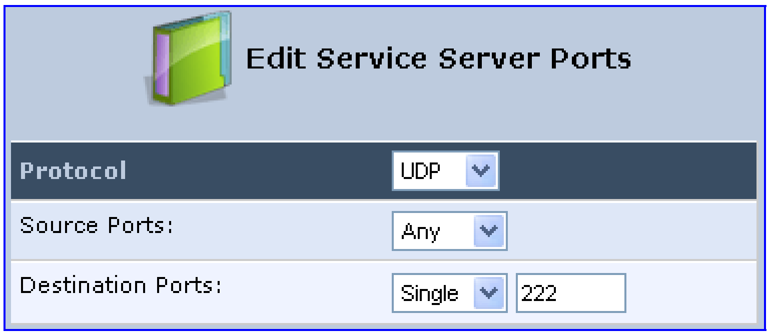

Edit Service Server Ports

Protocol	Other
Protocol Number:	0

3. In the 'Protocol' drop-down list, select 'UDP'; the screen refreshes, providing source and destination port options.

4. Leave the 'Source Ports' drop-down list at its default 'Any'. In the 'Destination Ports' drop-down list, select 'Single'; the screen refreshes again, providing an additional field in which you should enter '222' as the destination port.

Figure 13-15: Edit Service Server Ports


Edit Service Server Ports

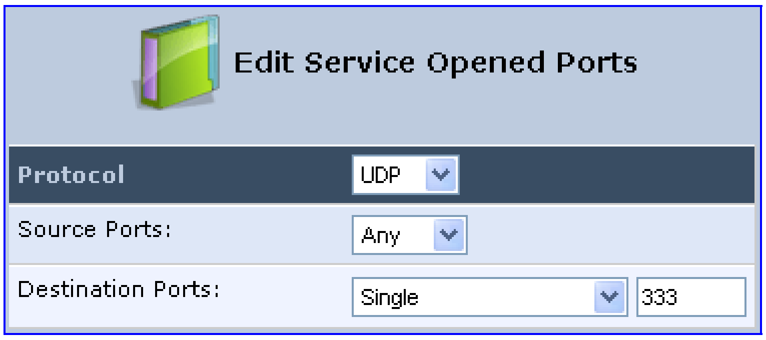
Protocol	UDP	
Source Ports:	Any	
Destination Ports:	Single	222

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.

7. Similar to the trigger ports screen, select UDP as the protocol, leave the source port at 'Any', and enter a 333 as the single destination port.

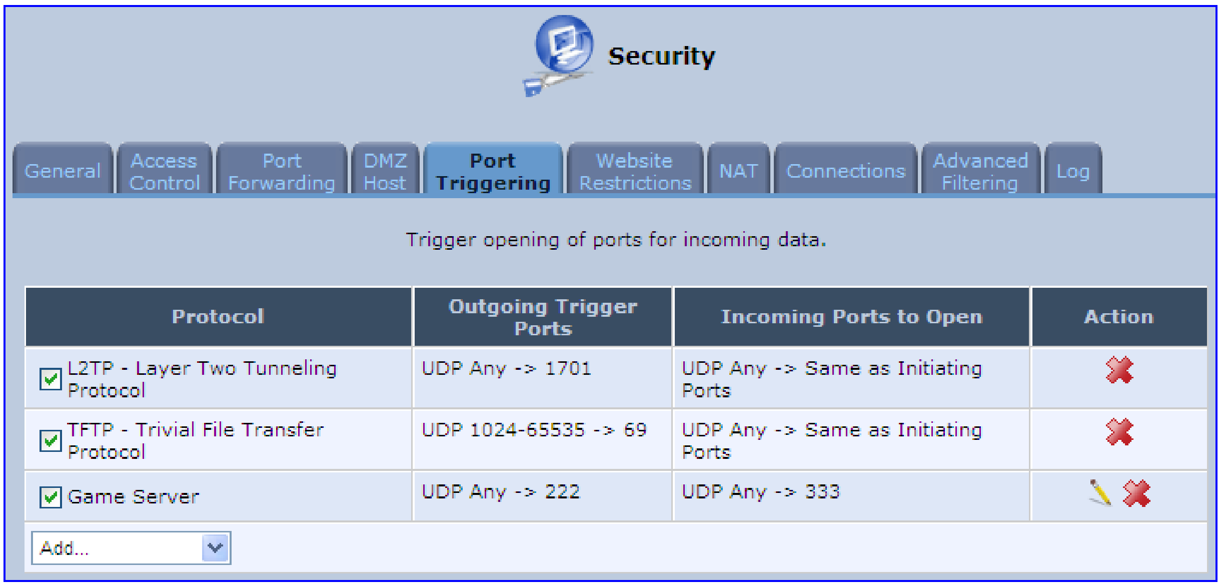
Figure 13-16: Edit Service Opened Ports


Edit Service Opened Ports

Protocol	UDP	
Source Ports:	Any	
Destination Ports:	Single	333

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.

Figure 13-17: New Port Triggering Rule



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 Ports	✖
✓ TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	UDP Any -> Same as Initiating Ports	✖
✓ Game Server	UDP Any -> 222	UDP Any -> 333	✎ ✖

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 corresponding to the service name.
- To reinstate it later, simply reselect the check box.
- To remove a rule, click the **Remove** icon 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 MP-20x functionality.

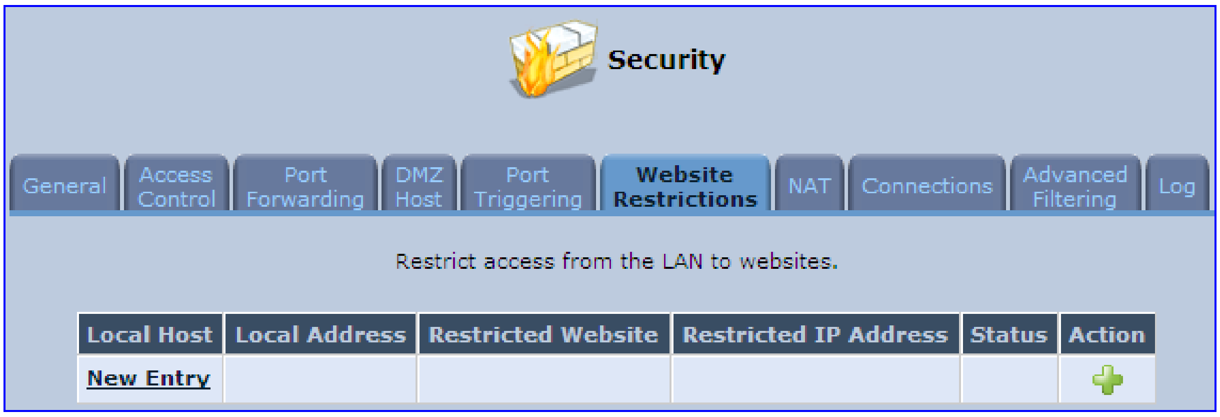
13.6 Website Restrictions

You can configure MP-20x 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. From the sidebar menu, click the **Security** menu, and in the screen 'Security', click the **Website Restrictions** tab; the screen 'Website Restrictions' opens.

Figure 13-18: Website Restrictions

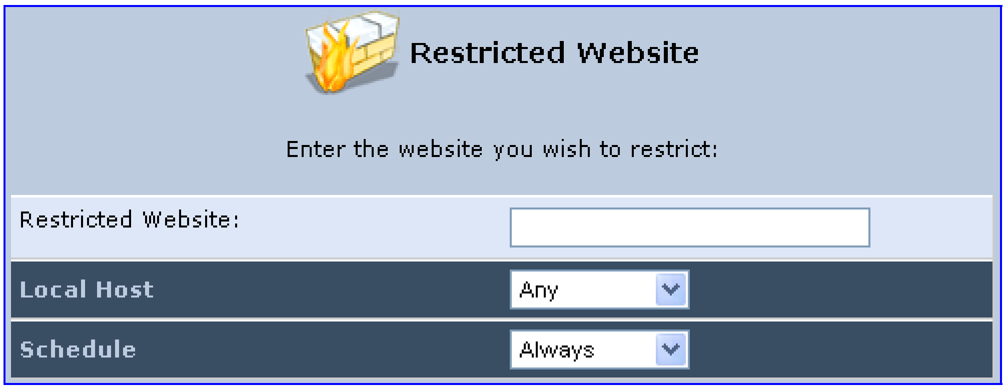


Restrict access from the LAN to websites.

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

2. Click the link **New Entry**; the 'Restricted Website' screen opens.

Figure 13-19: Restricted Website



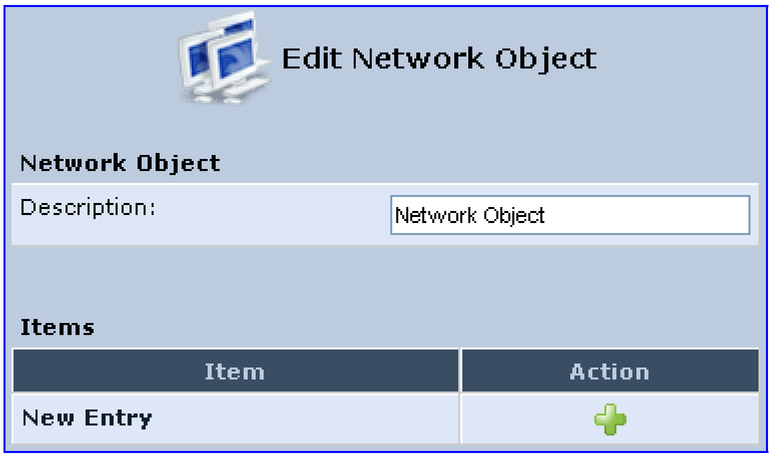
Enter the website you wish to restrict:

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 are also blocked). If the website address has multiple IP addresses, MP-20x resolves all additional addresses and automatically adds them to the restrictions table.

4. The 'Local Host' drop-down list 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 'User Defined', the screen refreshes and the 'Edit Network Object' appears:

Figure 13-20: Add a Specific Host



Edit Network Object

Network Object

Description:	Network Object

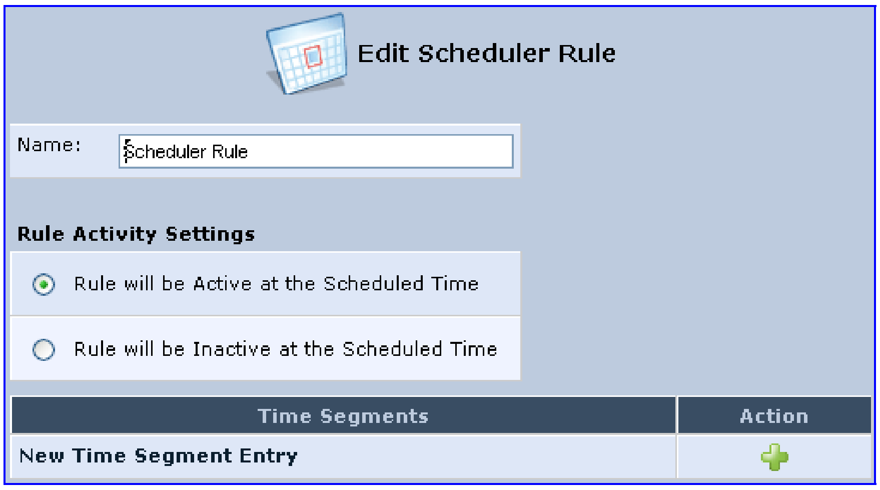
Items

Item	Action
New Entry	✚

5. Click the link **New Entry** to specify a computer address. Specify an address creating a 'Network Object'.

6. The parameter Schedule allows you to define the time period during which this rule takes effect. You can select between 'Always' or a specific schedule. If you choose the option 'User Defined', the screen 'Edit Scheduler Rule' appears:

Figure 13-21: Add a Specific Schedule



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	✚

7. Click the link 'New Time Segment Entry' to specify the time segment, and then click **OK**.

8. Click **OK** to save the settings; MP-20x attempts to find the site. 'Resolving...' appears in the Status column while the site is being located (the URL is 'resolved' into one or more IP addresses).

9. Click the **Refresh** button to update the status if necessary. If the site is successfully located, 'Resolved' appears in the status bar; if not, 'Hostname Resolution Failed' appears.

➢ If MP-20x 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 MP-20x.
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 icon **Edit** for the restriction; the screen 'Restricted Website' opens. 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 the button **Resolve Now**; MP-20x 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 icon **Remove** for the service; the service is permanently removed.

13.7 NAT

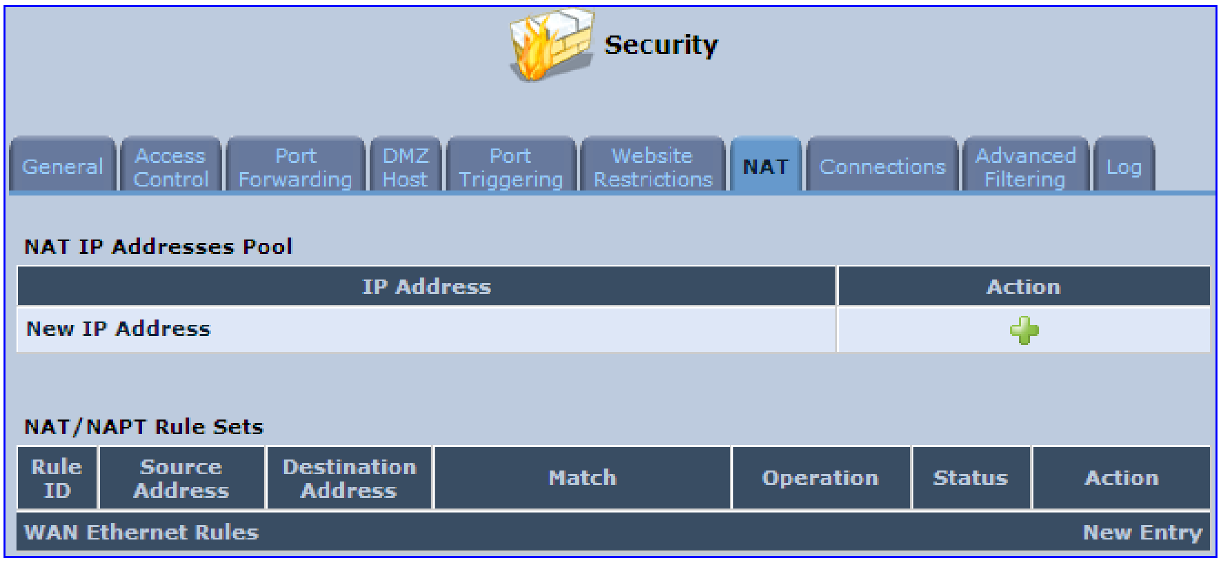
MP-20x features a configurable Network Address Translation (NAT) and Network Address Port Translation (NAPT) mechanism, allowing you to control the network addresses and ports of packets routed through your gateway. When enabling multiple computers on your network to access the Internet using a fixed number of public IP addresses, you can statically define which LAN IP address will be translated to which NAT IP address and/or ports.

By default, MP-20x operates in NAPT routing mode. However, you can control your network translation by defining static NAT/NAPT rules. Such rules map LAN computers to NAT IP addresses. The NAT/NAPT mechanism is useful for managing Internet usage in your LAN, or complying with various application demands. For example, you can assign your primary LAN computer with a single NAT IP address, in order to assure its permanent connection to the Internet. Another example is when an application server with which you wish to connect, such as a security server, requires that packets have a specific IP address – you can define a NAT rule for that address.

➢ To define NAT:

1. From the sidebar menu, click the **Security** menu, and in the screen 'Security', click the **NAT** tab; the screen 'NAT' opens.

Figure 13-22: NAT Screen



Security

General | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | NAT | Connections | Advanced Filtering | Log

NAT IP Addresses Pool

IP Address	Action
New IP Address	✚

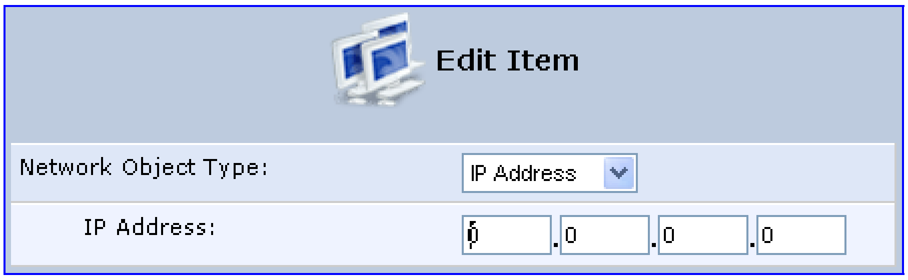
NAT/NAPT Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						New Entry

2. Before configuring NAT/NAPT rules, you must first enter the additional public IP addresses obtained from your ISP as your NAT IP addresses, in the 'NAT IP Addresses Pool' section. The primary IP address used by the WAN device for dynamic NAPT should not be added to this table.

a. To add a NAT IP address, click the **New IP Address** link; the 'Edit Item' screen appears.

Figure 13-23: Adding a NAT IP Address



Edit Item

Network Object Type: IP Address

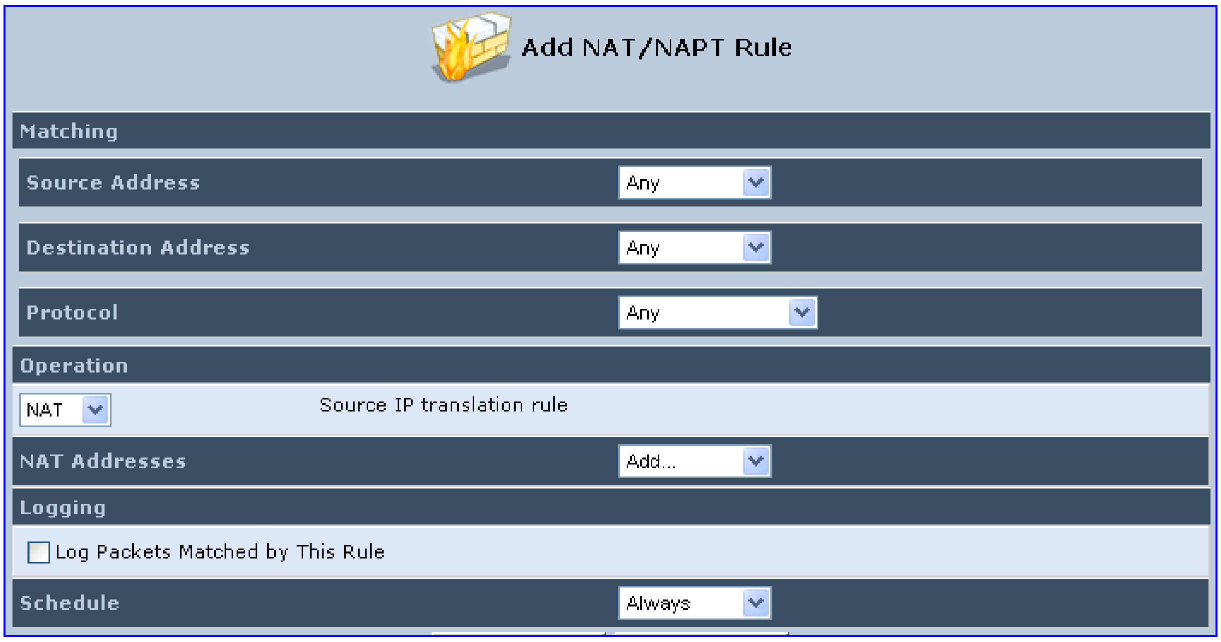
IP Address: 0 . 0 . 0 . 0

b. From the 'Network Object Type' drop-down list, select between IP address, subnet or range, and then enter the information respectively, and click **OK** to save the settings.

3. To add a new NAT/NAPT rule:

   a. In the 'NAT/NAPT Rule Sets' section, click the **New Entry** link; the 'Add NAT/NAPT Rule' screen appears.

Figure 13-24: Adding NAT/NAPT Rule



Add NAT/NAPT Rule

Matching

Source Address: Any

Destination Address: Any

Protocol: Any

Operation

NAT — Source IP translation rule

NAT Addresses: Add...

Logging

☐ Log Packets Matched by This Rule

Schedule: Always

This screen is divided into two main sections: 'Matching' and 'Operation'. The 'Matching' section defines the LAN addresses to be translated to the external addresses, which are defined in the 'Operation' section.

4. 'Matching' section (define characteristics of the packets matching the rule):

   a. **Source Address:** source address of packets sent or received by MP-20x. You can select the computer or group of computers on which you would like to apply the rule. To apply the rule on all the LAN hosts, select 'Any' . If you would like to add a new address, select the 'User Defined'. This commences a sequence to add a new Network Object, representing the new host.

   b. **Destination Address:** destination address of packets sent or received by MP-20x. This address can be configured in the same manner as the source address. This entry enables further filtration of the packets.

   c. **Protocol:** specifies a traffic protocol. Selecting the 'Show All Services' option expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This commences a sequence that adds a new Service, representing the protocol. Using a protocol requires observing the relationship between a client and a server to distinguish between the source and destination ports.

5. Operation section (define the operation to apply on the IP addresses, matching the criteria defined above): NAT or NAPT.
   - **NAT Addresses:** NAT address into which the original IP address is translated. The drop-down list displays all of your available NAT addresses/ranges from which you can select an entry. If you would like to add a single address or a sub-range from the given pool/range, select the 'User Defined' option. This commences a sequence that adds a new Network Object, representing the new host.
   - **NAPT Address:** NAPT address into which the original IP address is translated. The drop-down list displays all of your available NAPT addresses/ranges from which you can select an entry. If you would like to add a single address or a sub-range from the given pool/range, select the 'User Defined' option. This commences a sequence that adds a new Network Object, representing the new host. . Note, that in this case the network object may only be an IP address, as NAPT is port-specific.
     - ♦ **NAPT Ports:** specify the port(s) of the IP address into which the original IP address is translated. Enter a single port or select 'Range' (the screen refreshes, enabling you to enter a range of ports).
6. Select the 'Log Packets Matched by This Rule' check box to log the first packet from a connection that was matched by this rule.
7. By default, the 'Schedule' rule is always active. However, you can configure scheduler rules to define time segments during which the rule may be active.
8. Click **OK** to save the settings.

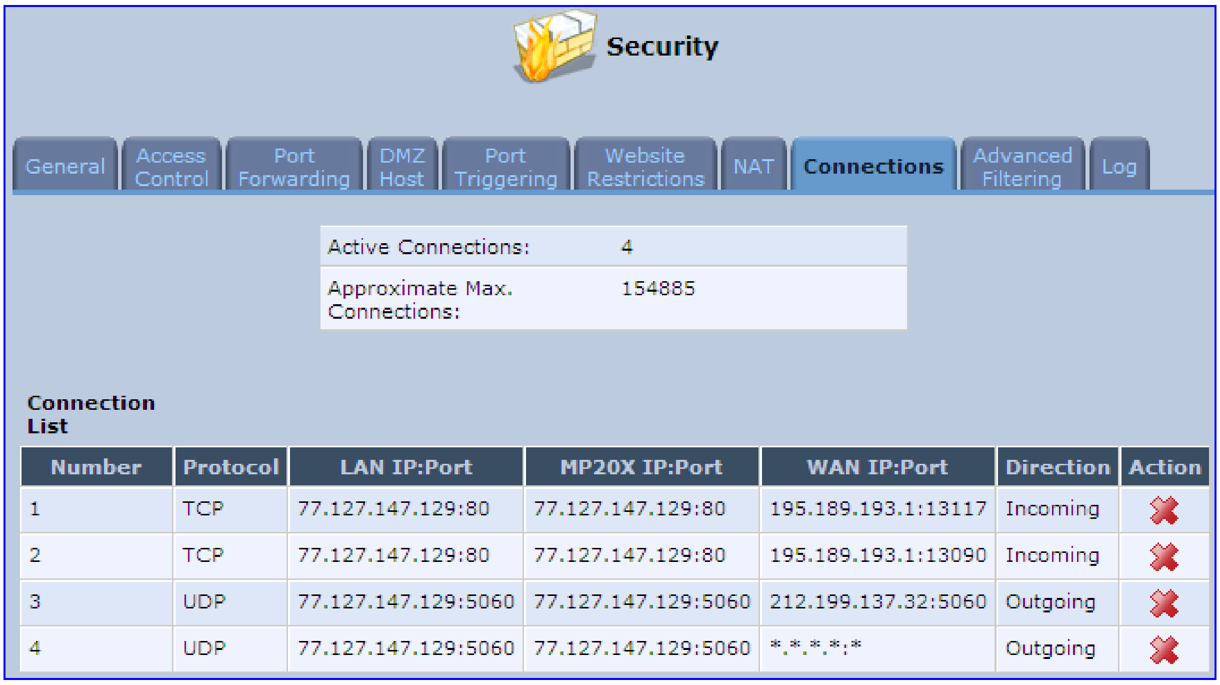
13.8 Connections

The connection list displays all the connections that are currently open, as well as various details and statistics. You can use this list to close an undesired connection by clicking its corresponding action icon. The basic display includes the name of the protocol, the different ports it uses, and the direction in which the connection was initiated.

➢ To view currently open connections:

- From the sidebar menu, click the **Security** menu, and in the screen 'Security', click the **Connections** tab; the screen 'Connections' opens.

Figure 13-25: Connections Screen



Active Connections:	4
Approximate Max. Connections:	154885

Connection List

Number	Protocol	LAN IP:Port	MP20X IP:Port	WAN IP:Port	Direction	Action
1	TCP	77.127.147.129:80	77.127.147.129:80	195.189.193.1:13117	Incoming	✗
2	TCP	77.127.147.129:80	77.127.147.129:80	195.189.193.1:13090	Incoming	✗
3	UDP	77.127.147.129:5060	77.127.147.129:5060	212.199.137.32:5060	Outgoing	✗
4	UDP	77.127.147.129:5060	77.127.147.129:5060	*.*.*.*:*	Outgoing	✗

Click the **Advanced** button to display the following details:

- Connection's time-to-live
- Number of kilobytes and packets received and transmitted
- Device type
- Routing mode

The 'Approximate Max. Connections' value represents the amount of additional concurrent connections possible.

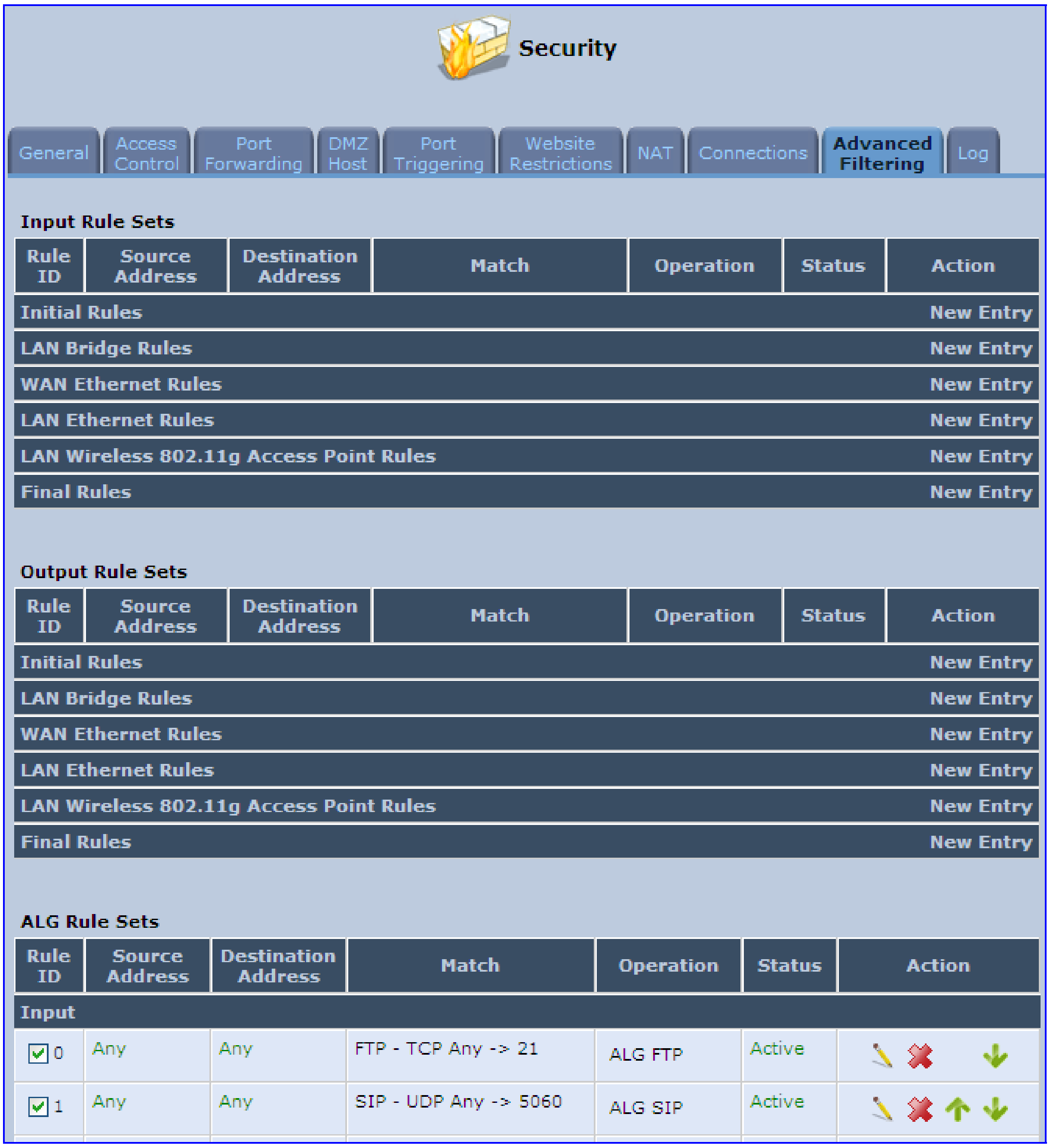
13.9 Advanced Filtering

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 MP-20x's advanced filtering options:**

- From the sidebar menu, click the **Security** menu, and in the screen 'Security', click the **Advanced Filtering** tab; the 'Advanced Filtering' opens.

Figure 13-26: Advanced Filtering



Input Rule Sets

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

Output Rule Sets

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

ALG Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Input						
✓ 0	Any	Any	FTP - TCP Any -> 21	ALG FTP	Active	
✓ 1	Any	Any	SIP - UDP Any -> 5060	ALG SIP	Active	

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 are applied first, on all MP-20x devices.
2. Network devices rules - rules can be defined per MP-20x.
3. Final rules - rules defined here are applied last, on all MP-20x devices.

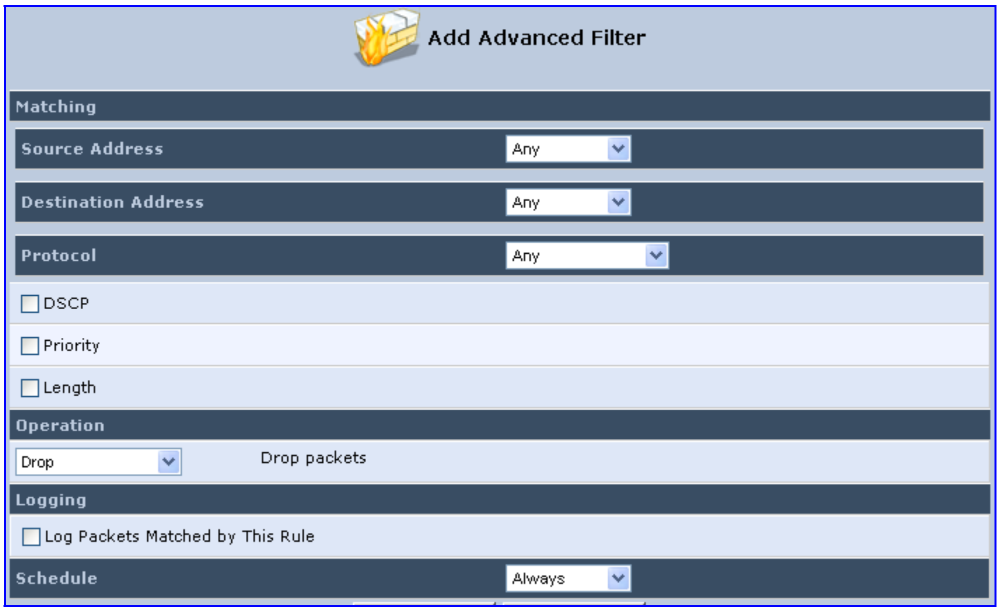
Numerous rules are automatically inserted by the firewall to provide improved security and block harmful attacks.

Note: The order of appearance of the firewall rules determines the sequence by which they are applied.

➢ To configure an advanced filtering rule:

1. After choosing the traffic direction and the device on which to set the rule, click the corresponding link **New Entry**; the screen 'Add Advanced Filter' opens.

Figure 13-27: Add Advanced Filter



Add Advanced Filter

Matching

Source Address: Any

Destination Address: Any

Protocol: Any

☐ DSCP

☐ Priority

☐ Length

Operation

Drop — Drop packets

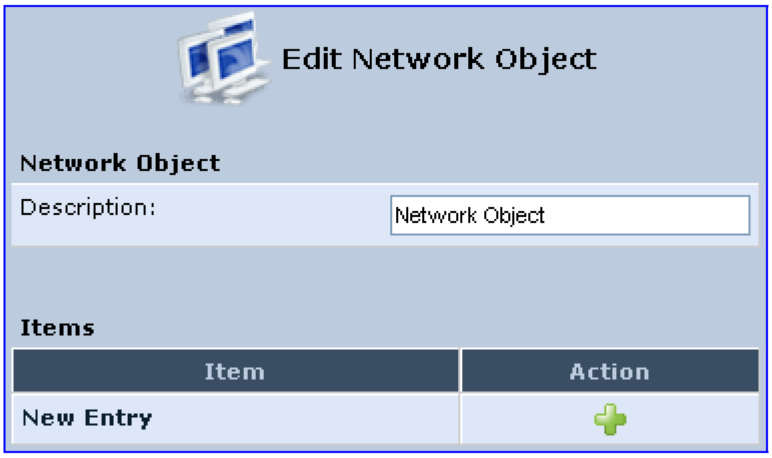
Logging

☐ Log Packets Matched by This Rule

Schedule: Always

2. In the section 'Matching', define a match between IP addresses and a traffic protocol:
   a. Configure the source address of the packets sent to or received from the network object. To add an address, select the option 'User Defined' from the drop-down list; the screen 'Edit Network Object' appears.

Figure 13-28: Add a Specific Host


Edit Network Object

Network Object

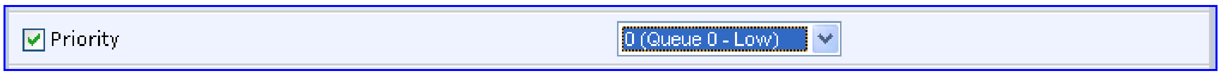
Description: Network Object

Items

Item	Action
New Entry	✚

   Click the link **New Entry**; this commences a sequence that adds a new network object.
   b. 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.
   c. From the 'Protocol' drop-down list, select a specific traffic protocol or add a new one (by selecting 'User Defined'); the 'Edit Services' screen appears. Click the link **New Server Ports**; this commences a sequence that adds a new protocol.
3. Select the check box 'DSCP' to mark a DSCP value on packets matching this rule; the screen refreshes, allowing you to enter the hexadecimal value of the DSCP.
4. Select the check box 'Priority' to add a priority to the rule; the screen refreshes, 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 13-29: Set Priority Rule


✓ Priority 0 (Queue 0 - Low)

5. Select the check box 'Length' to specify the length of packets or the length of their data portion.
6. In the section 'Operation', define the action of the rule:
   - **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 Connection:** Allow access to packets that match the source and destination IP addresses and service ports defined in 'Matching'. The data transfer session is 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 is not handled using Stateful Packet Inspection (SPI), meaning that other packets that match this rule are not automatically allowed access. For example, this can useful when creating rules that allow broadcasting.

7. Under the section 'Logging', select the parameter 'Log Packets Matched By This Rule' to log the first packet from a connection that was matched by this rule.
8. By default, the 'Schedule' rule is always active. However, you can configure scheduler rules to define time segments during which the rule may be active.
9. Click **OK** to save the settings.

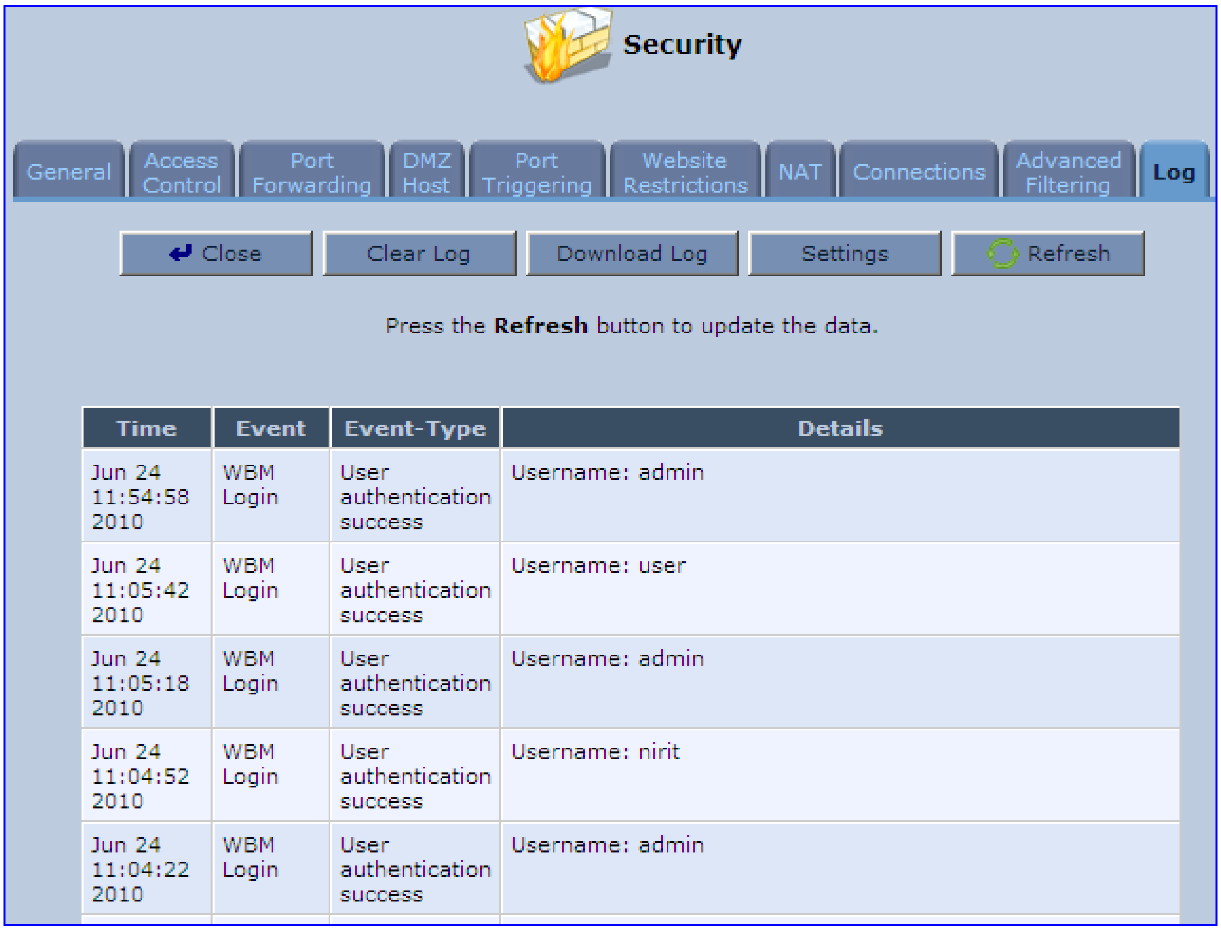
13.10 Security Log

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. From the sidebar menu, click the **Security** menu, and in the screen 'Security', click the **Log** tab; the screen 'Log' opens.

Figure 13-30: Security Log



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

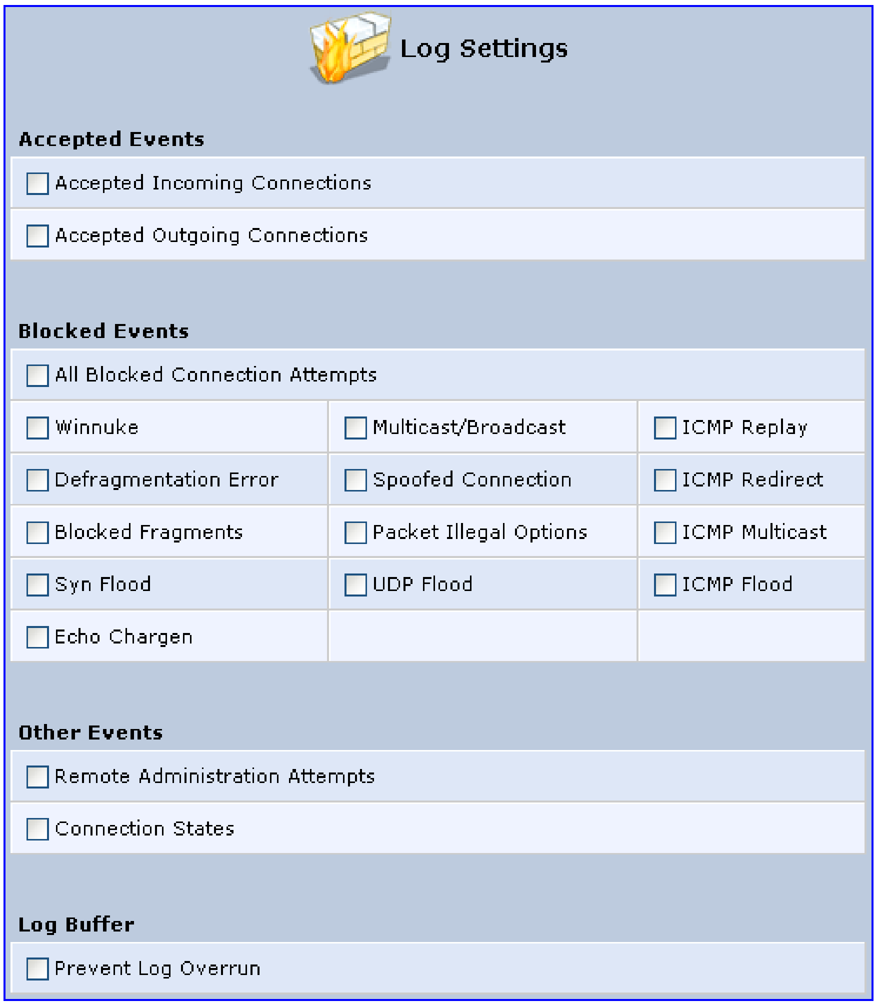
Time	Event	Event-Type	Details
Jun 24 11:54:58 2010	WBM Login	User authentication success	Username: admin
Jun 24 11:05:42 2010	WBM Login	User authentication success	Username: user
Jun 24 11:05:18 2010	WBM Login	User authentication success	Username: admin
Jun 24 11:04:52 2010	WBM Login	User authentication success	Username: nirit
Jun 24 11:04:22 2010	WBM Login	User authentication success	Username: admin

2. The log table displays the following:
   - **Time:** to determine the time the event occurred.
   - **Event:** 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).
   - **Event-Type:** 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.
   - **Details:** details of the packet or the event, such as protocol, IP addresses, ports, etc.

➢ To change the security log settings:

1. In the 'Log' screen, click **Settings**; the screen 'Log Settings' opens.

Figure 13-31: Security Log Settings



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 is 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.

The event types that can be recorded in the 'Log' screen include the following:

- Firewall internal - an accompanying explanation from the firewall internal mechanism is 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

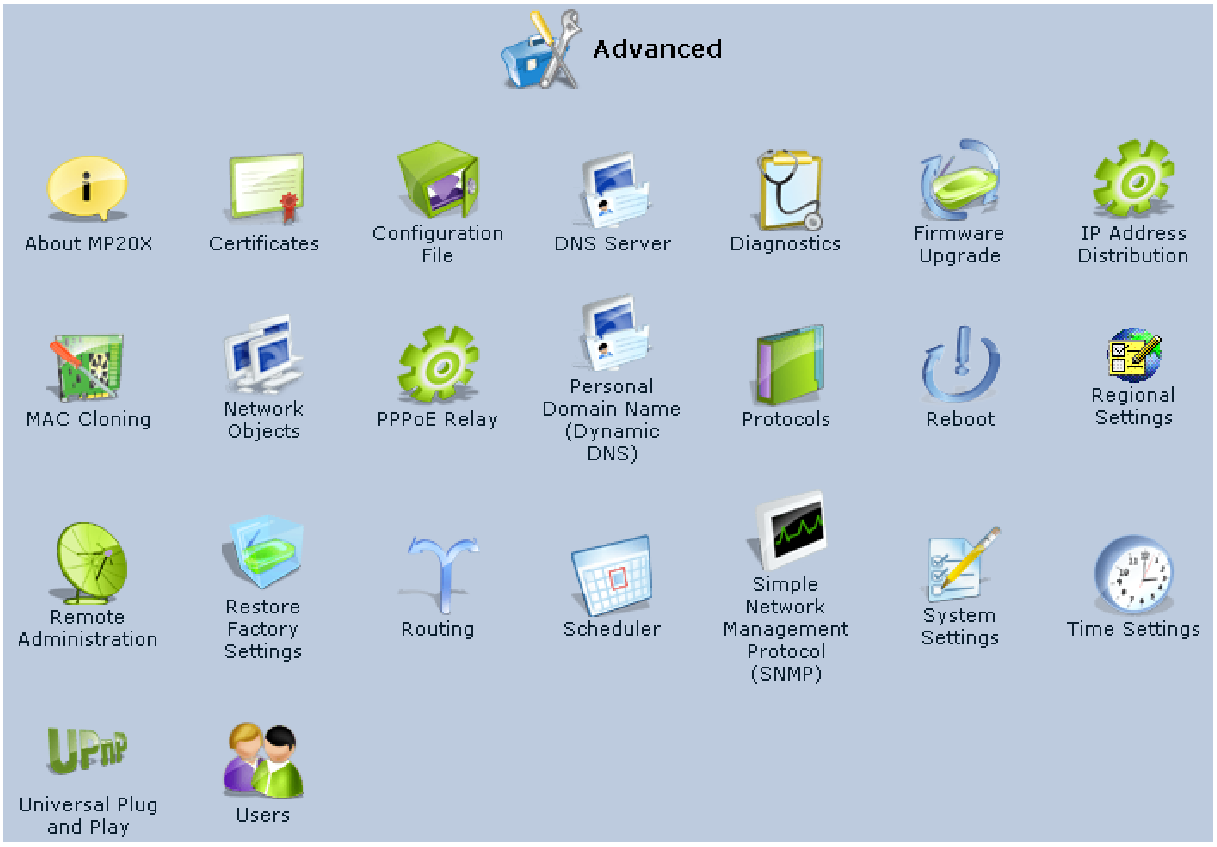
Reader’s Notes

14 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 MP-20x and the home network, and should be made with caution.

The left sidebar's **Advanced** menu opens the 'Advanced' screen.

Figure 14-1: Advanced Screen



This screen displays icons for accessing the advanced options, as described in the table below:

Table 14-1: Icon Description in the Advanced Screen

Icon	Name	Description
	About MP-20x	View technical information about MP-20x, including version number
	Certificates	Manages digital certificates.

Icon	Name	Description
	Configuration File	Load the Configuration File to MP-20x **Note:** You can hide the **Configuration File** icon, by running the following CLI command in a Telnet session with MP-20x: rg_conf_set rmt_config/hide_config_file_page 1. This is useful, for example, in scenarios where you want to prevent a user accessing the Web interface to change the configuration file.
	DNS Server	Alias a dynamic IP address to a static hostname
	Diagnostics	Perform networking diagnostics
	Firmware Upgrade	Perform a Firmware Upgrade
	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
	MAC Cloning	Clone MP-20x's MAC address.
	Network Objects	Define groups of LAN devices for system rules.
	PPPoE Relay	Enable PPPoE relay on MP-20x.
	Personal Domain Name (Dynamic DNS)	View and modify the DNS Hosts table.
	Protocols	Manage protocols.
	Reboot	Restart MP-20x.
	Regional Settings	Change the regional settings.
	Remote Administration	Configure remote administration privileges.
	Restore Factory Settings	Restore default factory settings.

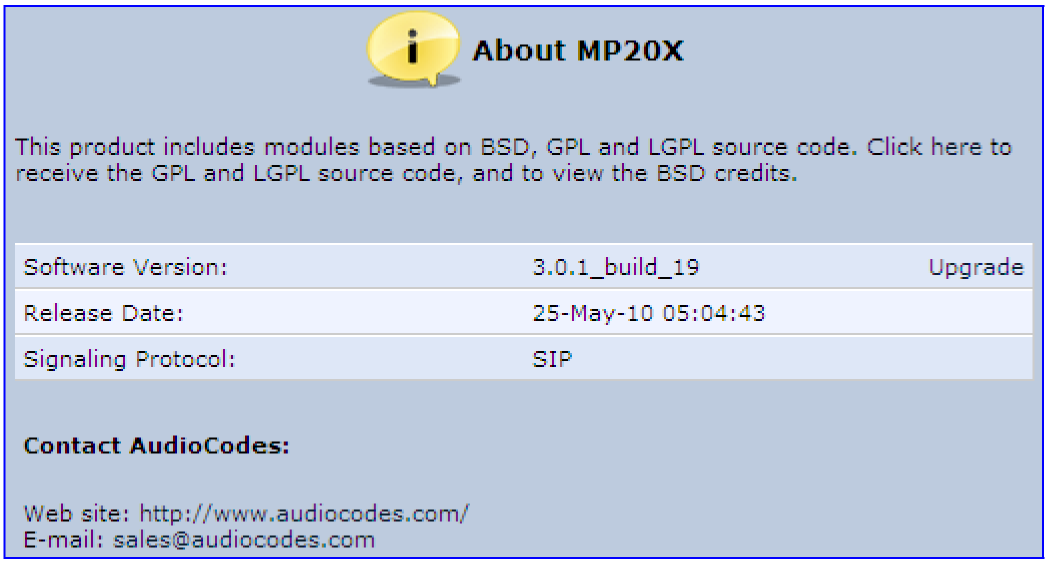
Icon	Name	Description
	Routing	Manage routing policies.
	Scheduler	Define time segments for system rules.
	Simple Network Management Protocol (SNMP)	Configure MP-20x's SNMP agent.
	System Settings	Modify administrator settings, including MP-20x's hostname.
	Time Settings	Set the local date and time.
	Universal Plug and Play	Configure Universal Plug and Play (UPnP) parameters.
	Users	Configure users.

14.1 About the MP-20x

➢ **To view technical information regarding MP-20x:**

1. In the 'Advanced' screen, click the **About the MP-20x** icon; the screen 'About the MP-20x' appears showing the version, the release date and the supported features.

Figure 14-2: Advanced - About the Gateway


About MP20X

This product includes modules based on BSD, GPL and LGPL source code. Click here to receive the GPL and LGPL source code, and to view the BSD credits.

Software Version:	3.0.1_build_19	Upgrade
Release Date:	25-May-10 05:04:43	
Signaling Protocol:	SIP	

Contact AudioCodes:

Web site: http://www.audiocodes.com/
E-mail: sales@audiocodes.com

You can upgrade the software running on MP-20x, by clicking the **Upgrade** link, which opens the 'MP-20x Firmware Upgrade' screen (refer to 'Firmware Upgrade' on page 226).

14.2 Certificates

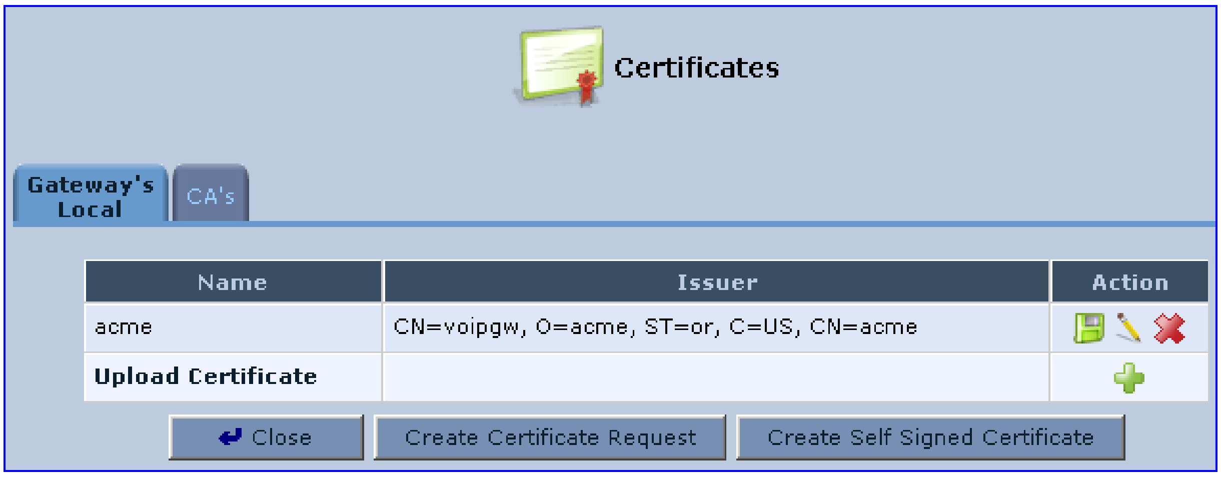
When a service provider implements remote provisioning in which a unique configuration file (per MP-20x) is placed on a server located on the WAN, the service provider can ensure that only its deployed MP-20x units are able to connect to the HTTP server via HTTPS. This is performed by using a certification validation process (client-server). There are two types of certificates:

- Self-signed certificates
- Certificate Authority (CA) signed certificates

➢ To work with self-signed certificates:

1. In the 'Advanced' screen, click the **Certificates** icon; the 'Certificates' screen is displayed.

Figure 14-3: New Certificates Screen



Certificates

Gateway's Local | CA's

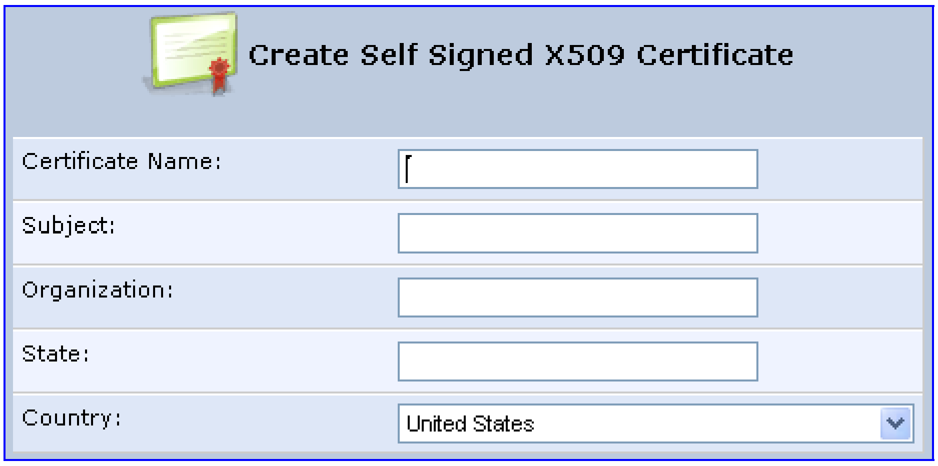
Name	Issuer	Action
acme	CN=voipgw, O=acme, ST=or, C=US, CN=acme	
Upload Certificate		

2. Create a self-signed certificate (**Note:** You can also create a self-signed certificate using the OpenSSL utility, downloaded from http://sial.org/howto/openssl/self-signed):

   a. Select the **Gateway's Local** tab.

   b. Click the **Create Self Signed Certificate** button and create the certificate; the 'Create Self Signed X509 Certificate' screen appears.

Figure 14-4: Create Self Signed X509 Certificate Screen



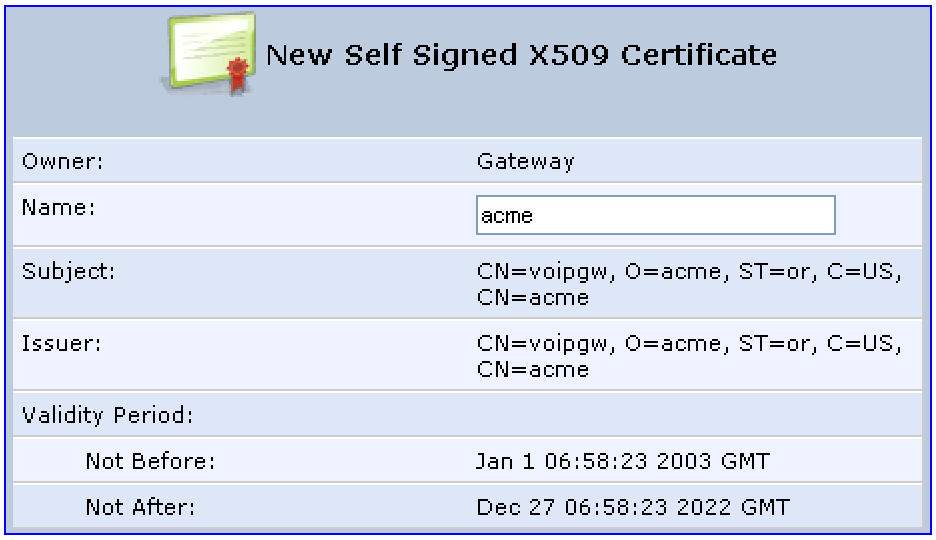
Create Self Signed X509 Certificate

Certificate Name:	
Subject:	
Organization:	
State:	
Country:	United States

   c. Enter the fields in the 'Create Self Signed X509 Certificate' screen, and then click **Generate**; a message appears notifying you that this process may take a few minutes.

d. After a few moments, click **Refresh**; the 'New Self Signed X509 Certificate' screen appears.

Figure 14-5: New Self Signed X509 Certificate Screen



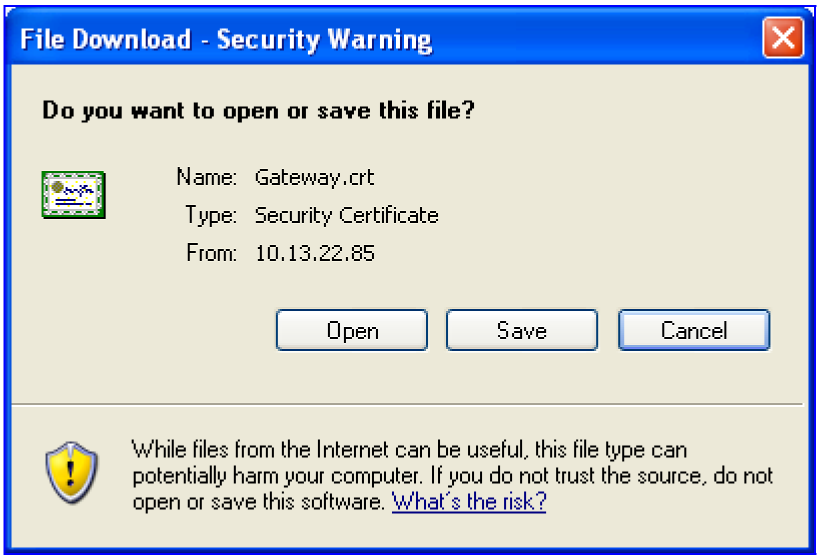
New Self Signed X509 Certificate

Owner:	Gateway
Name:	acme
Subject:	CN=voipgw, O=acme, ST=or, C=US, CN=acme
Issuer:	CN=voipgw, O=acme, ST=or, C=US, CN=acme
Validity Period:	
Not Before:	Jan 1 06:58:23 2003 GMT
Not After:	Dec 27 06:58:23 2022 GMT

e. Click **OK**; the new certificate appears listed in the 'Certificates' screen.

f. In the 'Certificates' screen, click the **Download** icon corresponding to the new self-signed certificate that you created; the 'File Download' window appears.

Figure 14-6: File Download Window



File Download - Security Warning

Do you want to open or save this file?

Name: Gateway.crt
Type: Security Certificate
From: 10.13.22.85

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

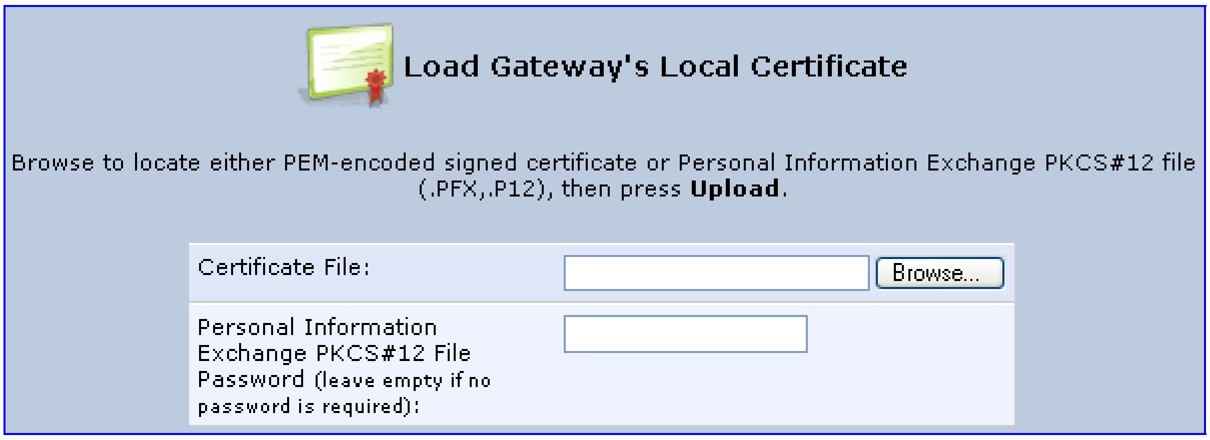
g. Click **Save**, and then browse to the folder to where you want to save the file; the file is saved as a *.crt file.

3. Configure the Apache server, by configuring the SSLCACertificateFile parameter to point to the location where the certificate file is located. Since this is a self-signed certificate, you are also considered the CA.

4. Load the self-signed certificate to MP-20x:

   a. In the 'Certificates' screen, click **Upload Certificate**; the 'Load Gateway's Local Certificate' screen appears.

Figure 14-7: Load Gateway's Local Certificate



Load Gateway's Local Certificate

Browse to locate either PEM-encoded signed certificate or Personal Information Exchange PKCS#12 file (.PFX,.P12), then press **Upload**.

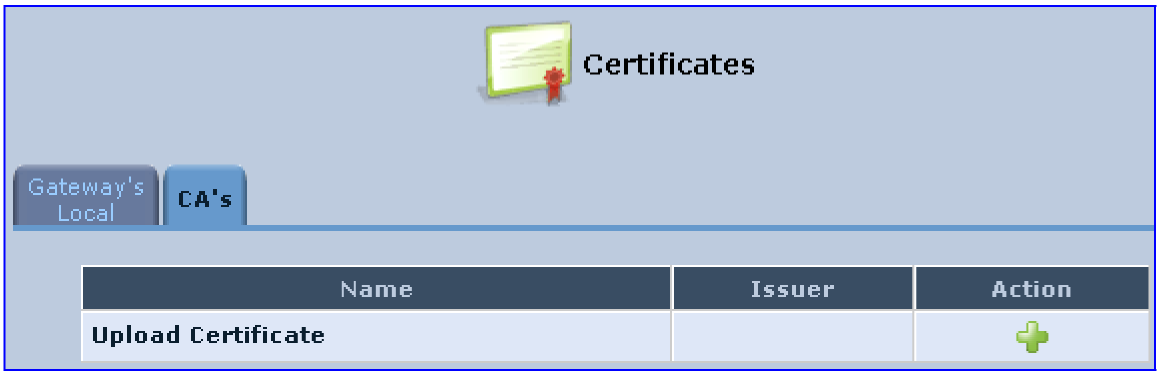
Certificate File:	[ ] Browse...
Personal Information Exchange PKCS#12 File Password (leave empty if no password is required):	[ ]

   b. Click **Browse**, locate the certification file that you created, and then click **Upload** to load the file.

5. Load the CA's certificate to MP-20x:

   a. Select the **CA's** tab; the 'CA's' screen appears.

Figure 14-8: CA's Certificates Page

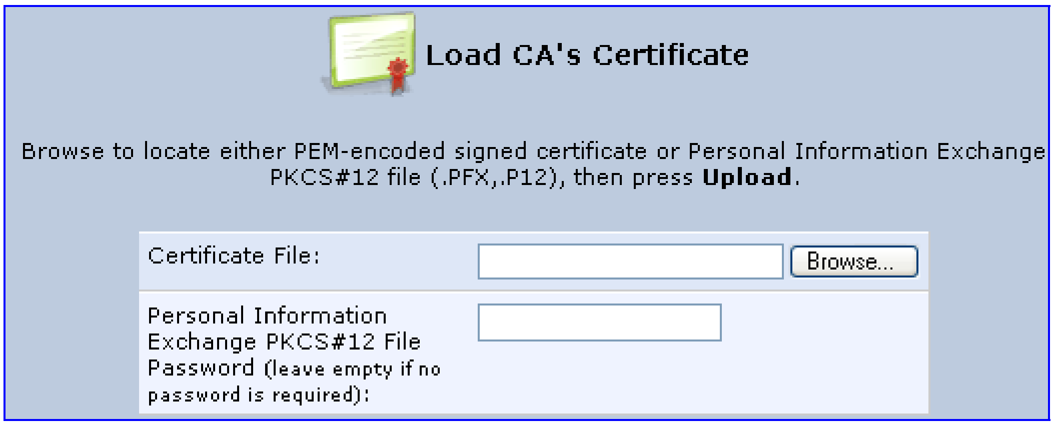


Certificates

Name	Issuer	Action
Upload Certificate		✚

b. Click **Upload Certificate**; the 'Load CA's Certificate' screen appears.

Figure 14-9: Load CA's Certificate Page



Load CA's Certificate

Browse to locate either PEM-encoded signed certificate or Personal Information Exchange PKCS#12 file (.PFX,.P12), then press **Upload**.

Certificate File:	Browse...
Personal Information Exchange PKCS#12 File Password (leave empty if no password is required):	

c. Click **Browse**, locate the CA certification file that you created, and then click **Upload** to load the file.

6. Configure the Apache server, using the following parameters:

- SSLCACertificateFile: Set the path to the CA's certificate.
- SSLCertificateFile: Set the path to your signed certificate.
- SSLCertificateKeyFile: Set the path to your private key.

14.3 Configuration File

Your MP-20x enables you to view, save, and load its configuration file to backup and restore your current configuration. MP-20x also supports configuration file encryption, allowing you to load encrypted configuration files (using the file name extensions .cfx or .inx). For a description on encrypting a configuration file (refer to 'Encrypting a Configuration File Using CLI' on page 220).

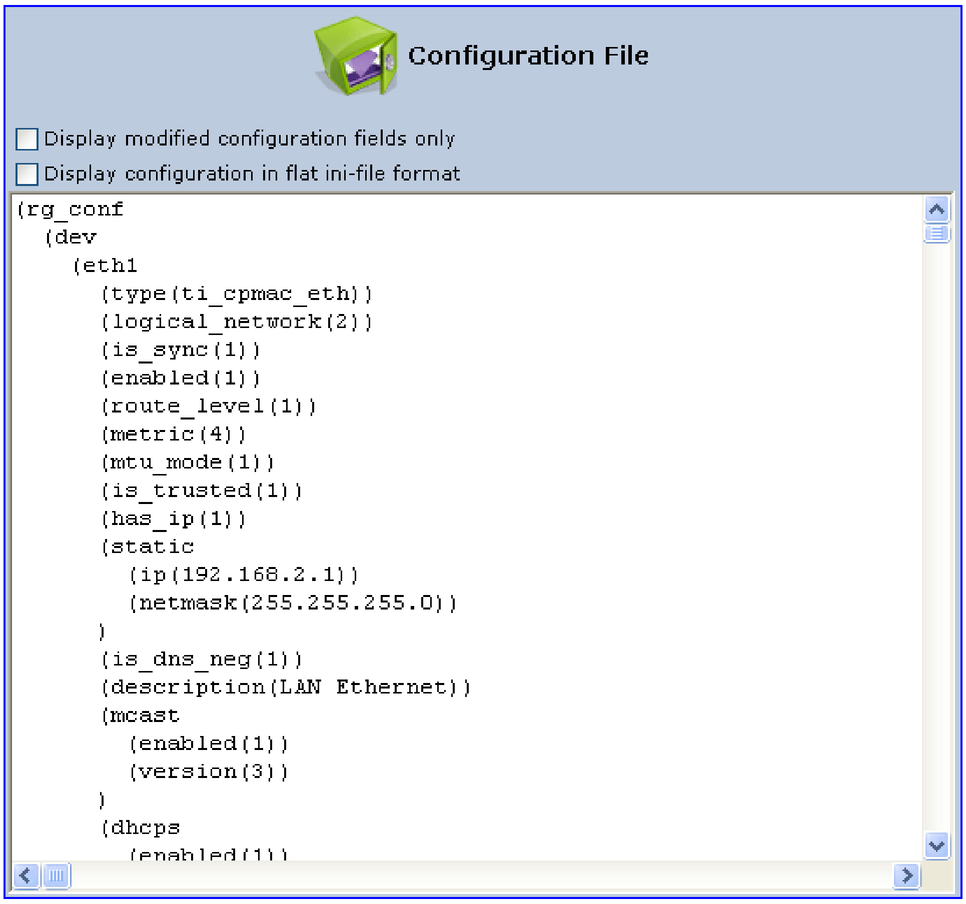
MP-20x allows you to use un-encrypted passwords in the configuration file (.cfg or .ini file) that you want to load, and then encrypt the passwords before burning to flash. This is achieved by using the format {"<value>"} in the configuration file for password fields which are normally encrypted. Below are two examples of this feature

- In an .ini file: **rg_conf/voip/line/1/auth_password={"foobaa"}**
- In a .cfg file: **(auth_password({"foobaa"}))**

➢ To save and restore the configuration file:

1. In the 'Advanced' screen, click the **Configuration File** icon; the 'Configuration File' screen appears, showing the entire contents of the configuration file.

Figure 14-10: Contents of the Configuration File


Configuration File
☐ Display modified configuration fields only
☐ Display configuration in flat ini-file format

```
(rg_conf
  (dev
    (eth1
      (type(ti_cpmac_eth))
      (logical_network(2))
      (is_sync(1))
      (enabled(1))
      (route_level(1))
      (metric(4))
      (mtu_mode(1))
      (is_trusted(1))
      (has_ip(1))
      (static
        (ip(192.168.2.1))
        (netmask(255.255.255.0))
      )
      (is_dns_neg(1))
      (description(LAN Ethernet))
      (mcast
        (enabled(1))
        (version(3))
      )
      (dhcps
        (enabled(1))
```

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. To back up your current configuration to a file on your PC, click **Download Configuration 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 MP-20x'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 MP-20x, using the procedure described in 'Loading From a Computer in the Network' on page 216.

4. To restore your configuration from a file saved on your PC, click **Upload Configuration File**.

Note: Do not load this file to a different MP-20x as it includes the MAC address, which is specific to MP-20x from where it was saved.

When creating a file for remote configuration update, it is recommended to only select 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.

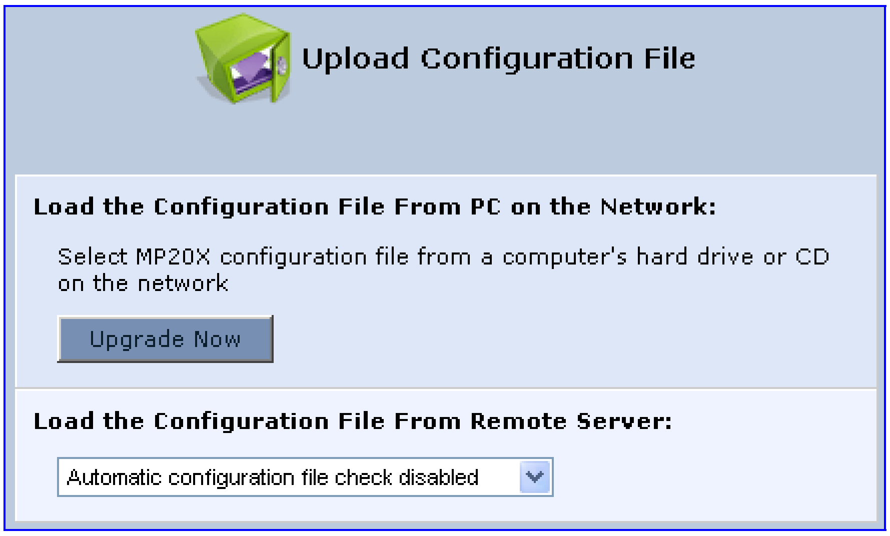
Note: When rebooting, MP-20x restores the settings from its configuration file. However, if reboot attempts fail three times consecutively, MP-20x resets the configuration file by restoring factory defaults before attempting to reboot.

14.3.1 Uploading from a PC on the Network

➢ To load MP-20x's configuration file from a computer on the network:

1. Click the **Upload Configuration File**; the screen 'Upload Configuration File' opens.

Figure 14-11: Upload Configuration File



Upload Configuration File

Load the Configuration File From PC on the Network:

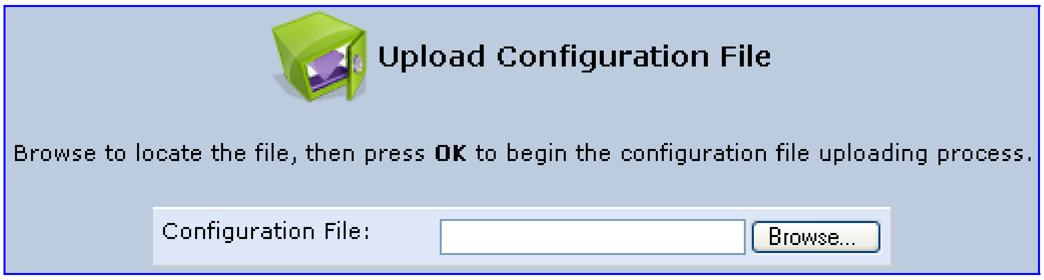
Select MP20X configuration file from a computer's hard drive or CD on the network

Load the Configuration File From Remote Server:

Automatic configuration file check disabled

2. In the section 'Load the Configuration File From a PC on the Network', click **Upgrade Now**; the screen 'Upload Configuration File' opens.

Figure 14-12: Advanced - Loading Configuration File from a PC on the Network



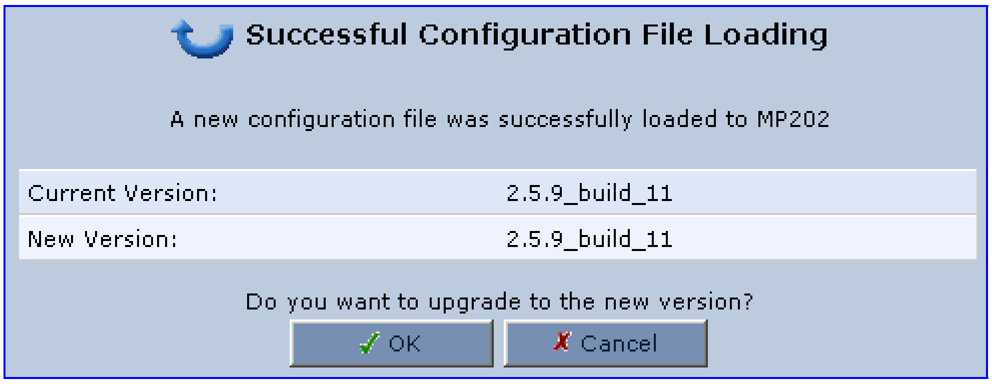
Upload Configuration File

Browse to locate the file, then press **OK** to begin the configuration file uploading process.

Configuration File: Browse...

3. 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 MP-20x. When loading is complete, the screen 'Successful Configuration File Loading' opens, prompting you to confirm configuration file load.

Figure 14-13: Successful Configuration File Loading



Successful Configuration File Loading

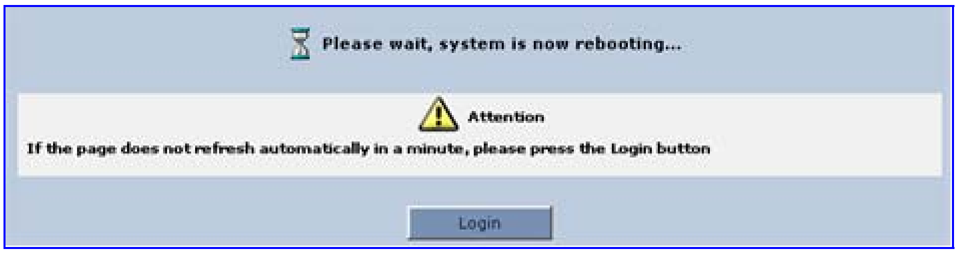
A new configuration file was successfully loaded to MP202

Current Version:	2.5.9_build_11
New Version:	2.5.9_build_11

Do you want to upgrade to the new version?

4. 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 MP-20x.

Figure 14-14: 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: During the load process, it is recommended not to power down MP-20x or stop the file load process so as not to damage the main firmware. However, if you do, MP-20x runs a recovery firmware image (also stored on its flash memory). Except for the analog or VoIP interfaces, the recovery image supports all interfaces and enables MP-20x to reconnect to the Internet and then download the primary software.

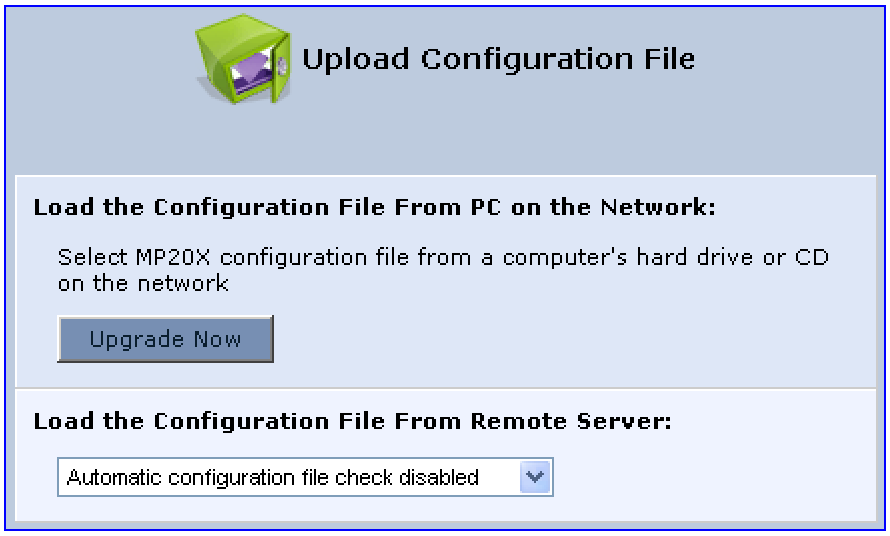
14.3.2 Uploading from a Remote Server

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 MP-20x restarts, as well as letting you perform manual checks.

➢ To load MP-20x's configuration file from a remote server:

1. Click the **Upload Configuration File**; the screen 'Upload Configuration File' opens.

Figure 14-15: Upload Configuration File



Upload Configuration File

Load the Configuration File From PC on the Network:

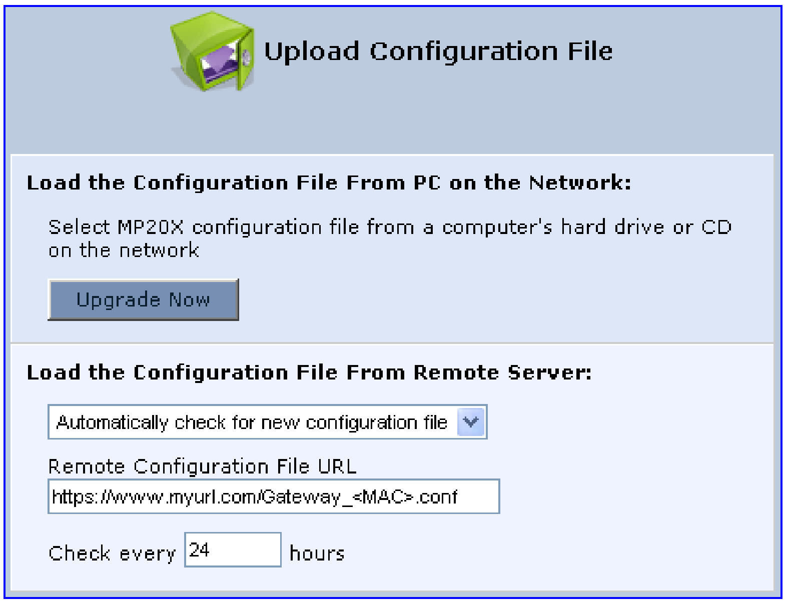
Select MP20X configuration file from a computer's hard drive or CD on the network

Load the Configuration File From Remote Server:

Automatic configuration file check disabled

2. 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
   - Automatic configuration file check disabled

Figure 14-16: Upload from Remote Server



Upload Configuration File

Load the Configuration File From PC on the Network:

Select MP20X 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

Remote Configuration File URL
https://www.myurl.com/Gateway_<MAC>.conf

Check every 24 hours

3. In the 'Remote Configuration File URL' field, enter the URL address of the remote server where the configuration file is located. The URL format is as follows: **protocol://server/filename.<conf/ini>,** for example:

   - ftp://10.10.10.10/MP20x_<MAC>.conf
   - http://20.20.20.20/MP20x_<MAC>.ini

   where <MAC> is replaced with the MAC address of MP-20x's WAN.

4. In the 'Check every' field, enter the time interval (in hours) for which MP-20x periodically checks for a new configuration file. if 0 is defined, MP-20x checks only once for a new configuration file, and this occurs after the system restarts.

5. Click the **OK** button. A download process begins. When downloading is completed, a confirmation screen appears, asking you if you want to load the new version.

6. Click **OK** to confirm. The upgrade process begins and should take no longer than one minute to complete. At the conclusion of the upgrade process, MP-20x 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:

- For additional security, MP-20x can be configured to use HTTPS client-server certification when connecting to a remote server (refer to 'Certificates' on page 210).
- 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. MP-20x 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 MP-20x 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 MP20x.conf file. A recommended procedure is to start with a MP-20x 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 243.
- The string <MAC> enables the ISP to pre-configure all its deployed MP-20xs with the same URL and file details (under rmt_config/url) and still have each MP-20x download its unique configuration file. Once the URL is configured with the string <MAC>, MP-20x that is trying to update its configuration file automatically replaces <MAC> with its own unique MAC address. For example, if there's a MP-20x 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 MP-20x, 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.

14.3.3 Encrypting a Configuration File Using CLI

Encrypted files include the file name extension .cfx (instead of .cfg) or .inx (instead of .ini). After MP-20x loads the encrypted file from the HTTP server, it automatically identifies the encrypted file by its file name extensions .cfx or .inx, and subsequently decrypts the file before saving it to flash memory.

The following procedure describes how to encrypt configuration files.

➢ To encrypt a configuration file:

- Run the following CLI shell command (on Linux or Windows PC with OpenSSL installed):

  ```
  openssl des3 -in <original file> -out <encrypted file> -k
  <password> -S <salt value>
  ```

  Where,

  - <original file> depicts the original cleartext configuration file (.cfg or .ini file).
  - <encrypted file> depicts the output file (an encrypted .cfx or .inx file).
  - <password> depicts the password that is used to encrypt the file.
  - <salt value> depicts the 8 bytes of a special key value that is combined with the password. The format is 16 hexadecimal digits [0-9,A-F].

  An example of this command is shown below:

```
openssl des3 -in c:\temp\try_enc_conf.cfg -out
c:\temp\try_enc_conf.cfx -k MyPassword123456 -S 0123456789ABCDEF
```

Notes:

- You can choose any <salt value> – MP-20x does not have to know about it.
- A password can be pre-configured in MP-20x, using the following CLI command: rg_conf_set_obscure /rmt_config/password <password>
- You can also define the password in a configuration file that you download from the server.
- If you don't define a password in the configuration file, a default password is used. Different default passwords are defined per customer, according to the config-file url hostname

14.3.4 Automatic Upload Using SIP NOTIFY Message

You can enable automatic software upgrade for MP-20x from a remote server, using the SIP NOTIFY message. The contents of the configuration file can initiate ("push") the remote server to upgrade (or a downgrade) MP-20x to a desired SW version.

➢ To "push" a configuration file when a change of parameter is needed:

1. Create a new configuration file with the required change.
2. Place the file on the HTTP server.
3. Send the SIP NOTIFY message to MP-20x; MP-20x integrates the contents of the new file and reboots.

➢ To “push” a configuration file and initiate an upgrade or downgrade:

1. Create a new configuration file that includes two important entries:

   a. In rg_conf/rmt_upd/chech_sync_version, configure the details of the version to which you want MP-20x to upgrade or downgrade, for example:
   ```
   (rmt_upd
           (check_sync_version(2.6.0_build_1))
   )
   ```
   a. You may need to update the URL address from where MP-20x is downloading the firmware (the path is configured in rmt_upd/url).

Note: In the case of a downgrade, the service provider MUST put a configuration file based on a template that matches the version to which the system is downgrading.

2. Place the file on the HTTP server.

3. Send the SIP NOTIFY message to MP-20x; MP-20x integrates the contents of the new file and reboots. After rebooting, MP-20x compares the currently running version with the version which is configured in rmt_upd/chech_sync_version and then determines whether to connect to the rmt_upd/url for downloading the new rmt file. Once the file is downloaded, it’s headers are parsed, and only if it represents the same version which was configured in the value of rmt_upd/chech_sync_version, does the upgrade/downgrade process begin.

14.4 DNS Server

Domain Name System (DNS) provides a service that translates domain names into IP addresses and vice versa. MP-20x'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 MP-20x'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).

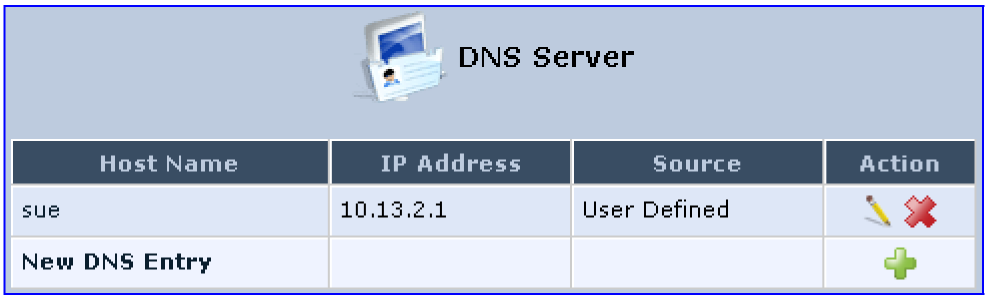
The DNS server does not require configuration. However, you may wish to view the list of computers known by the DNS, edit the host name or IP address of a computer on the list, or manually add a new computer to the list.

14.4.1 Viewing and Modifying the DNS Table

➢ To add a new host computer to the DNS table:

1. In the 'Advanced' screen, click the **DNS Server** icon; the DNS table is displayed.

Figure 14-17: DNS Server

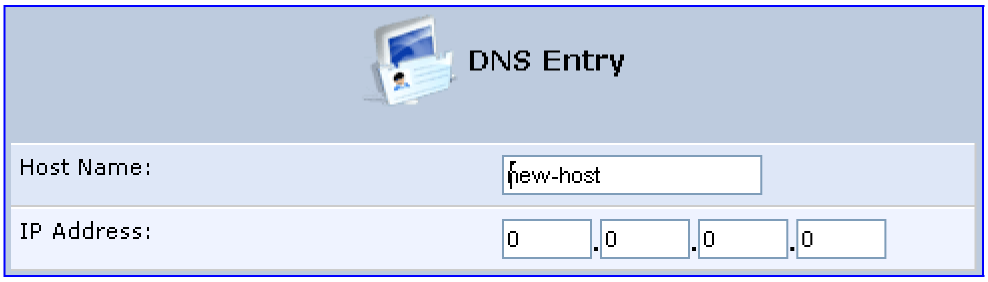


DNS Server

Host Name	IP Address	Source	Action
sue	10.13.2.1	User Defined	✎ ✖
New DNS Entry			✚

2. Click the link **New DNS Entry**; the 'DNS Entry' screen opens.

Figure 14-18: DNS Entry



Host Name:	new-host
IP Address:	0 . 0 . 0 . 0

3. Enter the computer's host name and IP address.
4. Click **OK** to save your changes.

➢ To edit the host name or IP address of an entry:

1. Click the **Edit** icon corresponding to the host that you want to edit; 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 the **Delete** icon corresponding to the host that you want to delete; the entry is removed from the table.

14.5 Diagnostics

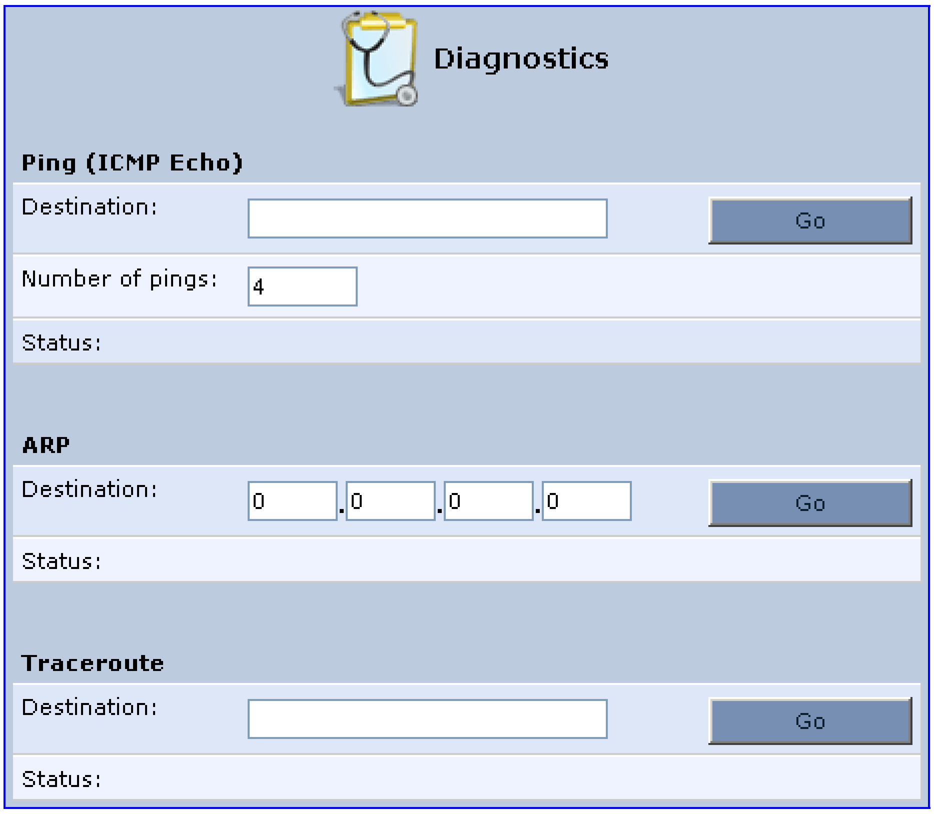
The 'Diagnostics' screen can assist you to test network connectivity and view statistics, such as the number of packets transmitted and received, round-trip time and success status. The test tools are platform-dependent and are not available simultaneously.

14.5.1 Diagnosing Network Connectivity

➢ To diagnose network connectivity:

1. In the 'Advanced' screen, click the **Diagnostics** icon; the 'Diagnostics' screen is displayed.

Figure 14-19: Advanced - Diagnostics



Diagnostics

Ping (ICMP Echo)

Destination:		Go
Number of pings:	4	
Status:		

ARP

Destination:	0 . 0 . 0 . 0	Go
Status:		

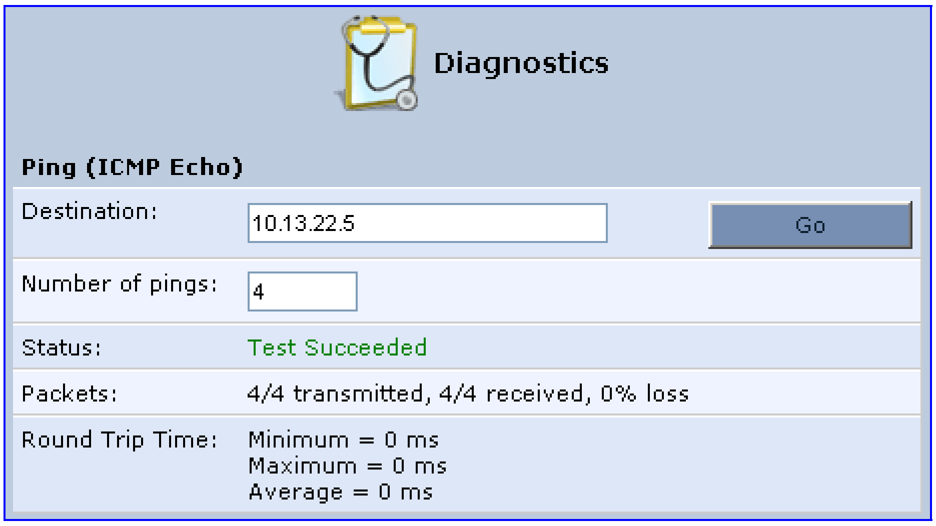
Traceroute

Destination:		Go
Status:		

2. Under the section 'Ping (ICMP Echo)', perform the following:
   - In the 'Destination' field, enter the IP address or URL to be tested.
   - In the 'Number of pings' field, enter the number of pings you want to perform.

3. Click the **Go** button; after a few seconds, diagnostic statistics are displayed. If no new information is displayed, click the **Refresh** button.

Figure 14-20: Advanced - Diagnostics - Statistics


Diagnostics

Ping (ICMP Echo)

Destination:	10.13.22.5	Go
Number of pings:	4	
Status:	Test Succeeded	
Packets:	4/4 transmitted, 4/4 received, 0% loss	

Round Trip Time:	Minimum = 0 ms
	Maximum = 0 ms
	Average = 0 ms	

14.5.2 Performing an ARP Test

The Address Resolution Protocol (ARP) test is used to query the physical address (MAC) of a host.

➢ To run the ARP test:

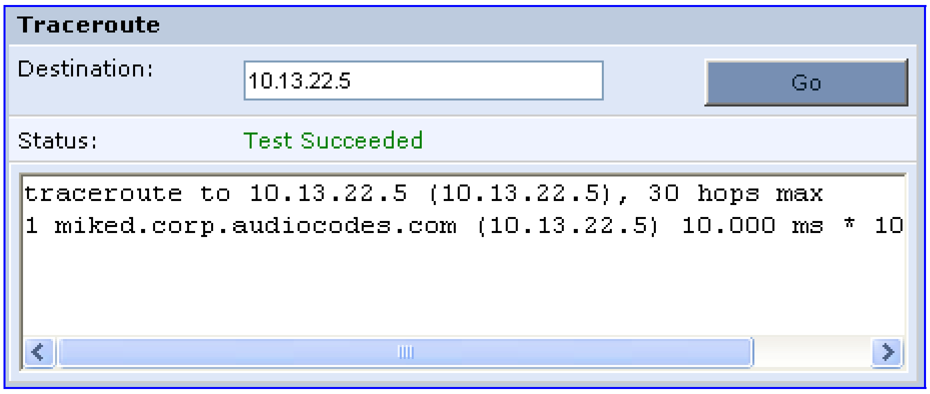
1. In the 'Destination' field, enter an IP address of the target host.
2. Click **Go**; after a few moments, diagnostic statistics is displayed. If no new information is displayed, click **Refresh**.

14.5.3 Performing a Traceroute

➢ **To perform a traceroute:**

1. In the 'Advanced' screen, click the **Diagnostics** icon; the 'Diagnostics' screen is displayed.
2. Under the section 'Traceroute', in the 'Destination' field, enter the IP address or URL to be tested.
3. Click **Go**; a traceroute commences, constantly refreshing the screen.

Figure 14-21: Traceroute Results



Destination: 10.13.22.5

Status: Test Succeeded

```
traceroute to 10.13.22.5 (10.13.22.5), 30 hops max
1 miked.corp.audiocodes.com (10.13.22.5) 10.000 ms * 10
```

4. To stop the trace and view the results, click **Cancel**.

14.6 Firmware Upgrade

MP-20x 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. (Refer to 'Upgrading from a Computer on the Network' on page 226.)
- 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. (Refer to 'Upgrading from the Internet' on page 228.)

MP-20x provides a flash memory of 8 MB, which is capable of storing two firmware images. In addition to the primary firmware, MP-20x also stores a recovery firmware, which is used only if the primary image is missing or damaged (e.g. if the user unplugs the power during firmware upgrade). Except for the analog or VoIP interfaces, the recovery image supports all interfaces and enables MP-20x to reconnect to the Internet and download the primary firmware.

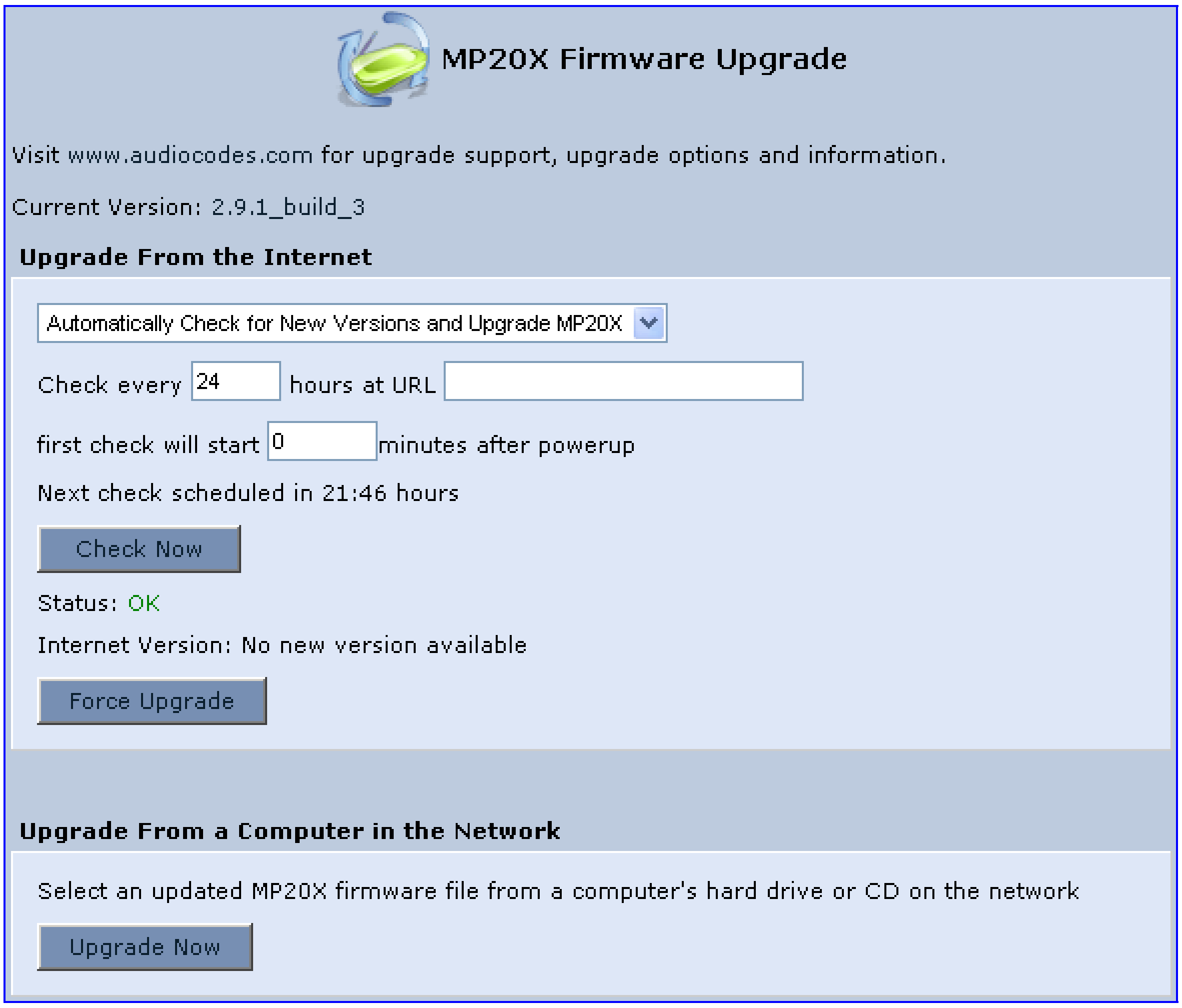
14.6.1 Upgrading from a Computer on the Network

➢ **To upgrade MP-20x'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. In the 'Advanced' screen, click the **Firmware Upgrade** icon; the screen 'MP-20x Firmware Upgrade' opens.

Figure 14-22: MP-20x Firmware Upgrade Screen



MP20X Firmware Upgrade

Visit www.audiocodes.com for upgrade support, upgrade options and information.

Current Version: 2.9.1_build_3

Upgrade From the Internet

Automatically Check for New Versions and Upgrade MP20X

Check every 24 hours at URL

first check will start 0 minutes after powerup

Next check scheduled in 21:46 hours

Check Now

Status: OK

Internet Version: No new version available

Force Upgrade

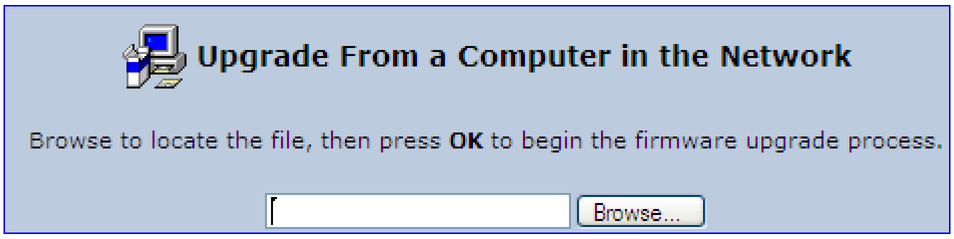
Upgrade From a Computer in the Network

Select an updated MP20X firmware file from a computer's hard drive or CD on the network

Upgrade Now

2. In the section 'Upgrade From a Computer in the Network', click the button **Upgrade Now**; the screen 'Upgrade From a Computer in the Network' opens.

Figure 14-23: Upgrade From a Computer in the Network Screen



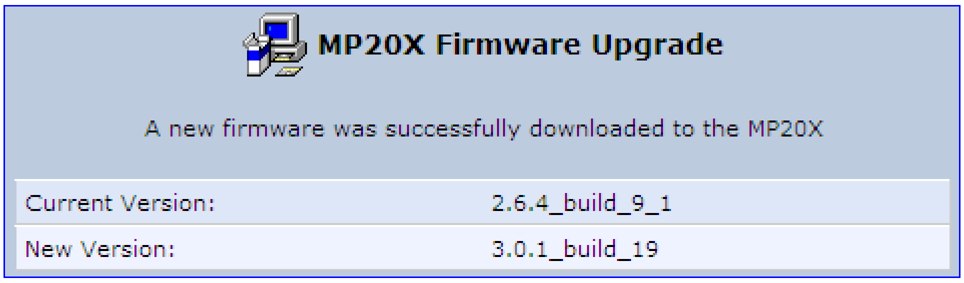
Upgrade From a Computer in the Network

Browse to locate the file, then press **OK** to begin the firmware upgrade process.

3. In the 'Firmware Upgrade File' field, enter the path of the software image file or click **Browse** and navigate to the *rmt* file on your PC.

4. Click **OK**; the MP-20x uploads the file from your PC. When loading is complete, a confirmation screen prompts you if you want to upgrade to the new version.

Figure 14-24: Confirming Firmware Upgrade Screen



MP20X Firmware Upgrade

A new firmware was successfully downloaded to the MP20X

Current Version:	2.6.4_build_9_1
New Version:	3.0.1_build_19

5. Click **OK** to confirm; the upgrade process commences (a few minutes). At the conclusion of the upgrade process, the device automatically reboots. The new software version runs, maintaining your custom configurations and settings.

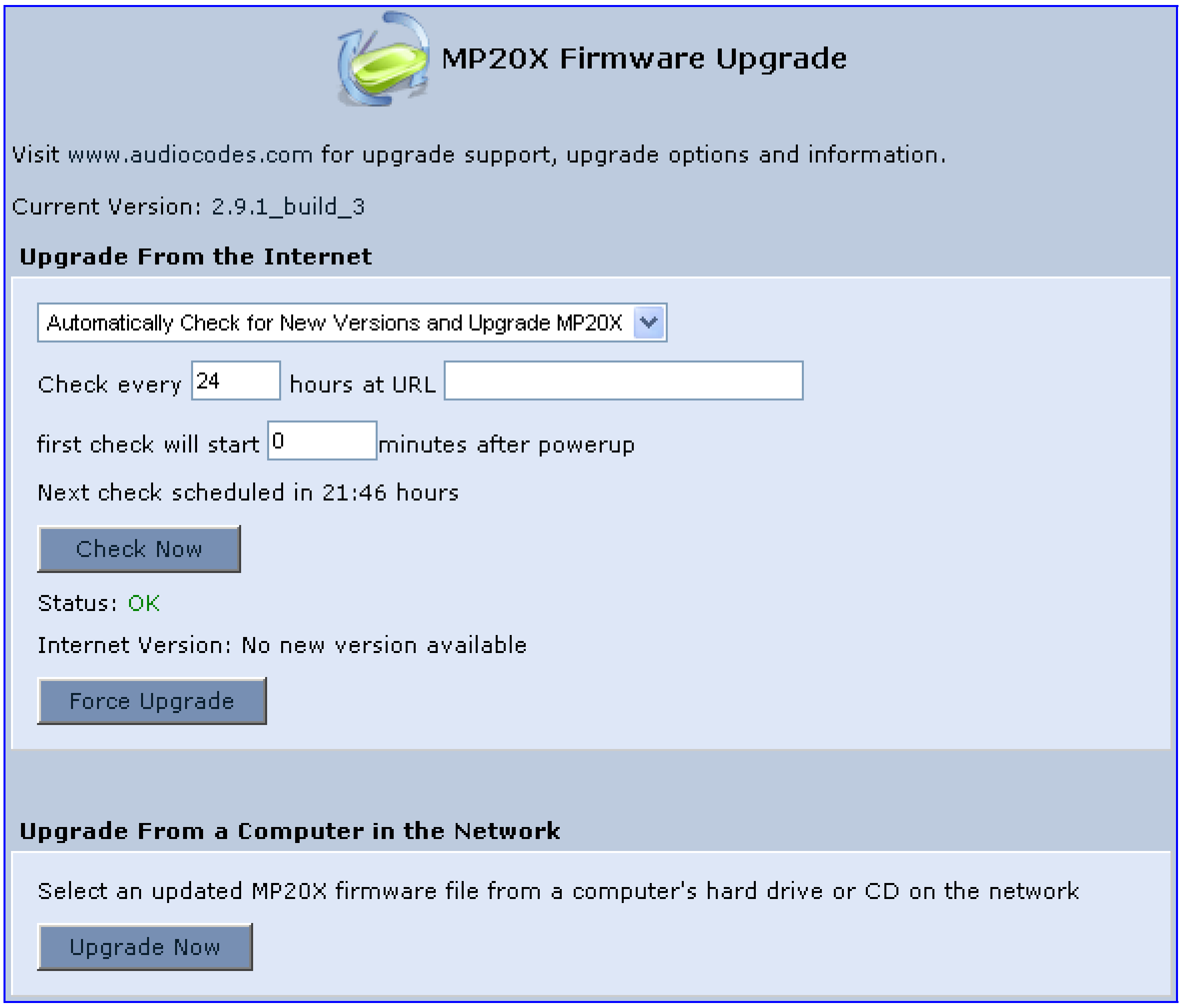
14.6.2 Upgrading From the Internet

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. These updates are from a user-defined URL.

➢ **To upgrade MP-20x's software image from the Internet:**

1. In the 'Advanced' screen, click the **Firmware Upgrade** icon; the screen 'MP-20x Firmware Upgrade' opens.

Figure 14-25: Advanced - Firmware and Configuration Upgrade



MP20X Firmware Upgrade

Visit www.audiocodes.com for upgrade support, upgrade options and information.

Current Version: 2.9.1_build_3

Upgrade From the Internet

Automatically Check for New Versions and Upgrade MP20X

Check every 24 hours at URL

first check will start 0 minutes after powerup

Next check scheduled in 21:46 hours

Status: OK

Internet Version: No new version available

Upgrade From a Computer in the Network

Select an updated MP20X firmware file from a computer's hard drive or CD on the network

2. In the 'Upgrade From the Internet' section, you can select the utility's checking method and interval.
   - **Automatically Check for New Versions and Upgrade MP20X:** MP-20x automatically checks for new versions every user-defined interval (defined in the 'Check every' field) at the URL address defined in the 'URL' field. You can define the time (in minutes) after which the first check commences after MP-20x is reset.
   - **Automatic Check Disable:** MP-20x checks for a new version at the URL address defined in the 'URL' field, when you click the **Check Now** button.

The result of the last performed check is displayed between the **Check Now** and **Force Upgrade** buttons, indicating whether a new version is available or not.

3. If a new version is available:
   a. Click the **Force Upgrade** button. A download process begins. When downloading is complete, a confirmation screen appears, asking you if you want to upgrade to the new version.
   b. Click **OK** to confirm. The upgrade process begins and should take no longer than one minute to complete. At the conclusion of the upgrade process, MP-20x automatically reboots and the new software version runs.
4. If a new version is unavailable:
   a. 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.
   b. Click the **Refresh** button until the check is completed and the result is displayed.

14.7 IP Address Distribution

Your MP-20x'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. MP-20x'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 also receives 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 then makes the IP address available for use by others.

Your MP-20x's DHCP server:

- Displays a list of all DHCP host devices connected to MP-20x
- 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

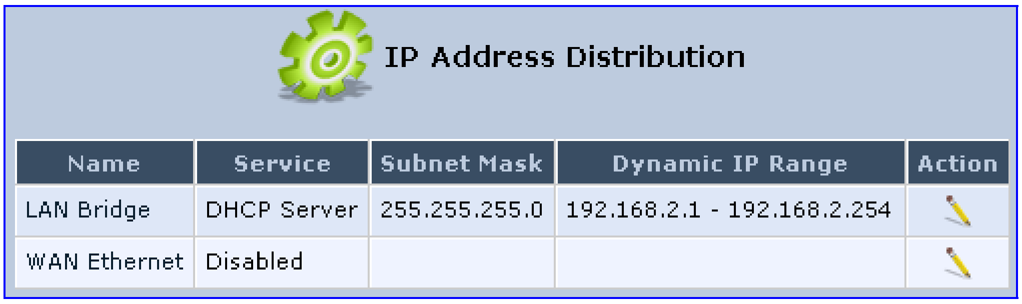
Additionally, MP-20x can act as a DHCP relay, escalating DHCP responsibilities to a WAN DHCP server. In this case, MP-20x acts merely as a router, while its LAN hosts receives their IP addresses from a DHCP server on the WAN.

With MP-20x's optional Zero Configuration Technology feature, the IP Auto Detection method detects statically-defined IP addresses in addition to MP-20x'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.

➢ **To view a summary of the services currently being provided by the DHCP server:**

- In the 'Advanced' screen, click the **IP Address Distribution** icon; the 'IP Address Distribution' screen opens.

Figure 14-26: DHCP Server Summary



IP Address Distribution

Name	Service	Subnet Mask	Dynamic IP Range	Action
LAN Bridge	DHCP Server	255.255.255.0	192.168.2.1 - 192.168.2.254	✎
WAN Ethernet	Disabled			✎

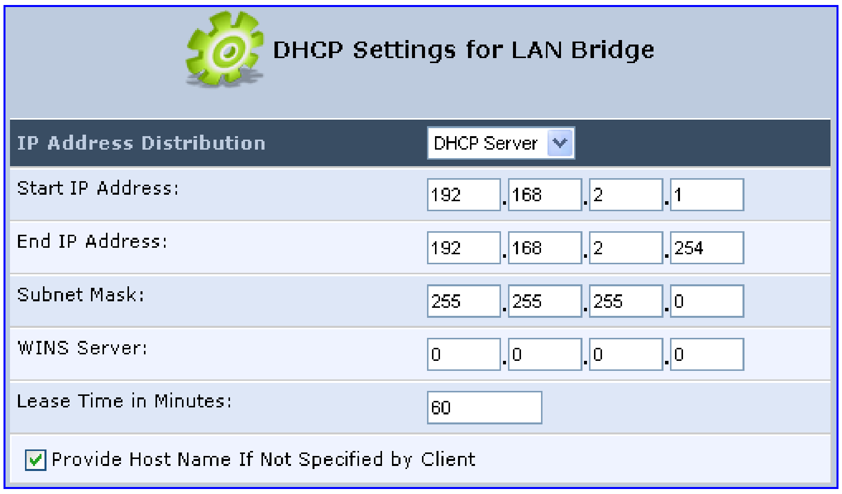
Note: If In the column 'Service', if a MP-20x is indicated 'Disabled', then DHCP services are not being provided to hosts connected to the network through that MP-20x. This means that MP-20x does not assign IP addresses to these computers, which is useful if you wish to work with static IP addresses only.

14.7.1 DHCP Server Parameters

➢ To edit the DHCP server settings for a device:

1. In the 'IP Address Distribution' screen, click the **Edit** icon corresponding to the entry that you want to edit; the DHCP Server settings for this device are displayed.

Figure 14-27: DHCP Settings Screen



DHCP Settings for LAN Bridge

IP Address Distribution	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 (MP-20x serves as a DHCP server or DHCP relay) or disable the DHCP server.

   - **DHCP Server:** the screen is displayed as shown in the figure above.

     a. **Start IP Address** and **End IP Address** (IP address range): determines the number of hosts that may be connected to the network in this subnet. The 'Start IP Address' field specifies the first IP address that may be assigned in this subnet; the 'End IP Address' field specifies the last IP address in the range.

     b. **Subnet Mask:** mask used to determine the subnet to which an IP address belongs (e.g., 255.255.0.0).

     c. **Lease Time in Minutes:** each device is assigned an IP address by the DHCP server for a limited time when it connects to the network. When the lease expires the server determines 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 become available for other computers on the network.

     d. **Provide Host Name If Not Specified by Client:** if the DHCP client does not have a host name, the Telephone Adapter assigns the client a default name.

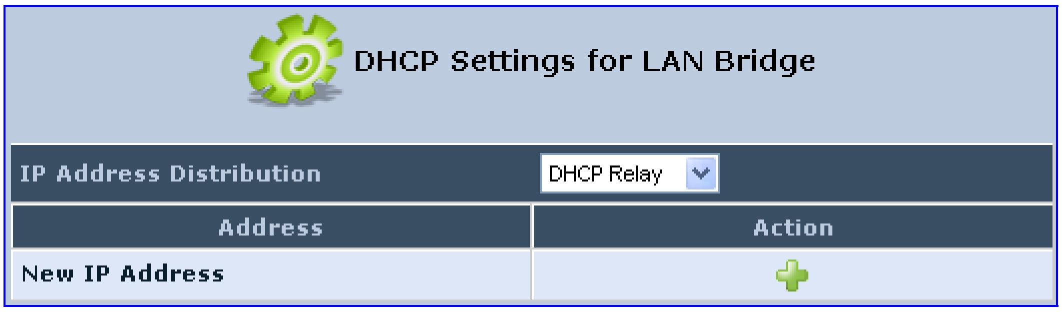
14.7.2 DHCP Relay Parameters

Your MP-20x can act as a DHCP relay in case you would like to dynamically assign IP addresses from a DHCP server other than your MP-20x's DHCP server. Note that when selecting this option you must also change MP-20x's WAN to work in routing mode.

➢ **To configure a device as a DHCP relay, perform the following steps:**

1. In the 'IP Address Distribution' screen, click the **Edit** icon corresponding to the entry that you want to edit; the DHCP Server settings for this device are displayed.
2. From the 'IP Address Distribution' drop-down list, select the 'DHCP Relay' option; the 'DHCP Settings' screen appears.

Figure 14-28: DHCP Settings



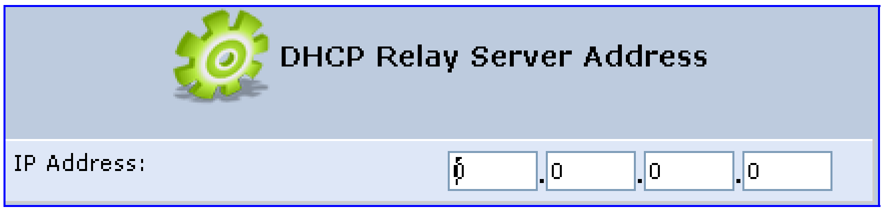
DHCP Settings for LAN Bridge

IP Address Distribution: DHCP Relay

Address	Action
New IP Address	✚

3. Click the **New IP Address** link; the screen 'DHCP Relay Server Address' screen appears.

Figure 14-29: DHCP Relay Server Address Screen



DHCP Relay Server Address

IP Address: 0 . 0 . 0 . 0

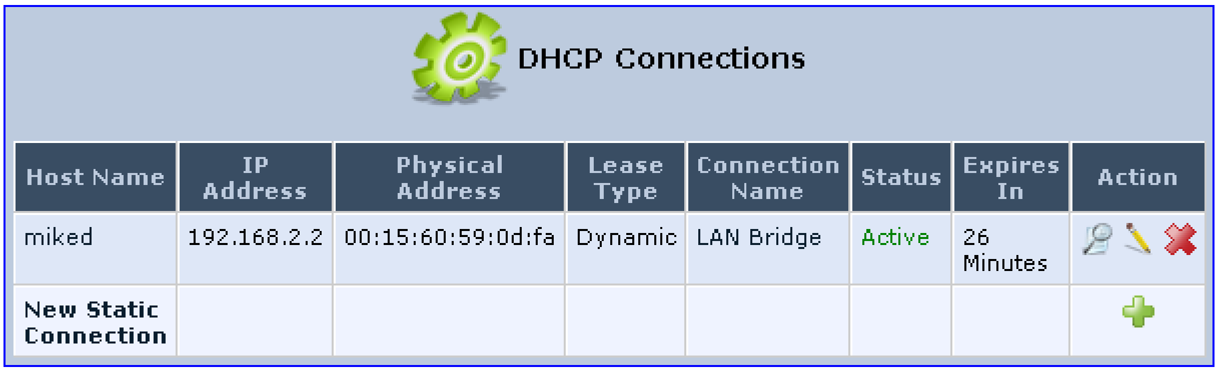
4. In the 'IP Address' field, enter the IP address of the DHCP server.
5. Click **OK** to save your changes.
6. Click **OK** once more in the 'DHCP Settings' screen.
7. Change MP-20x's WAN to work in routing mode:
   a. On the sidebar menu, click the **Network Connections** menu; the screen 'Network Connections' opens.
   b. Click the link 'WAN Ethernet'; the 'WAN Ethernet Properties' screen opens.
   c. Click the button **Settings**; the screen 'Configure WAN Ethernet' opens.
   d. In the screen section 'Routing', select 'Advanced' from the drop-down list; the screen refreshes.
   e. In the 'Routing Mode' drop-down list, select 'Route'; this changes MP-20x's WAN to work in routing mode, which is necessary in order for DHCP relaying to function correctly.
   f. Click **OK** to save the settings.

14.7.3 DHCP Connections

➢ To view a list of computers currently recognized by the DHCP server:

1. Open the screen 'IP Address Distribution'.
2. Click the **Connection List** button; the 'DHCP Connections' screen opens.

Figure 14-30: Advanced - IP Address Distribution - Connection List

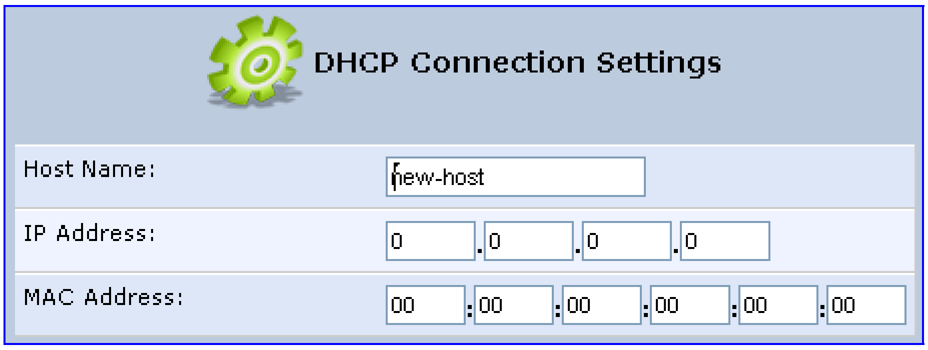

DHCP Connections

Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expires In	Action
miked	192.168.2.2	00:15:60:59:0d:fa	Dynamic	LAN Bridge	Active	26 Minutes	
New Static Connection							

➢ To define a new connection with a fixed IP address:

1. Click the link **New Static Connection**; the screen 'DHCP Connection Settings' opens.

Figure 14-31: 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. In the 'Host Name' field, enter a host name for this connection.
3. In the 'IP Address' field, enter the fixed IP address to be assigned to the computer.
4. In the 'MAC Address' field, 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.

5. 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' icons.

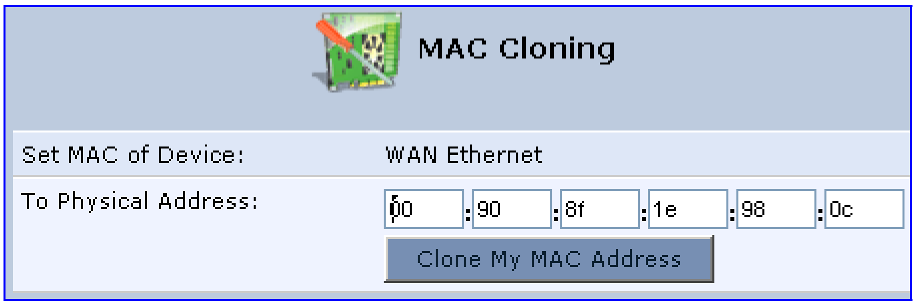
14.8 MAC Cloning

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 MP-20x, you can simplify the installation process by copying the MAC address of your existing PC to MP-20x. 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. In the 'Advanced' screen, click the **MAC Cloning** icon; the 'MAC Cloning' screen appears.

Figure 14-32: Advanced - MAC Cloning Settings



MAC Cloning

Set MAC of Device:	WAN Ethernet
To Physical Address:	00 : 90 : 8f : 1e : 98 : 0c

2. In the 'To Physical Address' field, enter the physical MAC address to be cloned.
3. Click the button **Clone My MAC Address**.

14.9 Network Objects

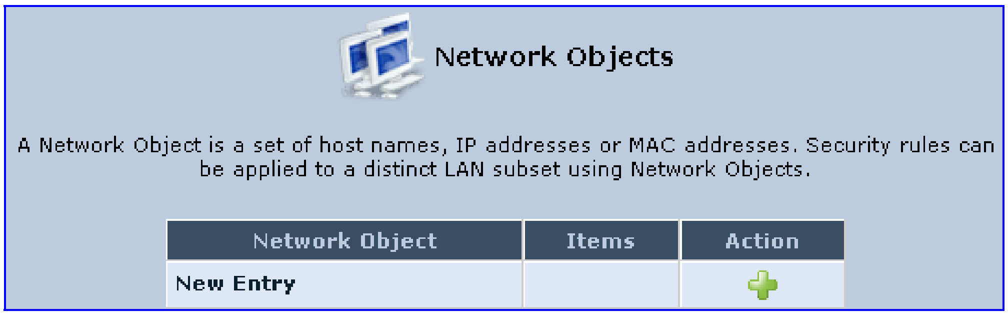
Network Objects is a method used to logically define a set of LAN hosts, according to one or more MAC address, IP address, and host name. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring MP-20x's security filtering settings such as IP address filtering, host name filtering or MAC address filtering.

You can use network objects 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. In the 'Advanced' screen, click the **Network Objects** icon; the 'Network Objects' screen appears.

Figure 14-33: Network Objects Screen



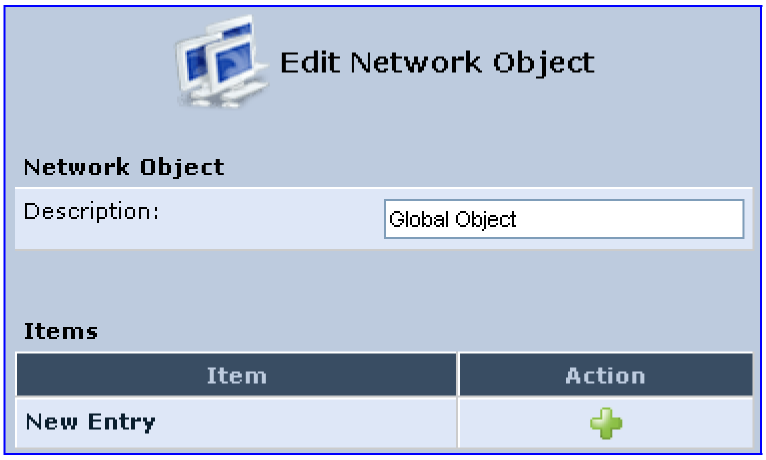
Network Objects

A Network Object is a set of host names, IP addresses or MAC addresses. Security rules can be applied to a distinct LAN subset using Network Objects.

Network Object	Items	Action
New Entry		✚

2. Click the link **New Entry**; the 'Edit Network Object' screen appears.

Figure 14-34: Edit Network Objects Screen



Edit Network Object

Network Object

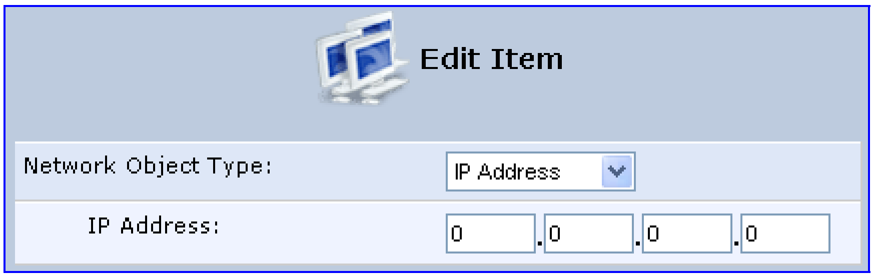
Description: Global Object

Items

Item	Action
New Entry	✚

3. In the 'Description' field, enter a name for the network object, and then click the **New Entry** link to create it; the 'Edit Item' screen appears.

Figure 14-35: Edit Item Screen


Edit Item

Network Object Type: IP Address

IP Address: 0 . 0 . 0 . 0

4. From the 'Network Object Type' drop-down lists, select a source address type:
   - IP Address
   - IP Subnet
   - IP Range
   - MAC Address
   - Host Name
   - DHCP Option (supporting options 60, 61, and 77)

   When selecting a method from the drop-down list, the screen refreshes, presenting the respective fields by which to enter the relevant information.

5. Click **OK** to save the settings.

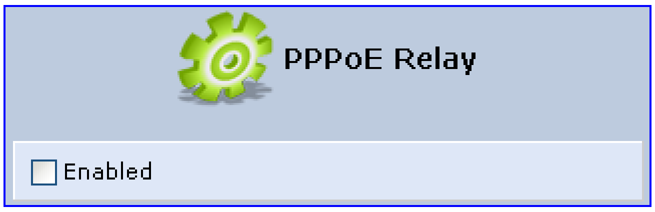
14.10 PPPoE Relay

PPPoE Relay enables MP-20x to relay packets on PPPoE connections, while keeping its designated functionality for any additional connections. The PPPoE Relay screen displays a check box that enables PPPoE Relay.

➢ To enable PPPoE relay:

1. In the 'Advanced' screen, click the **PPPoE Relay** icon; the 'PPPoE Relay' screen is displayed.

Figure 14-36: PPPoE Relay Screen


PPPoE Relay

☐ Enabled

2. Select the 'Enabled' check box.

14.11 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 changes accordingly to reflect the change. In this way, even though your IP address changes often, your domain name remains constant and accessible.

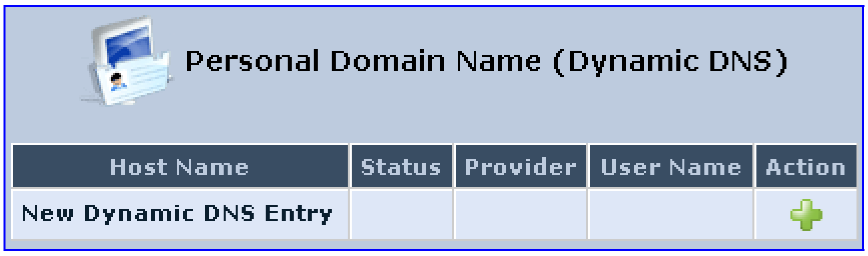
14.11.1 Opening a Dynamic DNS Account

To be able to use the Dynamic DNS (DDNS) feature, you must first open a free DDNS account at http://www.dyndns.org/account/create.html. When applying for an account, you need to specify a user name and password. Have them readily available when customizing MP-20x's DDNS support. For detailed information on DDNS, refer to http://www.dyndns.org.

➢ **To open a dynamic DNS account:**

1. In the 'Advanced' screen, click the **Personal Domain Name (Dynamic DNS)** icon; the 'Personal Domain Name (Dynamic DNS)' screen opens.

Figure 14-37: Personal Domain Name (Dynamic DNS) Screen

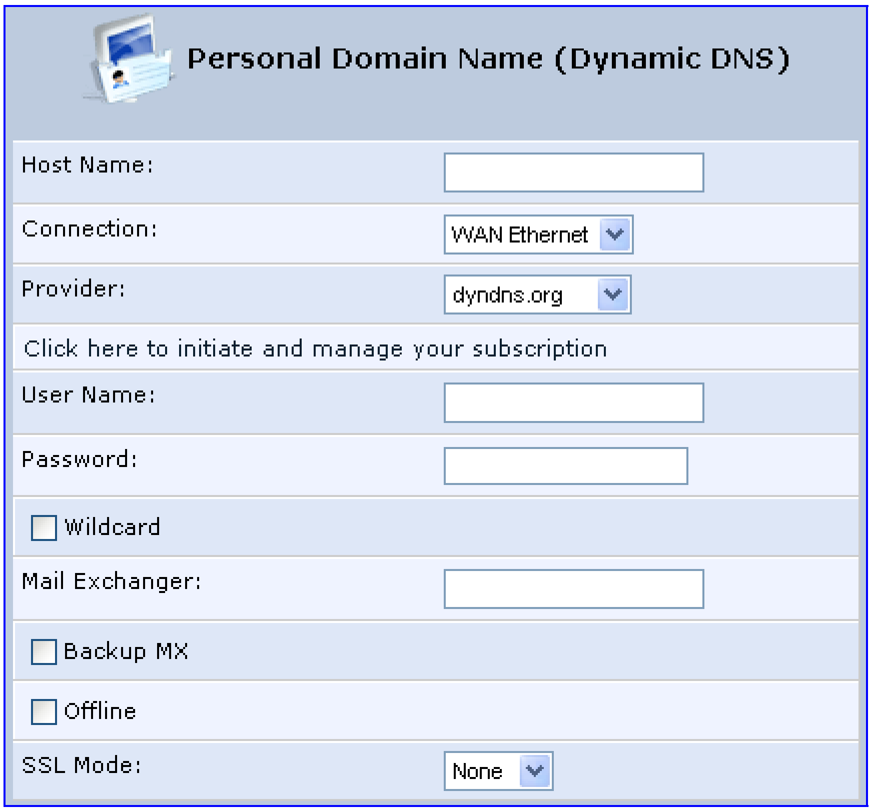


Personal Domain Name (Dynamic DNS)

Host Name	Status	Provider	User Name	Action
New Dynamic DNS Entry				✚

2. Click the link **New Dynamic DNS Entry** to add a new connection; the 'Personal Domain Name (Dynamic DNS)' screen appears.

Figure 14-38: Personal Domain Name (Dynamic DNS) - Adding



Personal Domain Name (Dynamic DNS)

Host Name:	
Connection:	WAN Ethernet
Provider:	dyndns.org
Click here to initiate and manage your subscription	
User Name:	
Password:	
☐ Wildcard	
Mail Exchanger:	
☐ Backup MX	
☐ Offline	
SSL Mode:	None

3. Configure the DDNS parameters. Use the table below as a reference.

Table 14-2: Dynamic DNS Parameter Descriptions

Parameter	Description
Host Name	Enter your full DDNS domain name.
Connection	In a single WAN scenario, the connection parameter appears as static text (non-configurable). However, if you have multiple WAN devices, a drop-down list box appears, 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 is used instead (assuming its route rules consent), until the chosen device is up again.
Provider	Select your DDNS service provider and then click the link **Click here to initiate and manage your subscription** to open the selected provider's account creation Web page. For example, when dyndns.org is selected, the following page opens: http://www.dyndns.com/account.
User Name	Enter your DDNS user name.
Password	Enter your DDNS password.
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.

Parameter	Description
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.
SSL Mode	With Secure Socket Layer (SSL), secured DDNS services are accessed using HTTPS. Upon connection, MP-20x validates the DDNS server's certificate. Use this entry to choose the certificate's validation method. ▪ **None:** Do not validate the server's certificate. ▪ **Chain:** Validate the entire certificate chain. When selecting this option, the screen refreshes, displaying the 'Validate Time' drop-down list for selecting whether to validate the certificate's expiration time ('Ignore' or 'Check' respectively). If the certificate has expired, the connection terminates immediately. ▪ **Direct:** Ensure that the server's certificate is directly signed by the root certificate. This option also provides the 'Validate Time' drop-down list for validation of the certificate's expiration time, as described above.

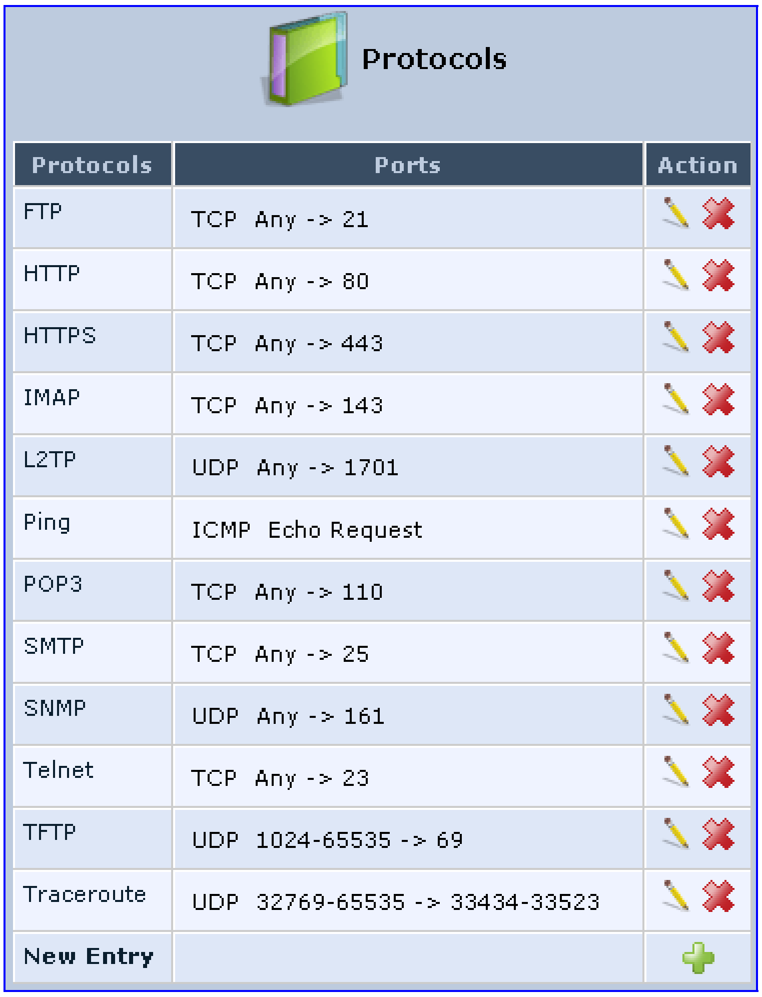
14.12 Protocols

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. In the 'Advanced' screen, click the **Protocols** icon;, the 'Protocols' screen appears.

Figure 14-39: Advanced - Protocols

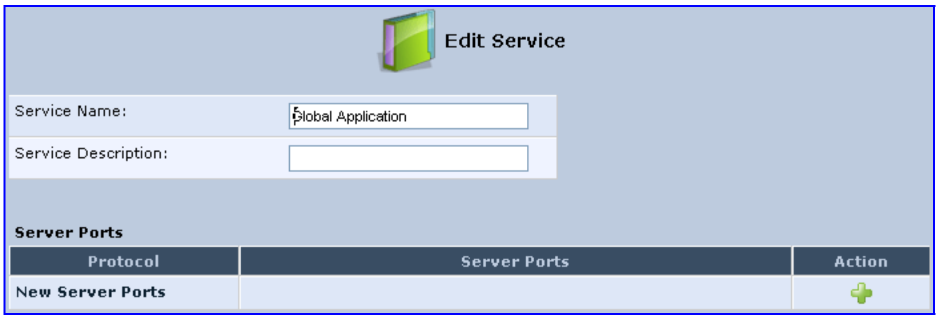


Protocols

Protocols	Ports	Action
FTP	TCP Any -> 21	
HTTP	TCP Any -> 80	
HTTPS	TCP Any -> 443	
IMAP	TCP Any -> 143	
L2TP	UDP Any -> 1701	
Ping	ICMP Echo Request	
POP3	TCP Any -> 110	
SMTP	TCP Any -> 25	
SNMP	UDP Any -> 161	
Telnet	TCP Any -> 23	
TFTP	UDP 1024-65535 -> 69	
Traceroute	UDP 32769-65535 -> 33434-33523	
New Entry		

2. Click the link **New Entry**; the 'Edit Service' screen appears.

Figure 14-40: Advanced - Protocols - Edit Service


Edit Service

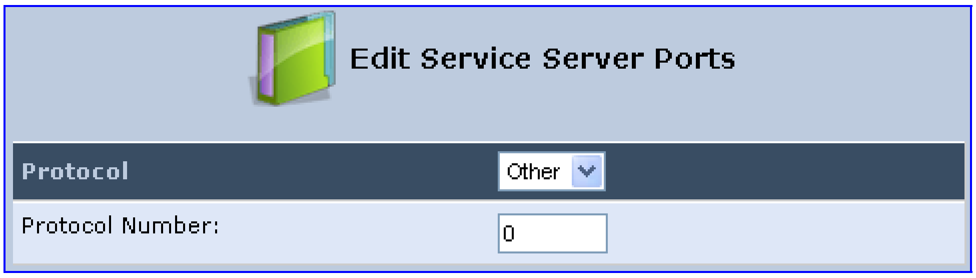
Service Name:	Global Application
Service Description:	

Server Ports

Protocol	Server Ports	Action
New Server Ports		✚

3. In the 'Service Name' field, enter the name of the service, and then click the link **New Service Ports**; the 'Edit Service Server Ports' screen appears.

Figure 14-41: Advanced - Protocols - Edit Service - Server Ports


Edit Service Server Ports

Protocol	Other
Protocol Number:	0

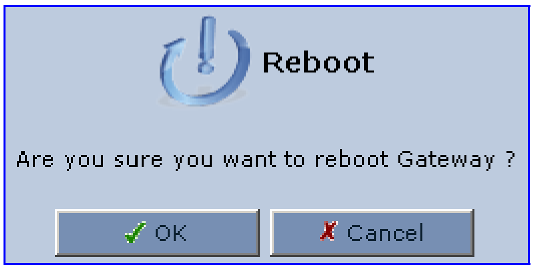
4. You may choose any of the protocols available in the drop-down list, or add a new one by selecting 'Other'. When selecting a protocol from the drop-down list, the screen refreshes, presenting the respective fields by which to enter the relevant information.
5. Select a protocol and enter the relevant information.
6. Click **OK** to save the settings.

14.13 Reboot

➢ **To reboot your MP-20x:**

1. In the 'Advanced' screen, click the **Reboot** icon; the 'Reboot' screen is displayed.

Figure 14-42: Reboot Screen


Reboot

Are you sure you want to reboot Gateway ?

2. Click **OK** to reboot MP-20x. This may take up to one minute.
3. To re-enter the Web-based management interface after rebooting MP-20x, click the browser's **Refresh** button.

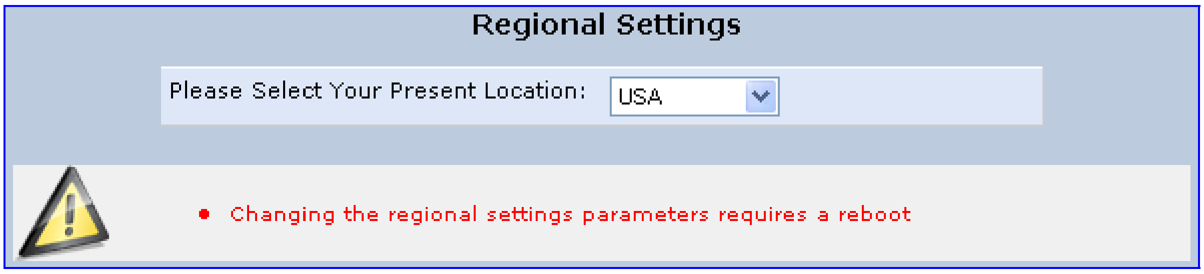
14.14 Regional Settings

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. MP-20x enables users to select the country they reside in and MP-20x automatically selects the correct regional settings.

➢ **To select your present location:**

1. In the 'Advanced' screen, click the **Regional Settings** icon; the 'Regional Settings' screen opens.
2. Select the country from the drop-down list. If your current location is not listed, contact your Service Provider.

Figure 14-43: Regional Settings


Regional Settings

Please Select Your Present Location: USA

● Changing the regional settings parameters requires a reboot

14.15 Remote Administration

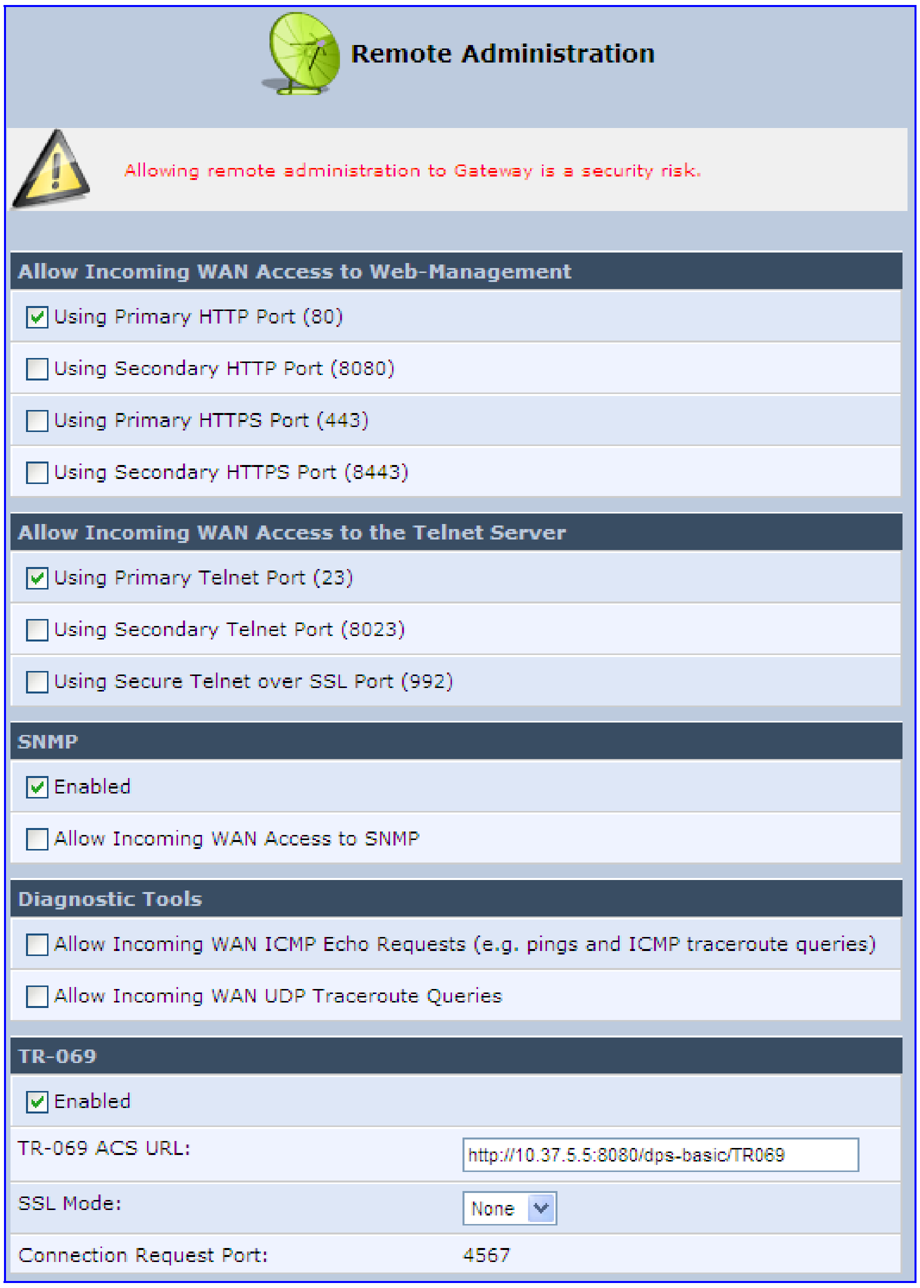
It is possible to access and control MP-20x not only from within the home network, but also from the Internet. This allows you to view or change settings while travelling. It also enables you to allow your ISP to change settings or help you trouble-shoot functionality or communication issues from a remote location.

Remote access to MP-20x 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 allow remote access to MP-20x services:

1. In the 'Advanced' screen, click the **Remote Administration** icon; the 'Remote Administration' screen appears.

Figure 14-44: Remote Administration Screen



Remote Administration

Allowing remote administration to Gateway is a security risk.

Allow Incoming WAN Access to Web-Management

- [✓] Using Primary HTTP Port (80)
- [ ] Using Secondary HTTP Port (8080)
- [ ] Using Primary HTTPS Port (443)
- [ ] Using Secondary HTTPS Port (8443)

Allow Incoming WAN Access to the Telnet Server

- [✓] Using Primary Telnet Port (23)
- [ ] Using Secondary Telnet Port (8023)
- [ ] Using Secure Telnet over SSL Port (992)

SNMP

- [✓] Enabled
- [ ] Allow Incoming WAN Access to SNMP

Diagnostic Tools

- [ ] Allow Incoming WAN ICMP Echo Requests (e.g. pings and ICMP traceroute queries)
- [ ] Allow Incoming WAN UDP Traceroute Queries

TR-069

- [✓] Enabled

TR-069 ACS URL: http://10.37.5.5:8080/dps-basic/TR069

SSL Mode: None

Connection Request Port: 4567

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.

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 MP-20x for the first time using encrypted remote administration, you are prompted by your browser with a warning regarding certificate authentication. This is due to the fact that MP-20x'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 MP-20x.

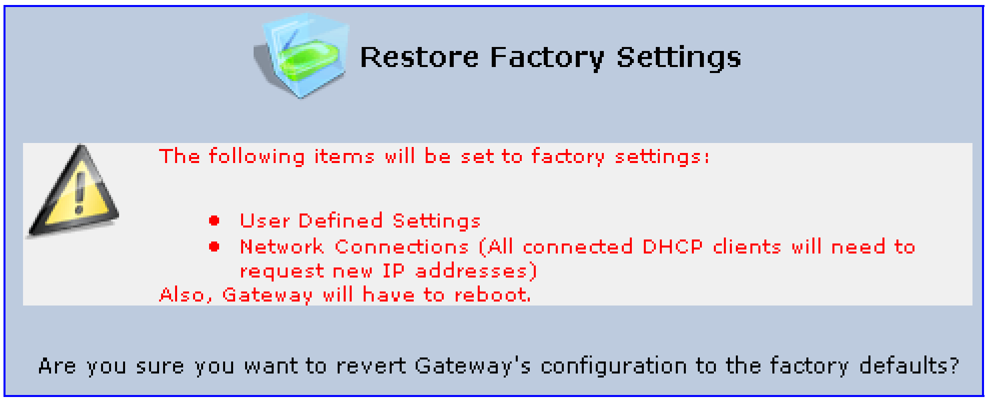
14.16 Restoring Factory Settings

You can restore MP-20x'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. In the 'Advanced' screen, click the **Restore Factory Settings** icon; the 'Restore Factory Settings' screen is displayed.

Figure 14-45: Restore Factory Settings Screen


Restore Factory Settings

The following items will be set to factory settings:

- User Defined Settings
- Network Connections (All connected DHCP clients will need to request new IP addresses)

Also, Gateway will have to reboot.

Are you sure you want to revert Gateway's configuration to the factory defaults?

2. Click **OK** to restore MP-20x's factory default settings.

Note: If you are accessing MP-20x's Web from the WAN, restoring the factory settings causes 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 MP-20x DC power cable.
2. Using a paper clip, press the push-button located on the bottom (base) of MP-20x (a pin hole located near one of the corners).
3. While pressing the push-button, power up the device. Keep the push-button pressed for another 5 seconds.

Note: All Web-based management settings and parameters, not only those in the **Advanced** menu are restored to their default values. This includes the administrator password; a user-specified password is no longer valid.

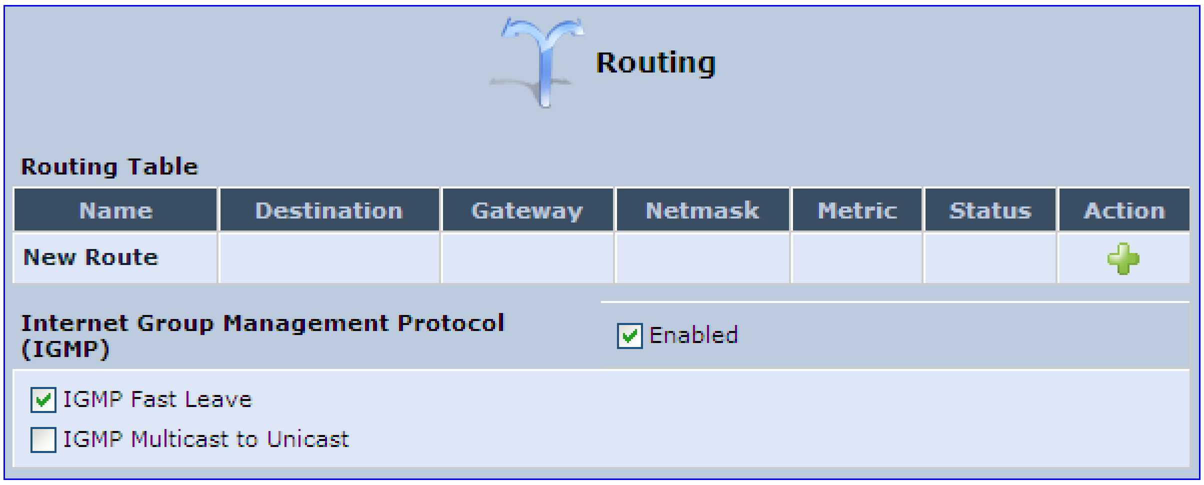
14.17 Routing

14.17.1 Managing Routing Table Rules

➢ **To manage routing tables:**

1. In the 'Advanced' screen, click the **Routing** icon; the 'Routing' screen is displayed.

Figure 14-46: Routing Rules



Routing

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						✚

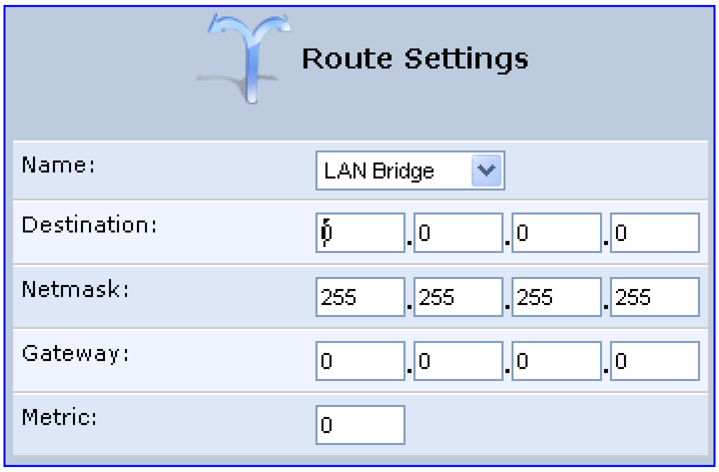
Internet Group Management Protocol (IGMP) ☑ Enabled

☑ IGMP Fast Leave

☐ IGMP Multicast to Unicast

2. Click the **New Route**; the 'Route Settings' screen opens.

Figure 14-47: Routing Rule Settings



Route Settings

Name: LAN Bridge

Destination: 0 . 0 . 0 . 0

Netmask: 255 . 255 . 255 . 255

Gateway: 0 . 0 . 0 . 0

Metric: 0

3. When adding a routing rule, you need to specify:

Table 14-3: 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.

14.17.2 Routing Protocols

MP-20x 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 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 MP-20x intercepts and processes the request. If MP-20x is set to 'Minimum Security' no further action is required. However, if MP-20x is set to 'Typical Security' or 'Maximum Security' you must add the group's IP address to MP-20x's 'Multicast Groups' screen. This allows incoming messages addressed to the group to pass through the Firewall and on to the correct LAN computer.

➢ **To configure routing protocols:**

1. In the 'Routing' screen, configure the desired routing protocols:
   - **Internet Group Management Protocol (IGMP) section:**
     a. Select the 'Enabled' check box to enable support for IGMP multicasting.
     b. Select the 'Enable IGMP Fast Leave' check box if you want MP-20x to stop forwarding traffic to a host that is the only subscriber, immediately upon request (without query delay).
     c. Select the 'IGMP Multicast to Unicast' check box to enable MP-20x to convert the incoming multicast data stream into unicast format to route it to the specific LAN host that had requested the data. In this way, MP-20x prevents flooding the rest of the LAN hosts with irrelevant multicast traffic.
   - **Domain Routing:** Select the 'Enabled' check box if you want MP-20x's DNS server to add a routing entry for the IP address of the reply through the device from which it arrived, when it receives a reply from an external DNS server. This means that future packets from this IP address will be routed through the device from which the reply arrived.
2. Click **OK**.

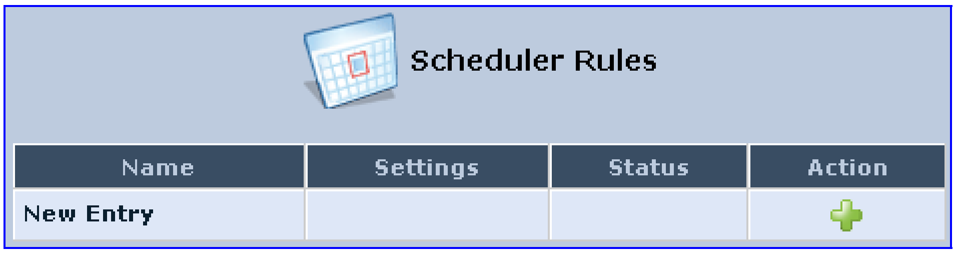
14.18 Scheduler Rules

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. In the 'Advanced' screen, click the **Scheduler** icon; the 'Scheduler Rules' screen appears.

Figure 14-48: Advanced - Scheduler Rules

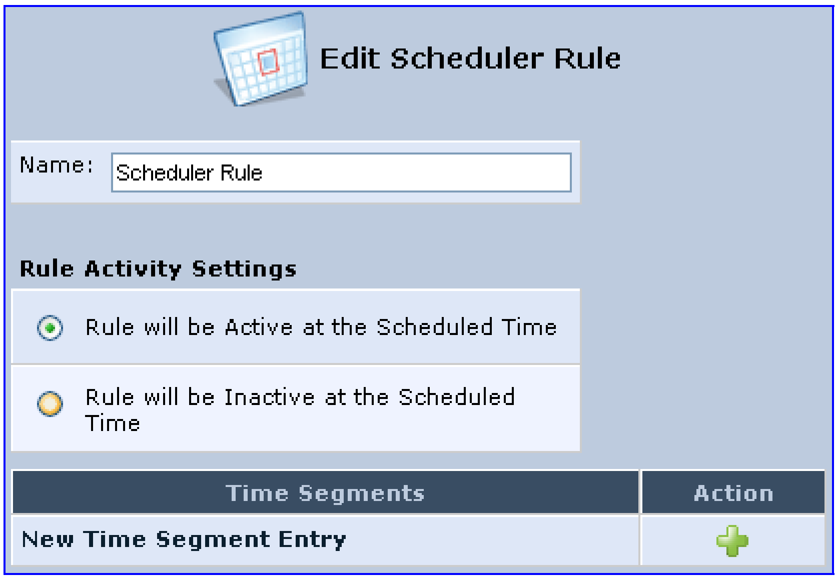


Scheduler Rules

Name	Settings	Status	Action
New Entry			✚

2. Click the link **New Entry**; the 'Edit Scheduler Rule' screen appears.

Figure 14-49: Edit Scheduler Rule Screen



Edit Scheduler Rule

Name: Scheduler Rule

Rule Activity Settings

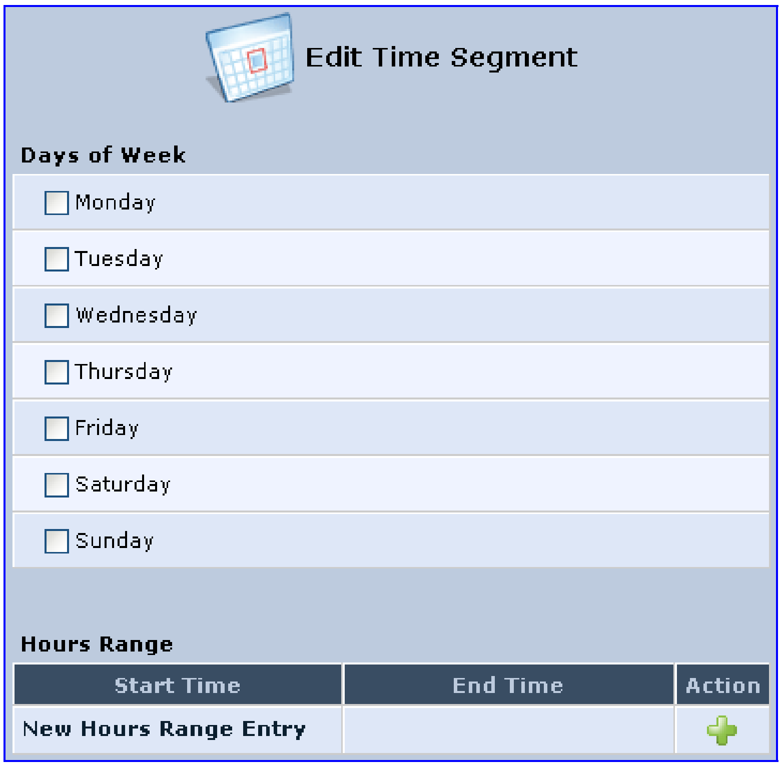
[✓ Rule will be Active at the Scheduled Time]

Rule will be Inactive at the Scheduled Time

Time Segments	Action
New Time Segment Entry	✚

3. In the 'Name' field, specify a name for the rule.
4. Under the 'Rule Activity Settings' section, specify if the rule is active or inactive during the designated time period, by selecting the appropriate check-box.
5. Click the link **New Time Segment Entry** to define the time segment to which the rule applies; the 'Edit Time Segment' screen appears.

Figure 14-50: Edit Time Segment Screen



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. In the 'Days of Week' list, select the days of the week for which you want the rule to be active.

b. In the 'Hours Range' table, click the link **New Hours Range Entry** to define an active/inactive hourly range.

6. Click **OK** to save the settings.

14.19 SNMP

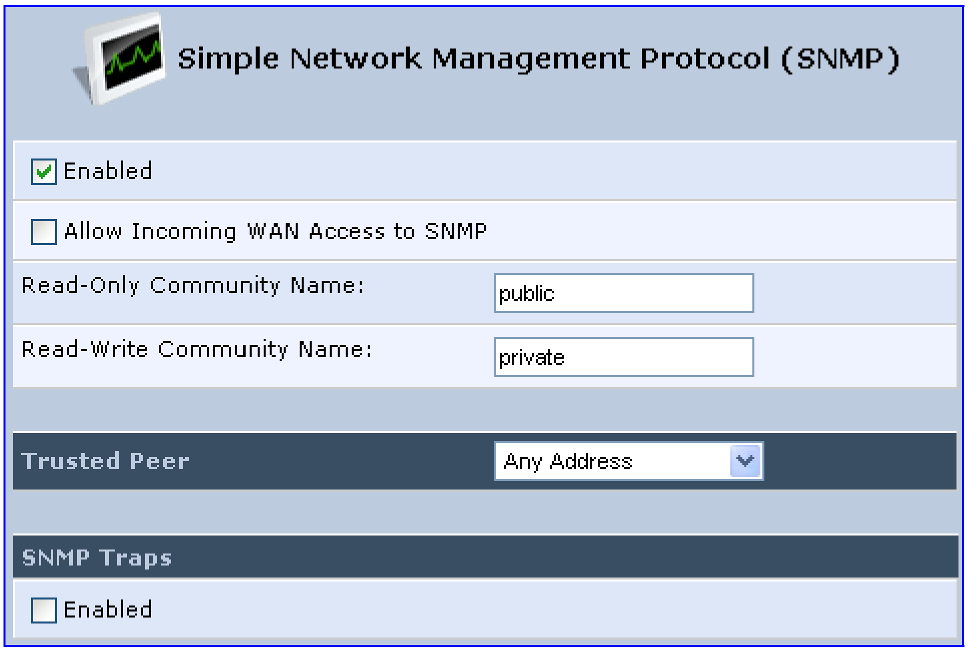
Simple Network Management Protocol (SNMP) enables Network Management Systems (NMSs) to remotely configure and monitor your MP-20x. Your Internet Service Provider (ISP) may use SNMP to identify and resolve technical problems.

Technical information regarding the properties of MP-20x's SNMP agent should be provided by your ISP.

➢ To configure MP-20x's SNMP agent:

1. In the 'Advanced' screen, click the **Simple Network Management Protocol (SNMP)** icon; the 'Simple Network Management Protocol (SNMP)' screen appears.

Figure 14-51: Advanced - SNMP


Simple Network Management Protocol (SNMP)

[✓] Enabled

[ ] Allow Incoming WAN Access to SNMP

Read-Only Community Name:	public
Read-Write Community Name:	private
Trusted Peer	Any Address

SNMP Traps

[ ] Enabled

2. Select the 'Enabled' check box to enable SNMP.

3. Define the SNMP parameters according to the instructions of the ISP:

Table 14-4: SNMP Parameters Description

Parameter	Description
Allow Incoming WAN Access to SNMP	Select this check box to allow access to MP-20x's SNMP over the Internet.
Read-Only/Write Community Names	SNMP community strings are passwords used in SNMP messages between the management system and MP-20x. A read-only community allows the manager to monitor MP-20x. A read-write community allows the manager to both monitor and configure MP-20x.
Trusted Peer	The IP address, or subnet of addresses, that identify which remote management stations are allowed to perform SNMP operations on MP-20x.
SNMP Traps	Messages sent by MP-20x to a remote management station, to notify the manager about the occurrence of important events or serious conditions. MP-20x supports both SNMP version 1 and SNMP version 2c traps. Select the 'Enabled' check box to enable traps, and then enter the following: ▪ **Version:** SNMP version - SNMP v1 or SNMP v2c. ▪ **Destination:** the remote management station's IP address. ▪ **Community:** the community name that is associated with the trap messages.

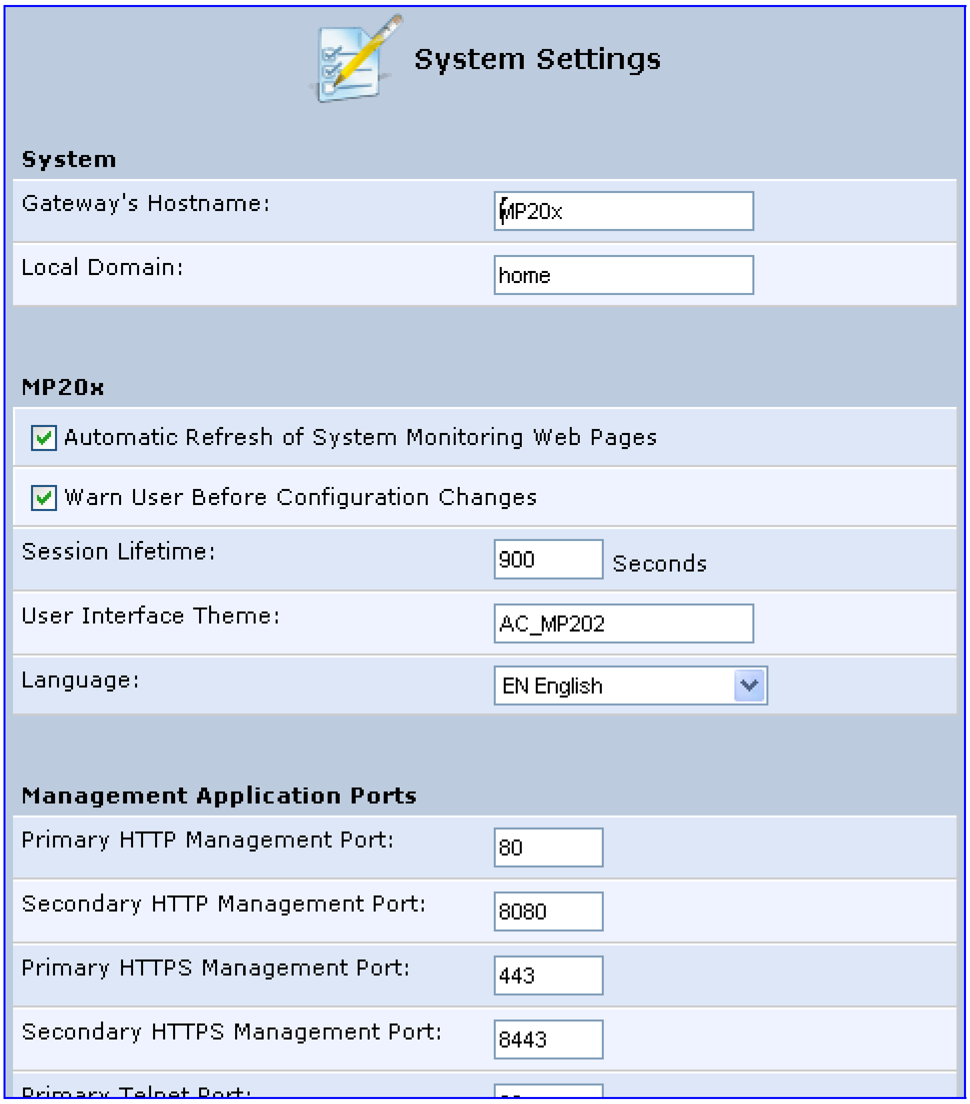
14.20 System Settings

The screen 'System Settings' allows you to configure various system and management parameters.

➢ To configure MP-20x's system, settings:

1. In the 'Advanced' screen, click the **System Settings** icon; the 'System Settings' screen appears.

Figure 14-52: System Settings Screen



System Settings

System

Gateway's Hostname:	MP20x
Local Domain:	home

MP20x

☑ Automatic Refresh of System Monitoring Web Pages

☑ Warn User Before Configuration Changes

Session Lifetime:	900 Seconds
User Interface Theme:	AC_MP202
Language:	EN English

Management Application Ports

Primary HTTP Management Port:	80
Secondary HTTP Management Port:	8080
Primary HTTPS Management Port:	443
Secondary HTTPS Management Port:	8443

2. Under the 'System Settings' section, configure the following:

   - In the 'Gateway's Hostname' field, enter the Telephone Adapter's host name. The host name is the Telephone Adapter's URL address.
   - In the 'Local Domain' field, enter your network's local domain.

3. Under the 'MP20x' section, configure the following:
   - **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 Configuration Changes:** select this check box to activate user warnings before network configuration changes take effect.
   - **Session Lifetime:** duration of idle time (in seconds) in which the Web session remains active. When this duration times out, the user must re-login.
   - **User Interface Theme:** select an alternative GUI theme from the list provided.
   - **Language:** select a different language for the Web interface.
4. Under the 'Management Application Ports' section, configure the following:
   - Primary/secondary HTTP management ports
   - Primary/secondary management HTTPS ports
   - Primary/secondary Telnet ports
   - Secure Telnet over SSL ports
5. Under the 'System Logging' section, configure the following:
   - **System Log Buffer Size:** size of the system log buffer in kilobytes.
   - **Remote System Notify Level:** MP-20x sends notifications to a remote host: None, Error, Warning, Information
   - **Persistent System Log:** select this check box to save the system log to the Flash - MP-20x's permanent memory. This prevents the system log from being erased when MP-20x reboots.
6. Under the 'Security Logging' section, configure the following:
   - **Security Log Buffer Size:** size of the security log buffer in Kilobytes
   - **Remote System Notify Level:** None, Error, Warning, Information
   - **Persistent Security Log:** select this check box to save the security log to the Flash. This prevents the security log from being erased when MP-20x reboots. Note: Do not leave the persistent logging feature enabled permanently, as continuous writing of the log files to the Flash reduces MP-20x's performance.
7. Under the 'HTTP Interception' section, configure the following:
   - **Intercept HTTP Traffic for Assisting with Internet Connectivity Problems:** If the WAN device is physically disconnected or cannot obtain an up and running status (even if an Internet connection exists), MP-20x displays an attention screen providing troubleshooting options (these options are displayed with distributions containing the "Support Cost Reduction (SCR)" feature; otherwise an explanation of the connection's status is provided). This screen is displayed instead of the browser's standard 'The page cannot be displayed' page. Note: Selecting the "Don't Show Me This Page Again" option in the attention screen disables this feature.
   - **Perform Web Authentication Over HTTPS:** Select this check box to secure MP-20x's interception page, in order to protect the required login details. Web authentication is performed through an HTTPS Web page.

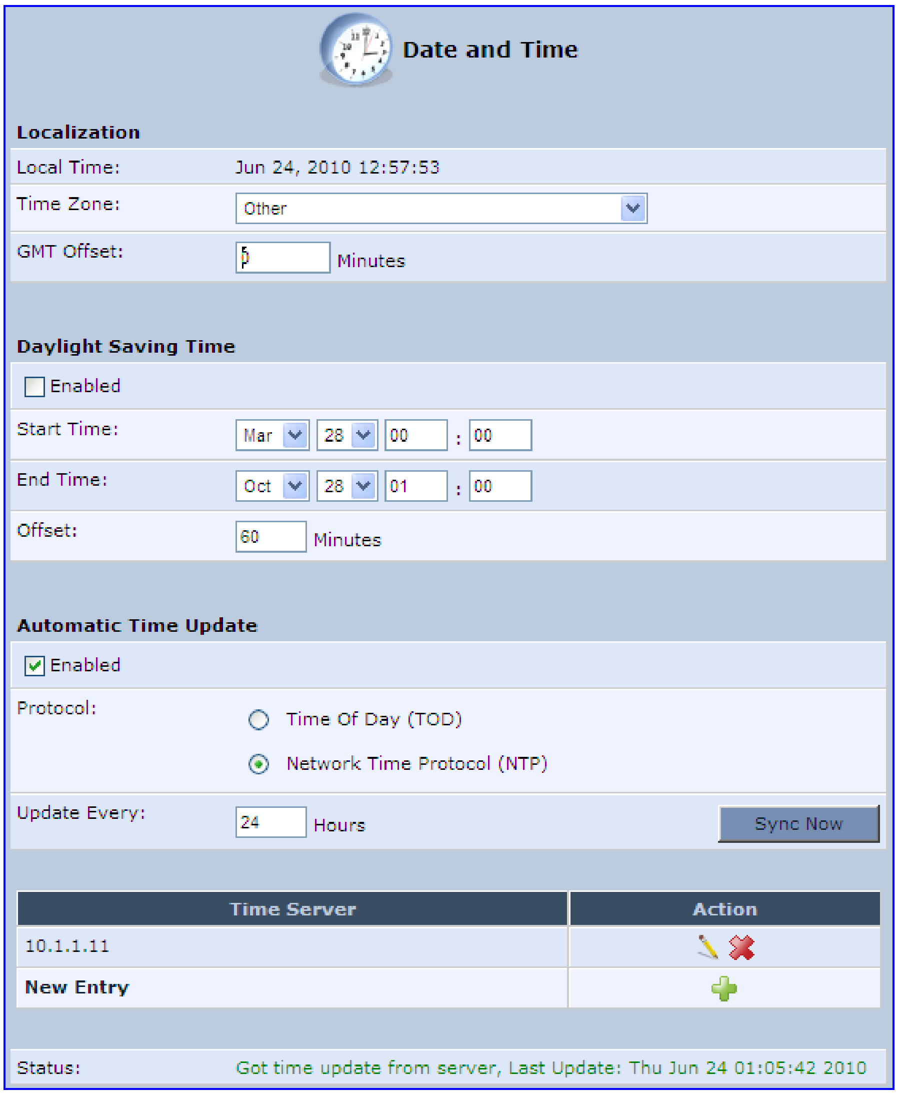
8. Under the 'Host Information' section, configure the following:
   - **Enable Auto Detection of Host Services:** If selected, it enables MP-20x to auto-detect its LAN hosts' properties, available services, traffic statistics, and connections.
9. Under the 'Installation Wizard' section, configure the following:
   - **Use Installation Wizard Pre-configured Values:** select this check box to have the wizard skip the steps for which parameters had been preconfigured and saved in the factory settings file (rg_factory).

14.21 Date & Time

➢ To configure date, time and daylight savings time settings:

1. In the 'Advanced' screen, click the **Time Settings** icon; the 'Date & Time' settings screen is displayed.

Figure 14-53: Date and Time Screen



Date and Time

Localization

Local Time:	Jun 24, 2010 12:57:53
Time Zone:	Other
GMT Offset:	5 Minutes

Daylight Saving Time

☐ Enabled	
Start Time:	Mar 28 00 : 00
End Time:	Oct 28 01 : 00
Offset:	60 Minutes

Automatic Time Update

☑ Enabled	
Protocol:	○ Time Of Day (TOD)
	● Network Time Protocol (NTP)
Update Every:	24 Hours [Sync Now]

Time Server	Action
10.1.1.11	✎ ✖
New Entry	✚

Status: Got time update from server, Last Update: Thu Jun 24 01:05:42 2010

2. From the 'Time Zone' drop-down list, select the local time zone. MP-20x can automatically detect daylight saving setting for selected time zones.
3. In the ‘GMT Offset’ field, enter the GMT offset time.
4. Under the 'Daylight Saving Time', configure the daylight saving settings for your time zone (if they are not automatically detected):
   - **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.
   - **Offset:** Daylight saving time offset.
5. For the Telephone Adapter to perform an automatic time update, under the 'Automatic Time Update' section, perform the following:
   a. Select the 'Enabled' check box.
   b. Select the protocol to be used for time update, by selecting either the 'Time of Day' or 'Network Time Protocol' option.
   c. In the 'Update Every' field, specify how often to perform the update.
   d. You can define Time server addresses, by clicking the **New Entry** link.

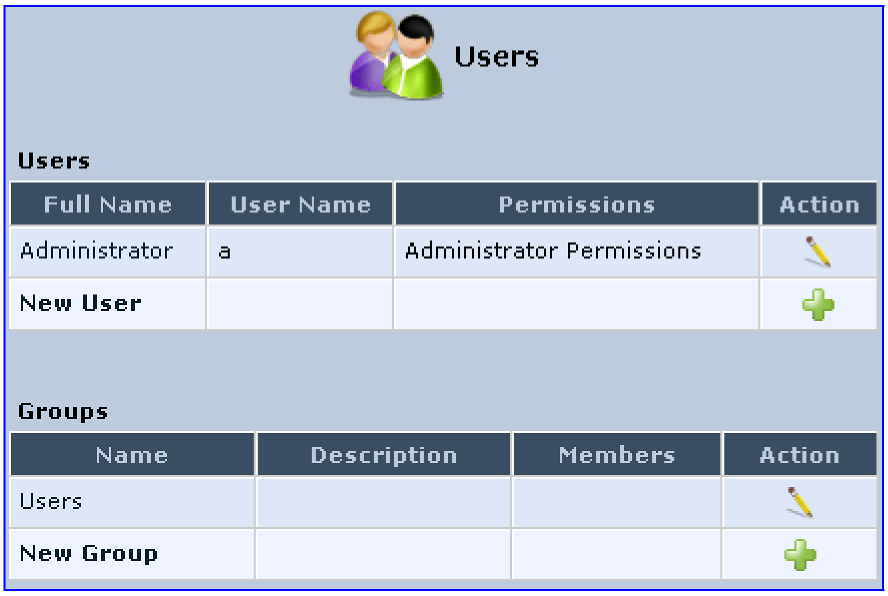
14.22 Configuring Users

The 'Users' screen lists the currently defined users and provides a link to add new users. You may also group users according to your preferences. The "Administrator" is a default user provided by the system. Administrator Permissions grants permissions to remotely modify the system settings via the Web-based management or Telnet.

➢ To configure users:

1. In the 'Advanced' screen, click the **Users** icon; the 'Users' screen appears.

Figure 14-54: Users Screen



Users

Users

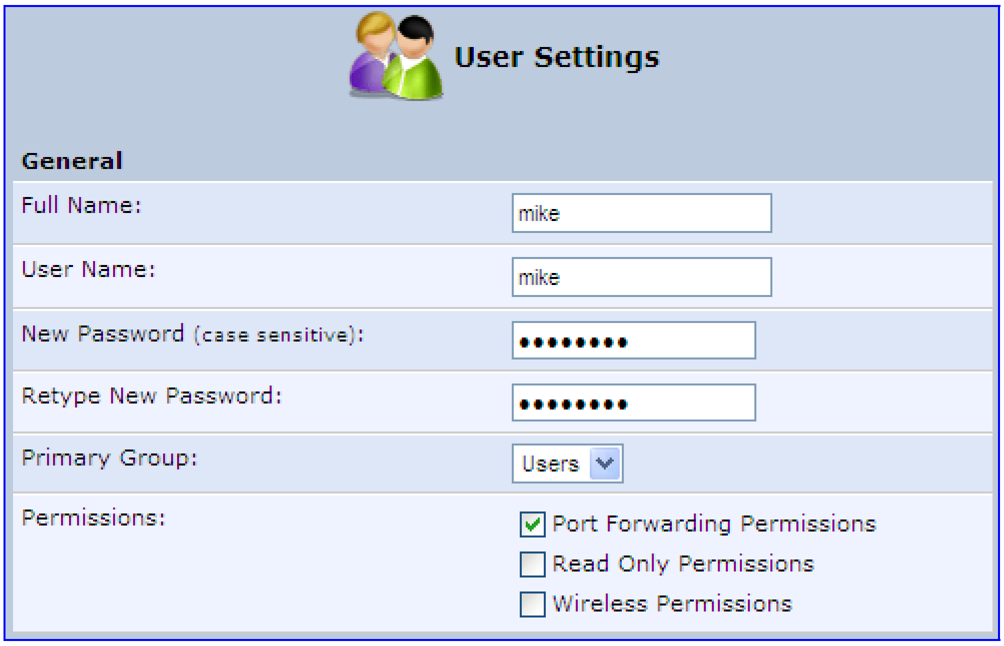
Full Name	User Name	Permissions	Action
Administrator	a	Administrator Permissions	✎
New User			✚

Groups

Name	Description	Members	Action
Users			✎
New Group			✚

2. In the 'Users' table, click **New User;** the 'Users Settings' screen appears.

Figure 14-55: Users Settings Screen



User Settings

General

Full Name:	mike
User Name:	mike
New Password (case sensitive):	••••••••
Retype New Password:	••••••••
Primary Group:	Users
Permissions:	✓ Port Forwarding Permissions ☐ Read Only Permissions ☐ Wireless Permissions

3. Add a new user by configuring the following fields:
   a. **Full Name:** enter a remote user's full name.
   b. **User Name:** enter a name a remote user uses to access your home network.
   c. **New Password:** enter a new password for the remote user. If you do not want to change the remote user's password leave this field empty.
   d. **Retype New Password:** if a new password was assigned, enter it again to verify correctness.
   e. **Permissions:** select the user's privileges on your home network:
      - **Port Forwarding:** user with the name "user" can modify the Port Forwarding screen.
      - **Read Only Permissions:** user can only view the current configuration, but cannot modify.
      - **Wireless Permissions:** grants permission to connect to the Internet via MP-20x's wireless access point. This permission level does not provide you with access to MP-20x's Web interface, unless you have administrator rights. **Note:** This permission is applicable only if MP-20x's wireless access point is configured with the 'Web Authentication' security level.

Note: A user whose user name is "user" (Full Name and User Name) has special privileges. By default, this user can access only the Quick Setup screen and can change the Internet connection type (and Wireless for MP-202C). In addition, this user can be defined with Port Forwarding permissions for configuring port forwarding.

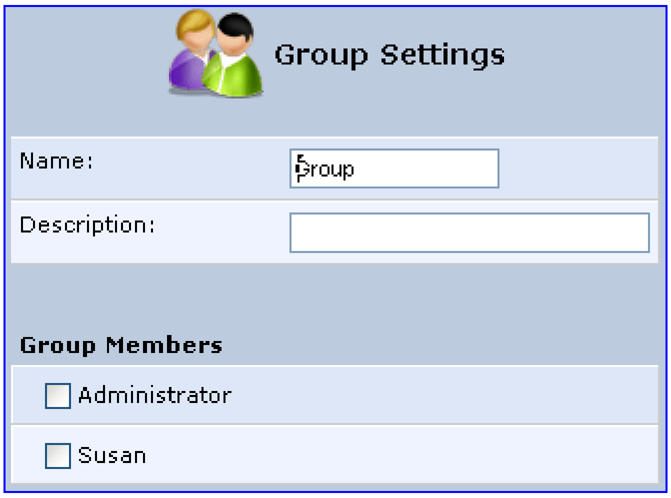
4. Click **OK**.

Note that changing any of the user parameters prompts the connection associated with the user to terminate. For changes to take effect you should activate the connection manually after modifying user parameters.

➢ **To configure user groups:**

1. In the 'Users' screen, under the 'Groups' section, click **New Group**; the 'Group Settings' screen appears.

Figure 14-56: Group Settings Screen



Group Settings

Name:	Group
Description:	

Group Members

☐ Administrator

☐ Susan

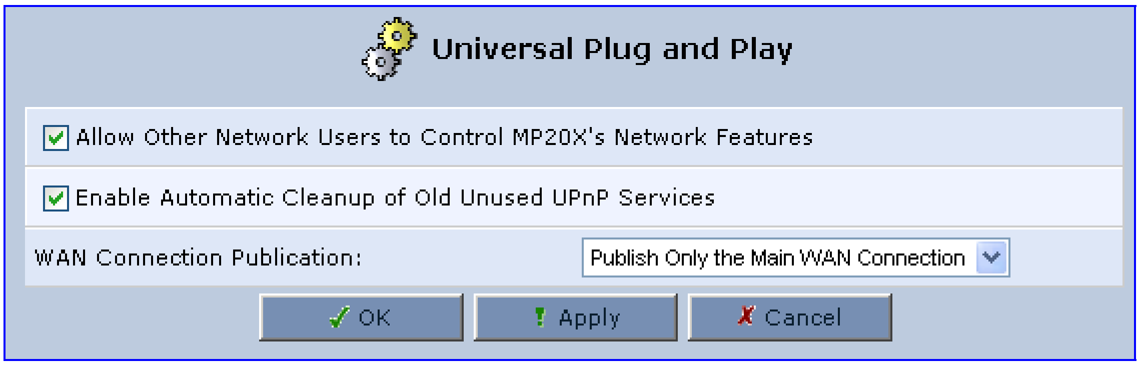
2. In the 'Name' field enter a name for the group.
3. In the 'Description' field, enter a brief description of this group.
4. In the 'Group Members' list, select the users that you want to assign to this group.
5. Click **OK**.

14.23 Universal Plug and Play

➢ **To configure UPnP:**

- In the 'Advanced' screen, click the **Universal Plug and Play** icon; the 'Universal Plug and Play' screen appears.

Figure 14-57: Advanced - Universal Plug n Play


Universal Plug and Play

✓ Allow Other Network Users to Control MP20X'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 MP-20x 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.

15 System Monitoring

The **System Monitoring** menu 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

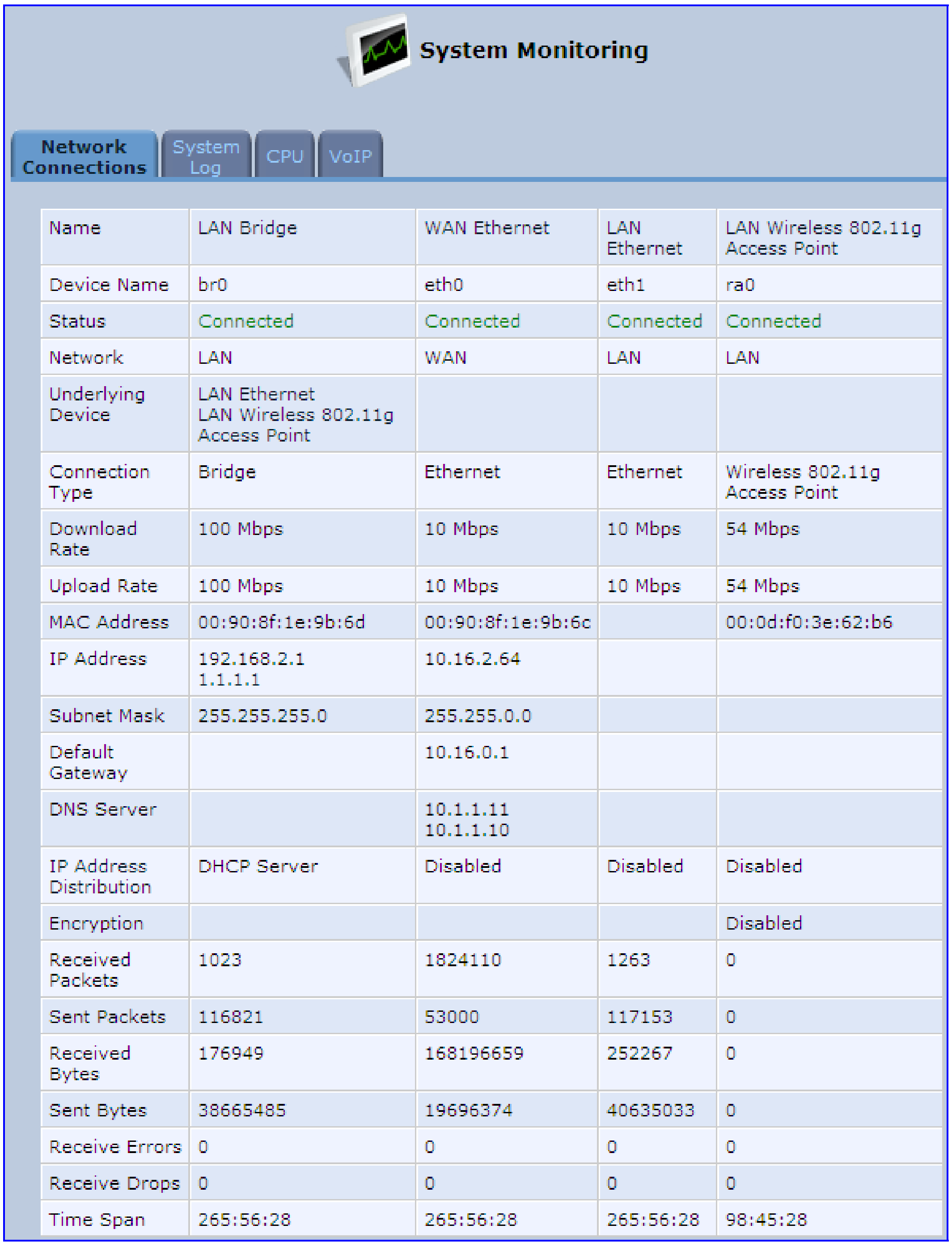
15.1 Network Connections

MP-20x constantly monitors 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 monitor connections:

1. From the left sidebar, click the menu **System Monitoring**; the 'System Monitoring' screen appears, displaying the screen of the tab **Connections**. This tab screen shows a read-only summary (with the exception of linked parameter 'IP Address Distribution') of the monitored connection data.

Figure 15-1: System Monitoring - Connections



Name	LAN Bridge	WAN Ethernet	LAN Ethernet	LAN Wireless 802.11g Access Point
Device Name	br0	eth0	eth1	ra0
Status	Connected	Connected	Connected	Connected
Network	LAN	WAN	LAN	LAN
Underlying Device	LAN Ethernet LAN Wireless 802.11g Access Point			
Connection Type	Bridge	Ethernet	Ethernet	Wireless 802.11g Access Point
Download Rate	100 Mbps	10 Mbps	10 Mbps	54 Mbps
Upload Rate	100 Mbps	10 Mbps	10 Mbps	54 Mbps
MAC Address	00:90:8f:1e:9b:6d	00:90:8f:1e:9b:6c		00:0d:f0:3e:62:b6
IP Address	192.168.2.1 1.1.1.1	10.16.2.64		
Subnet Mask	255.255.255.0	255.255.0.0		
Default Gateway		10.16.0.1		
DNS Server		10.1.1.11 10.1.1.10		
IP Address Distribution	DHCP Server	Disabled	Disabled	Disabled
Encryption				Disabled
Received Packets	1023	1824110	1263	0
Sent Packets	116821	53000	117153	0
Received Bytes	176949	168196659	252267	0
Sent Bytes	38665485	19696374	40635033	0
Receive Errors	0	0	0	0
Receive Drops	0	0	0	0
Time Span	265:56:28	265:56:28	265:56:28	98:45:28

2. Click the **Refresh** button to update the display, or click the **Automatic Refresh On** button to constantly update the displayed parameters.

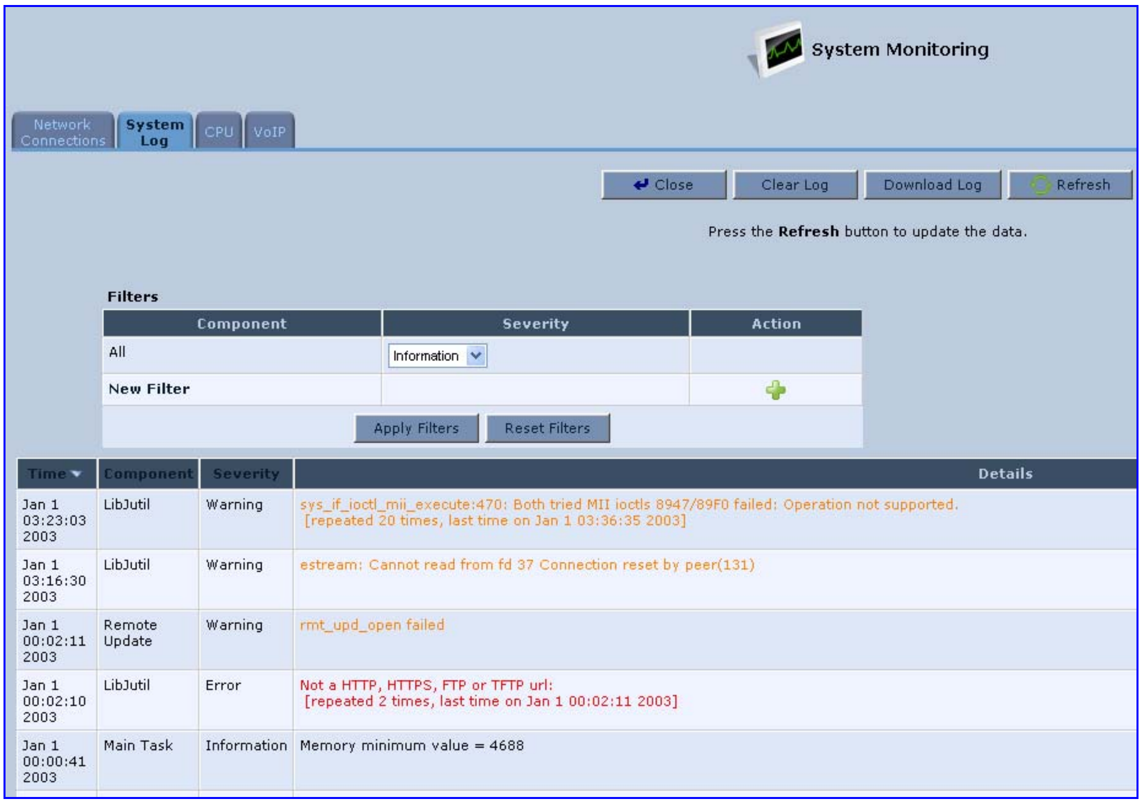
15.2 System Log

The System Log displays a list of the most recent activity that has taken place on MP-20x.

➢ **To open the system log:**

- In the 'System Monitoring' screen, click the **System Log** tab 'the 'System Monitoring - System Log' screen opens.

Figure 15-2: System Monitoring - System Log



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

Filters

Component	Severity	Action
All	Information	
New Filter		✚

Apply Filters Reset Filters

Time	Component	Severity	Details
Jan 1 03:23:03 2003	LibJutil	Warning	sys_if_ioctl_mii_execute:470: Both tried MII ioctls 8947/89F0 failed: Operation not supported. [repeated 20 times, last time on Jan 1 03:36:35 2003]
Jan 1 03:16:30 2003	LibJutil	Warning	estream: Cannot read from fd 37 Connection reset by peer(131)
Jan 1 00:02:11 2003	Remote Update	Warning	rmt_upd_open failed
Jan 1 00:02:10 2003	LibJutil	Error	Not a HTTP, HTTPS, FTP or TFTP url: [repeated 2 times, last time on Jan 1 00:02:11 2003]
Jan 1 00:00:41 2003	Main Task	Information	Memory minimum value = 4688

15.3 CPU

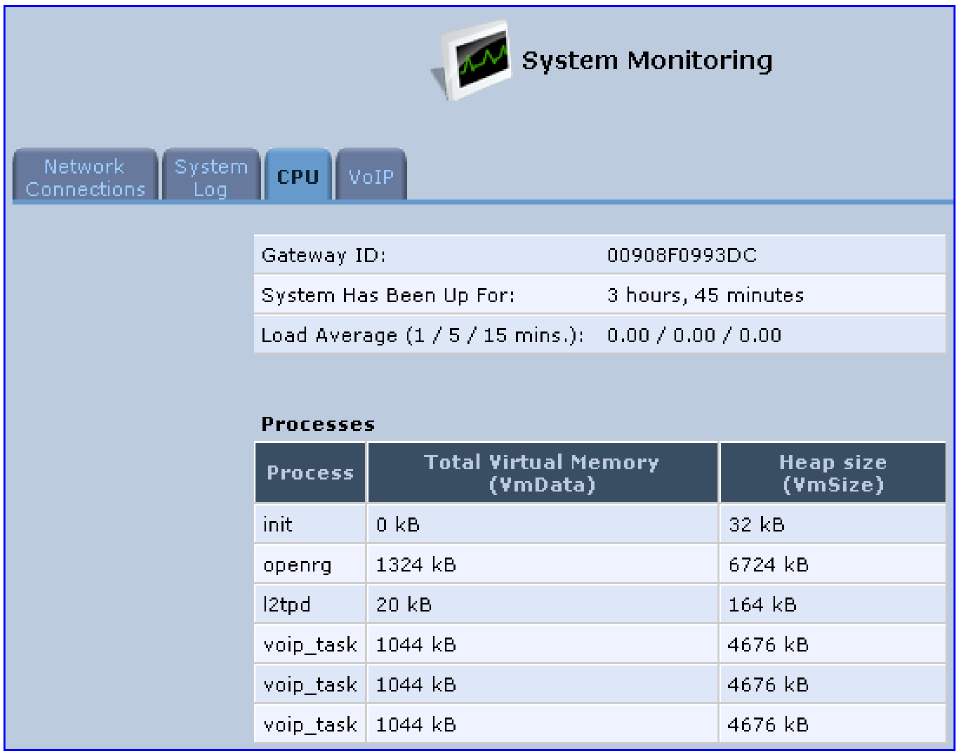
The 'CPU' screen displays the following system parameters:

- **System Has Been Up For:** amount of time that has passed since MP-20x was last started.
- **Load Average (1 / 5 / 15 mins.):** average number of processes that are either in a runnable or uninterruptible state. A process in the runnable state is either using the CPU or waiting to use the CPU. A process in the uninterruptible state is waiting for I/O access, e.g. waiting for the disk. The averages are taken over the three time intervals. The meaning of the load average value varies according to the number of CPUs in the system. This means for example, that a load average of 1 on a single-CPU system means that the CPU was loaded all the time, while on a 4-CPU system this means that the CPU was idle 75% of the time.
- **Processes:** processes currently running on MP-20x and their virtual memory usage. The amount of memory granted for each process is presented with the help of the following parameters:
  - **Total Virtual Memory (VmData):** amount of memory currently utilized by the running process.
  - **Heap size (VmSize):** total amount of memory allocated for the running process.

➢ To view the CPU statistics:

- In the 'System Monitoring' screen, click the **CPU** tab; the 'CPU' screen opens.

Figure 15-3: CPU Screen



Gateway ID:	00908F0993DC
System Has Been Up For:	3 hours, 45 minutes
Load Average (1 / 5 / 15 mins.):	0.00 / 0.00 / 0.00

Processes

Process	Total Virtual Memory (VmData)	Heap size (VmSize)
init	0 kB	32 kB
openrg	1324 kB	6724 kB
l2tpd	20 kB	164 kB
voip_task	1044 kB	4676 kB
voip_task	1044 kB	4676 kB
voip_task	1044 kB	4676 kB

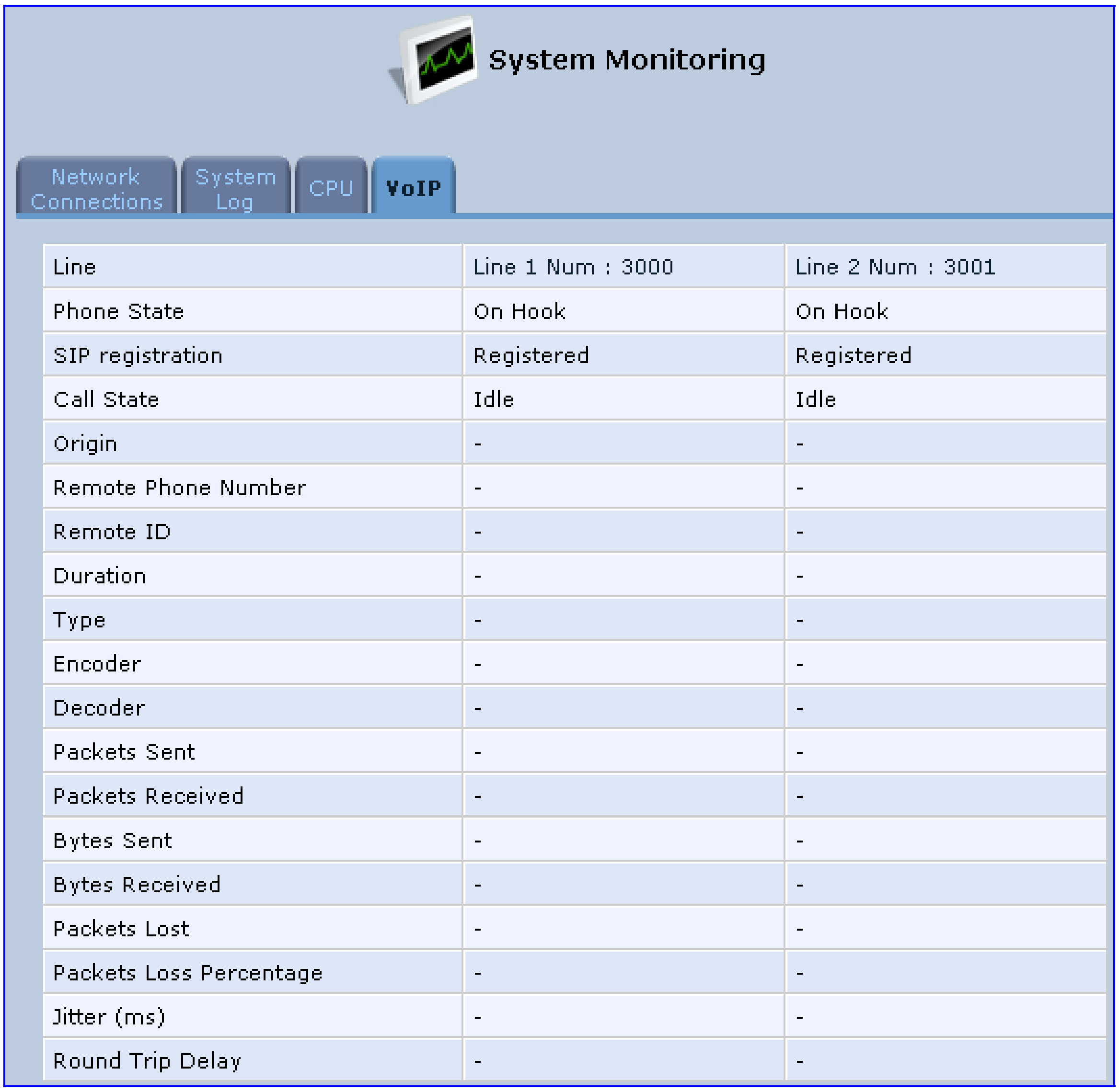
The screen is automatically refreshed by default, though you may change this by clicking **Automatic Refresh Off**.

15.4 Voice over IP

➢ To monitor VoIP:

- In the 'System Monitoring' screen, click the **VoIP** tab; the 'VoIP' screen opens showing read-only VoIP call related parameters.

Figure 15-4: Advanced - System Monitoring - VoIP



Line	Line 1 Num : 3000	Line 2 Num : 3001
Phone State	On Hook	On Hook
SIP registration	Registered	Registered
Call State	Idle	Idle
Origin	-	-
Remote Phone Number	-	-
Remote ID	-	-
Duration	-	-
Type	-	-
Encoder	-	-
Decoder	-	-
Packets Sent	-	-
Packets Received	-	-
Bytes Sent	-	-
Bytes Received	-	-
Packets Lost	-	-
Packets Loss Percentage	-	-
Jitter (ms)	-	-
Round Trip Delay	-	-

Note: The number of lines depends on the MP-20x model (one line for MP-201, two lines for MP-202, and four lines for MP-204).

Reader’s Notes

16 Syntax for Digit Maps and Dial Plans

Digit maps and dial plans are defined using special syntax rules, configured in the 'Dialing' screen (refer to 'Configuring Dialing Parameters' on page 43).

- **Digit Maps:** A phone's digit map allows MP-20x to know when an entered telephone number is complete and therefore, when it should initiate the call. If the phone digit map is defined incorrectly, MP-20x might start to dial before the telephone user has entered all the required digits. A digit map is defined either by a (case insensitive) "string" or by a list of strings. Each string in the list is an alternative numbering scheme, specified either as a set of digits or as an expression over which MP-20x attempts to find a shortest possible match. The syntax that can be used in each numbering scheme is described in the table below.
- **Dial Plans:** A dial plan translates specific patterns into specific SIP destination addresses. For example, dial plan rule "4xxx=Line_\\\@10.1.2.3" sends a dialed number consisting of the digit 4 followed by any three digits to IP address 10.1.2.3. The syntax of the pattern on the left of the '=' sign is described in the table below.

Table 16-1: Dial Plan (for Left of '=' Sign) and Digit Map Syntax

Type	Syntax
Digit	A digit from "0" to "9".
DTMF	A digit, or one of the symbols "A", "B", "C", "D", "#", or "*". Extensions may be defined.
Wildcard	The symbol "x" which denotes any digit ("0" to "9").
Range	One or more DTMF symbols enclosed between square brackets ("[" and "]").
Subrange	Two digits separated by a hyphen ("-") which matches any digit between and including the two. The subrange can only be used inside a range construct, i.e., between "[" and "]".
Position	A period (".") which matches an arbitrary number, including zero, of occurrences of the preceding construct.

For example:

[2-9]11|0|100|101|011xxx.|9011xxx.|1[2-9]xxxxxxxxx|91[2-9]xxxxxxxxx|9[2-9]xxxxxx|*xx|[8]xxxx|[2-7]xxx

- **[2-9]11:** 911 rule: 211, 311, 411, 511, 611, 711, 811, 911 are dialled immediately
- **0:** Local operator rule
- **100:** Auto-attendant default extension
- **101:** Voicemail default extension
- **011xxx.:** International rule without prefix
- **9011xxx.:** International rule with prefix
- **1[2-9]xxxxxxxxx:** LD rule without prefix
- **91[2-9]xxxxxxxxx:** LD rule with prefix
- **9[2-9]xxxxxx:** Local call with prefix

- ***xx:** 2-digit star codes
- **[1-7]xx:** A regular 3-digit extension that does not start with 9 or 8 is dialed immediately
- **[2-7]xx:** A regular 3-digit extension that does not start with 9, 8, or 1 is dialed immediately
- **[2-7]xxx:** A regular 4-digit extension that does not start with 9, 8, or 1 is dialed immediately
- **[8]xxx:** A 3-digit extension prefixed with an 8 (routes calls directly to voicemail of extension xxx)
- **[8]xxxx:** A-4 digit extension prefixed with an 8 (routes calls directly to voicemail of extension xxxx)

17 Software and Hardware Specifications

Note: For the list of features available in the current software version, refer to the latest Release Notes.

Table 17-1: MP-20x 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[2], traffic shaping ▪ STUN (RFC 3489)
Media Processing	▪ Voice Coders: G.711, G.723.1, G.729A/B, G.726[3] ▪ 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 ▪ Message Waiting Indication ▪ Call Forward ▪ 3-Way Conferencing[4]
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, TFTP, FTP, and HTTPS

[2] Not supported by MP-202C (please contact AudioCodes).

[3] MP-20x Rev B models only.

[4] MP-202C does not support two concurrent three-way conference calls.

Feature	Details
	▪ Configuration file encryption (3DES) ▪ SIP-triggered remote firmware and configuration upgrade ▪ Command-Line Interface (CLI) over Telnet ▪ Dual image management ▪ SNMP[5]
Packetization	▪ RTP/RTCP Packetization (RFC 3550, RFC 3551) ▪ DTMF Relay (RFC 2833)
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 Signaling ✓ On/Off Hook, Flash Hook
Wireless LAN[6]	▪ Wireless LAN - 802.11b/g Wireless Access Point ▪ Wireless Security: ✓ RADIUS Server (802.1x/WPA Client Authentication) ✓ WPA ✓ WPA2 ✓ WPA/WEP Mixed Mode ✓ TKIP Encryption ✓ MAC Filtering ▪ Operating frequency: 2.4 - 2.5 GHz ▪ Nominal data transfer rate: - 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps - 802.11b: 1, 2, 5.5, 11 Mbps ✓ Operating channels: - 11 for North America - 14 for Japan - 13 for Europe (ETSI)
Hardware	
Power	+12 VDC, 1A External Power Supply Adaptor, 110/220 VAC/50-60 Hz, available in the following models: ▪ **MP202A-PS-NR-EU/RPSD10007:** Power Supply 12VDC/1A Wall Mount EU Type 220VAC; DC Plug 5.5 x 2.5 x 8 mm Straight; 1.5 m cable with Ferrite bead ▪ **MP202A-PS-NR-US/RPSD10008:** Power Supply 12VDC/1A Wall Mount US Type 110VAC; DC Plug 5.5 x 2.5 x 8 mm Straight; 1.5 m cable with Ferrite bead ▪ **MP202A-PS-WR-US/RPSD10012:** Power Supply 12VDC/1A Wall Mount US Type 100-240VAC; DC Plug 5.5 x 2.5 x 8 mm Straight;

[5] Not supported by MP-202C-A.

[6] MP-202C-W model only.

Feature	Details
	1.5m cable with Ferrite bead ▪ **MP20x-PS-WR-UK/RPSD10011:** Power Supply 12VDC/1A Wall Mount UK Type 100-240VAC; DC Plug 5.5 x 2.5 x 8 mm Straight; 1.5m cable with Ferrite bead ▪ **MP202A-PS-WR-ARG/RPSD10014:** Power Supply 12VDC/1A Wall Mount ARG Type 100-240VAC; DC Plug 5.5 x 2.5 x 8 mm Straight; 1.5 m cable with Ferrite bead; Argentina ▪ **MP202A-PS-WR-ARG-2m/RPSD10016:** Power Supply 12VDC/1A Wall Mount ARG Type 100-240VAC; DC Plug 5.5 x 2.5 x 8 mm Straight; 2 m cable with Ferrite bead; Argentina
Interfaces	▪ WAN 10/100Base-T (RJ-45) ▪ LAN 10/100Base-T (RJ-45) ▪ RJ-11 FXS ports for telephones (POTS) ▪ Network Interface WAN/LAN 10/100 Base-T(RJ-45), 1 (MP-202C-A) or 4 (MP-202C-R/W) LAN 10/100 Base-T (RJ-45) ▪ Two antenna connectors - 802.11b/g WiFi antenna (MP-202C-W)
LED Indications	▪ LAN activity on Ethernet Port ▪ WAN ▪ Power on ▪ FXS Phone lines (1 to 4, depending on MP-20x model) - Registered, In Use, Alert ▪ WiFi enabled (Only MP-202C-W model)
SLIC characteristics	▪ Maximum Ringer Load (REN) = 5 ▪ Short Haul ▪ Ringer Voltage - up to 65Vrms ▪ Configurable Terminating Impedance
Environmental	▪ **Operating Temperature:** 0 to 40°C ▪ **Storage Temperature:** -25 to 70°C ▪ **Operating Humidity:** 10 to 90% non-condensing ▪ **Storage Humidity:** 10 to 90% non-condensing
Weight and Dimensions	▪ MP-202C-A: 223 g; 167.2 x 134 x 33.3 mm ▪ MP-202C-R: 249 g; 167.2 x 134 x 33.3 mm ▪ MP-202C-W: 263 g; 167.2 x 153 x 33.3 mm ▪ MP-202B: 257 g; 167 x 133 x 33 mm

AudioCodes CPE & Access Gateway Products

MP-20x series

MediaPack™ Series Telephone Adapters with Integrated Router

User's Manual

MP-20x Telephone Adapter

Version 3.0.1

AudioCodes

www.audiocodes.com