P-79X Series

G.SHDSL.bis Broadband Gateway

Version 1.00
Edition 1, 03/2016

User's Guide

Default Login Details	
IP Address	http://192.168.1.1
User Name	admin, user
Password	1234, user

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the P-79X and access the Web Configurator wizards. It contains information on setting up your network and configuring for Internet access.

- More Information

  Go to **support.zyxel.com** to find other information on the P-79X.

Contents Overview

Table of Contents

PART I
User's Guide

1

Getting To Know Your P-79X

This chapter introduces the main features and applications of your P-79X.

1.1 Overview

P-793H v3

The P-793H v3 is a secure G.SHDSL.bis bonded broadway gateway that provides high-speed LAN-to-LAN connection and Internet access over the your telephone. It supports symmetrical multi-rate data transmission speed that adjusts the data rate automatically according to the quality of the wire connection.

You can set up your P-793H v3 for high-speed Internet access or for high-speed point-to-point or point-to-2 points connections with other SHDSL models. The P-793H v3 can be used for either IP routing or bridging depending on your network configuration. As a router, the P-793H v3 provides features such as firewall, content filtering and bandwidth management. As a bridge, the P-793H v3 minimizes the configuration changes you have to make in your existing network.

P-792H v3

The P-792H v3 is a secure G.SHDSL.bis broadband gateway that provides high-speed LAN-to-LAN connection and Internet access over the your telephone. It supports symmetrical multi-rate data transmission speed that adjusts the data rate automatically according to the quality of the wire connection.

You can set up your P-792H v3 for high-speed Internet access or for high-speed point-to-point connections with another SHDSL model. The P-792H v3 can be used for either IP routing or bridging depending on your network configuration. As a router, the P-792H v3 provides features such as firewall, content filtering and bandwidth management. As a bridge, the P-792H v3 minimizes the configuration changes you have to make in your existing network.

P-791R v3

The P-791R v3 is a G.SHDSL.bis router providing high-speed LAN-to-LAN connection and Internet access through G.SHDSL.bis connection over the telephone line. You can use your P-791R v3 for either IP routing or bridging depending on your ISP (Internet Service Provider) configuration.This User's Guide covers the following models: P-793H v3, P-792H v3, and P-791R v3.

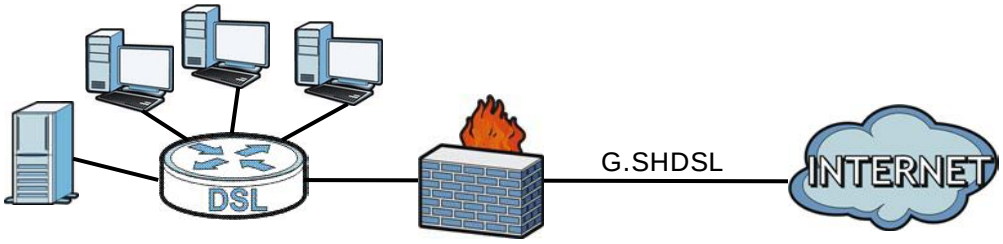
Table 1 P-79X Comparison Table

DETAILS	P-793H v3	P-792H v3	P-791R v3
G.SHDSL Interface	4-wire (Two Pairs Bonding)	2-wire (Single Pair)	2-wire (Single Pair)
10/100 Mbps Ethernet Ports	4	4	1

1.1.1 High-speed Internet Access with G.SHDSL

The P-79X provides high-speed G.SHDSL Internet access. The G.SHDSL (Single-pair High-speed Digital Subscriber Line) is a symmetrical, bi-directional DSL service that uses your telephone line to provide data rates up to 2.3 Mbits/sec. (The “G.” in “G.SHDSL” is defined by the G.991.2 ITU (International Telecommunication Union) state-of-the-art industry standard). Unlike ADSL or VDSL, G.SHDSL.bis supports the same high speed for transmission and receiving.

Figure 1 High-speed Internet Access with Your P-79X

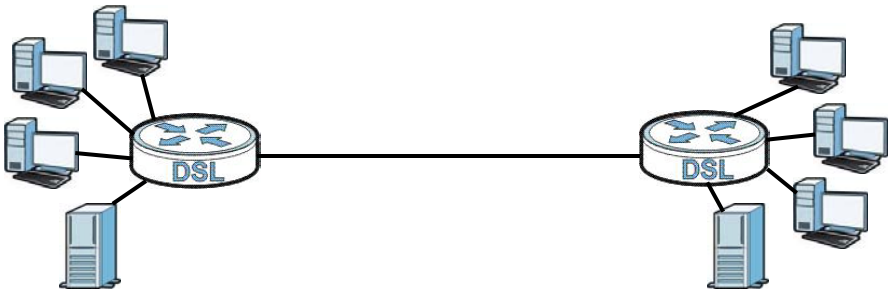


For Internet access, connect the DSL port to the phone port. Then, connect your computers or servers to the LAN ports for shared Internet access. (See the Quick Start Guide for detailed instructions about hardware connections.) Next, set up the P-79X as a router or as a bridge, depending on the desired configuration.

1.1.2 High-speed Point-to-point Connections

You can use another P-79X or any SHDSL device with the P-79X to create a cost-effective, high-speed connection for high-bandwidth applications such as videoconferencing and distance learning.

Figure 2 Point-to-point Connections with Your P-79X

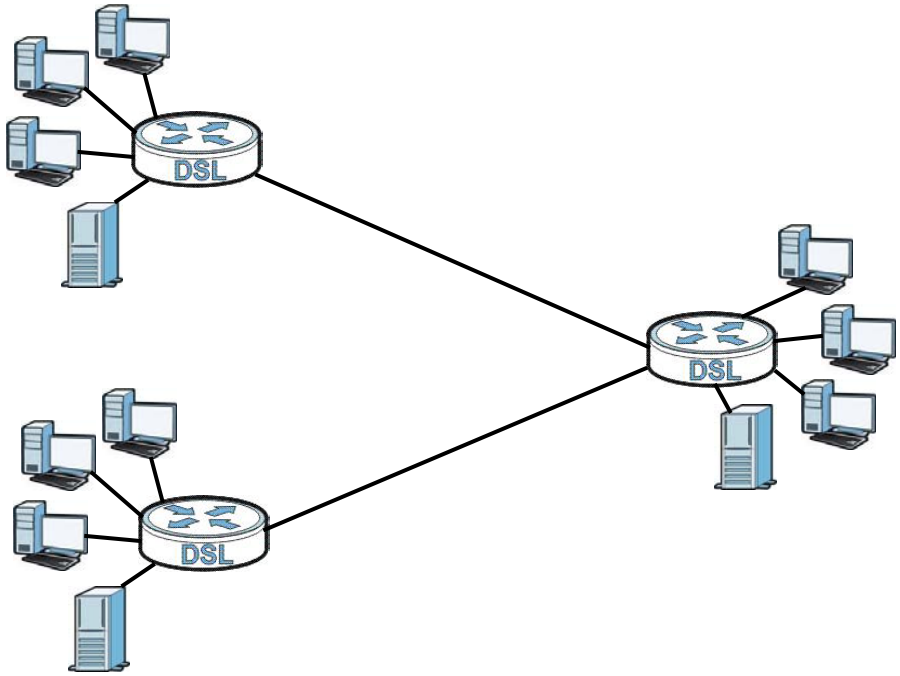


The P-79Xs provide a simple, fast point-to-point connection between two geographically-dispersed networks.

1.1.3 High-speed Point-to-2points Connections

Use three P-79Xs or 2 SHDSL devices with the P-79X to connect two remote networks to a central location. For example, connect the headquarters to two branch offices. In this scenario the central P-79X acts in a similar way as an Internet service provider.

Figure 3 Point-to-2points Connections with Your P-79X



Note: See Chapter 5 on page 38 for more information on setting up point-to-point and point-to-2points connections.

1.2 Ways to Manage the P-79X

Use any of the following methods to manage the P-79X.

- Web Configurator. This is recommended for everyday management of the P-79X using a (supported) web browser. See Chapter 2 on page 19.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers. See Appendix H on page 471.
- SMT. System Management Terminal is a text-based configuration menu that you can use to configure your device. See Chapter 25 on page 260.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore. See Chapter 17 on page 243.
- SNMP. The device can be monitored and/or managed by an SNMP manager. See Chapter 17 on page 243.
- TR-069. This is a standard that defines how your P-79X can be managed by a management server. See Chapter 17 on page 243.

1.3 Good Habits for Managing the P-79X

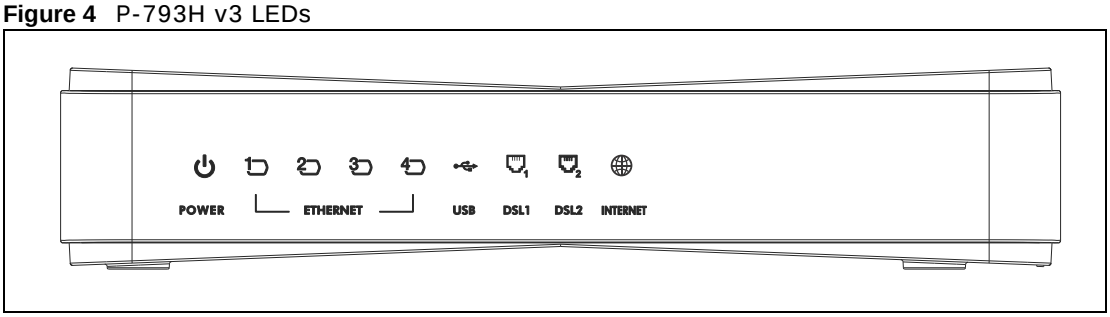
Do the following things regularly to make the P-79X more secure and to manage the P-79X more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the P-79X to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the P-79X. You could simply restore your last configuration.

1.4 LEDs

The following figure shows the LEDs.

Figure 4 P-793H v3 LEDs



The following table describes the LEDs.

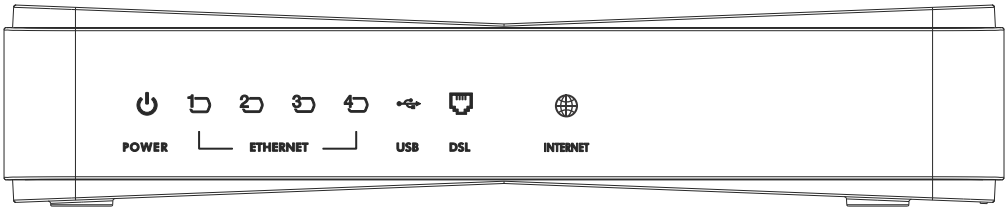
Table 2 P-793H v3 LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The P-793H v3 is receiving power and functioning properly.
		Blinking	The P-793H v3 is rebooting or performing diagnostics.
	Red	On	Power to the P-793H v3 is too low.
		Off	The system is not ready or has malfunctioned.
ETHERNET 1~4	Green	On	This port has a successful Ethernet connection.
		Blinking	This port is sending/receiving data.
		Off	This port is not connected.
USB	Green	On	The P-793H v3 recognizes a USB connection through the USB slot.
		Blinking	The P-793H v3 is sending/receiving data to /from the USB device connected to it.
		Off	The P-793H v3 does not detect a USB connection through the USB slot.
DSL1/DSL2	Green	On	The DSL line is up.
		Blinking	The P-793H v3 is initializing the DSL line.
		Off	The DSL line is down.
Note: For Internet access setup or point-to-point connections, the DSL1 and DSL2 LEDs indicate the status of a single connection (act as one LED). For point-to-2point connections, the DSL1 and DSL2 LEDs indicate the status of connection 1 and connection 2 respectively.			

Table 2 P-793H v3 LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
INTERNET	Green	On	The Internet connection is up, and the P-793H v3 has an IP address. (If the P-793H v3 uses RFC 1483 in bridge mode, this light does not turn on, but it does blink when the P-793H v3 is sending/receiving data.)
		Blinking	The P-793H v3 is sending/receiving data.
	Red	On	The P-793H v3 tried to get an IP address, but an error occurred.
		Off	The Internet connection is down.

Figure 5 P-792H v3 LEDs

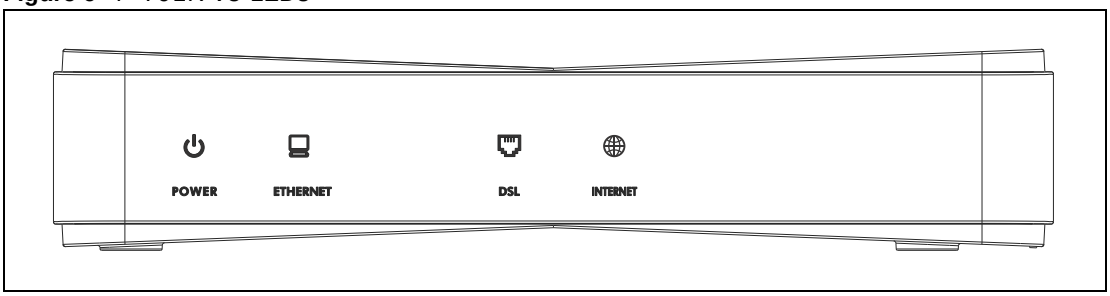


The following table describes the LEDs.

Table 3 P-792H v3 LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The P-792H v3 is receiving power and functioning properly.
		Blinking	The P-792H v3 is rebooting or performing diagnostics.
	Red	On	Power to the P-792H v3 is too low.
		Off	The system is not ready or has malfunctioned.
ETHERNET 1~4	Green	On	This port has a successful Ethernet connection.
		Blinking	This port is sending/receiving data.
		Off	This port is not connected.
USB	Green	On	The P-792H v3 recognizes a USB connection through the USB slot.
		Blinking	The P-792H v3 is sending/receiving data to /from the USB device connected to it.
		Off	The P-792H v3 does not detect a USB connection through the USB slot.
DSL	Green	On	The DSL line is up.
		Blinking	The P-792H v3 is initializing the DSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The Internet connection is up, and the P-792H v3 has an IP address. (If the P-792H v3 uses RFC 1483 in bridge mode, this light does not turn on, but it does blink when the P-792H v3 is sending/receiving data.)
		Blinking	The P-792H v3 is sending/receiving data.
	Red	On	The P-792H v3 tried to get an IP address, but an error occurred.
		Off	The Internet connection is down.

Figure 6 P-791R v3 LEDs



The following table describes the LEDs.

Table 4 P-791R v3 LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The P-791R v3 is receiving power and functioning properly.
		Blinking	The P-791R v3 is rebooting or performing diagnostics.
	Red	On	Power to the P-791R v3 is too low.
		Off	The system is not ready or has malfunctioned.
ETHERNET	Green	On	This port has a successful Ethernet connection.
		Blinking	This port is sending/receiving data.
		Off	This port is not connected.
DSL	Green	On	The DSL line is up.
		Blinking	The P-791R v3 is initializing the DSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The Internet connection is up, and the P-791R v3 has an IP address. (If the P-791R v3 uses RFC 1483 in bridge mode, this light does not turn on, but it does blink when the P-791R v3 is sending/receiving data.)
		Blinking	The P-791R v3 is sending/receiving data.
	Red	On	The P-791R v3 tried to get an IP address, but an error occurred.
		Off	The Internet connection is down.

1.5 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “1234”.

1.5.1 Using the RESET Button

1 Make sure the **POWER** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

2

Introducing the Web Configurator

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy P-79X setup and management via Internet browser. Use Internet Explorer 11.0 and later versions, Mozilla Firefox 43.04 and later versions, Google Chrome 32.0 and later versions, or Microsoft Edge 20.0 and later versions. The recommended screen resolution is 1024 by 768 pixels. In order to use the web configurator you need to allow:

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

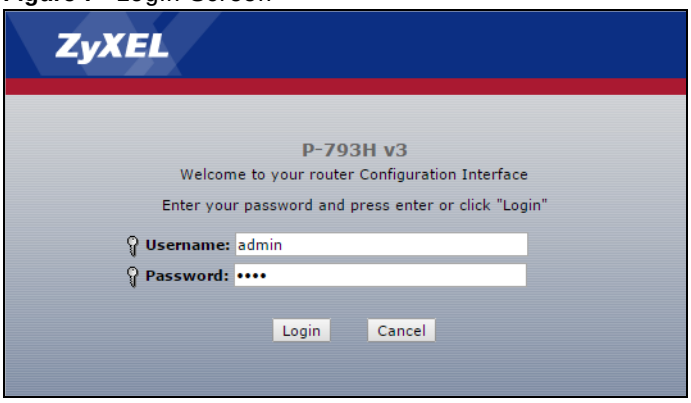
See the chapter on troubleshooting if you need to make sure these functions are allowed in Internet Explorer.

Note: This guide uses the P-793H v3 screens as an example. The screens may vary slightly for different models.

2.2 Accessing the Web Configurator

1. Make sure your P-79X hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.
4. A password screen displays. The P-79X has a dual login system. The default non-readable characters represents the user password (user by default). Clicking **Login without entering any password brings you to the system's status screen**. To access the administrative web configurator and manage the P-79X, type the admin password (1234 by default) in the password screen and click **Login**. Click **Cancel** to revert to the default user password in the password field. If you have changed the password, enter your password and click **Login**.

Figure 7 Login Screen



5 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

Figure 8 Change Password at Login

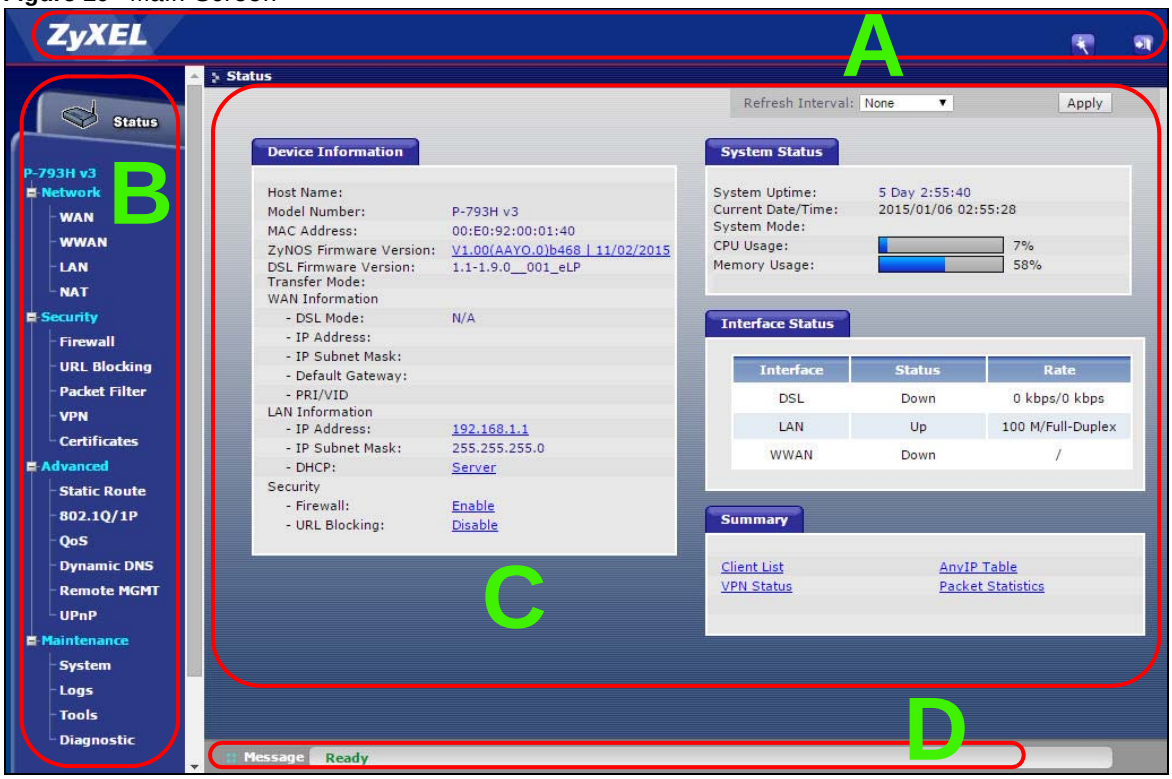
6 Select **Go to Wizard setup** and click **Apply** to display the wizard main screen. Otherwise, select **Go to Advanced setup** and click **Apply** to display the **Status** screen.

Figure 9 Select a Mode

Note: For security reasons, the P-79X automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

2.3 Web Configurator Main Screen

Figure 10 Main Screen



As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

2.3.1 Title Bar

The title bar provides some icons in the upper right corner.

The icons provide the following functions.

Table 5 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	**Wizards**: Click this icon to go to the configuration wizards. See Chapter 4 on page 31 for more information.
	**Logout**: Click this icon to log out of the web configurator.

2.3.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure P-79X features. The following tables describe each menu item.

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen shows the P-79X's general device and network status information. Use this screen to access the statistics and client list.
Network		
WAN	Internet Access Setup	Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and point-to-point or point-to-2point connections.
	More Connections	Use this screen to configure additional WAN connections.
	WAN Backup Setup	Use this screen to configure your traffic redirect properties and WAN backup settings.
WWAN	3G Wan Setup	Use this screen to configure 3G WAN connection.
LAN	IP	Use this screen to configure LAN TCP/IP settings and other advanced properties.
	DHCP Setup	Use this screen to configure LAN DHCP settings.
	Client List	Use this screen to view current DHCP client information and to always assign specific IP addresses to individual MAC addresses (and host names).
	IP Alias	Use this screen to partition your LAN interface into subnets.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world. This screen appears when you choose **SUA Only** from the **NAT** > **General** screen.

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
	Address Mapping	Use this screen to configure network address translation mapping rules. This screen appears when you choose **Full Feature** from the **NAT** > **General** screen.
	ALG	Use this screen to enable or disable SIP ALG.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall and the default action to take on network traffic going in specific directions.
	Rules	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Threshold	Use this screen to configure the thresholds for determining when to drop sessions that do not become fully established.
URL Blocking	Keyword	Use this screen to block access to web sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the P-79X to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering on your P-79X.
Packet Filter	Packet Filter	Use this screen to configure the rules for protocol and generic filter sets.
VPN	Setup	Use this screen to configure each VPN tunnel.
	Monitor	Use this screen to look at the current status of each VPN tunnel.
Certificates	Trusted CAs	Use this screen to import CA certificates to the P-79X.
Advanced		
Static Route	Static Route	Use this screen to configure IP static routes to tell your P-79X about networks beyond the directly connected remote nodes.
802.1Q	Group Setting	Use this screen to activate 802.1Q, specify the management VLAN group, display the VLAN groups and configure the settings for each VLAN group.
	Port Setting	Use this screen to configure the PVID.
QoS	General	Use this screen to enable QoS and traffic prioritizing, and configure bandwidth management on the WAN.
	Class Setup	Use this screen to define a classifier.
Dynamic DNS	Dynamic DNS	This screen allows you to use a static hostname alias for a dynamic IP address.

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTPS or HTTP to manage the P-79X.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the P-79X.
	SSH	Use this screen to configure through which interface(s) and from which IP address(es) users can use SSH to manage the P-79X.
	SNMP	Use this screen to configure your P-79X's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the P-79X.
	ICMP	Use this screen to set whether or not your P-79X will respond to pings and probes for services that you have not made available.
	CWMP	Use this screen to configure your P-79X to be managed by an Auto Configuration Server (ACS).
UPnP	General	Use this screen to turn UPnP on or off.
Maintenance		
System	General	Use this screen to configure your P-79X's name, domain name, management inactivity timeout and password.
	Time Setting	Use this screen to change your P-79X's time and date.
Logs	View Log	Use this screen to display your P-79X's logs.
	Log Settings	Use this screen to select which logs and/or immediate alerts your P-79X is to record. You can also set it to e-mail the logs to you.
Tools	Firmware	Use this screen to upload firmware to your P-79X.
	Configuration	Use this screen to backup and restore your P-79X's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the P-79X without turning the power off.
Diagnostic	General	Use this screen to test the connections to other devices.
	DSL Line	These screen displays information to help you identify problems with the DSL connection.

2.3.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See Chapter 3 on page 25 for more information about the **Status** screen.

2.3.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

3

Status Screens

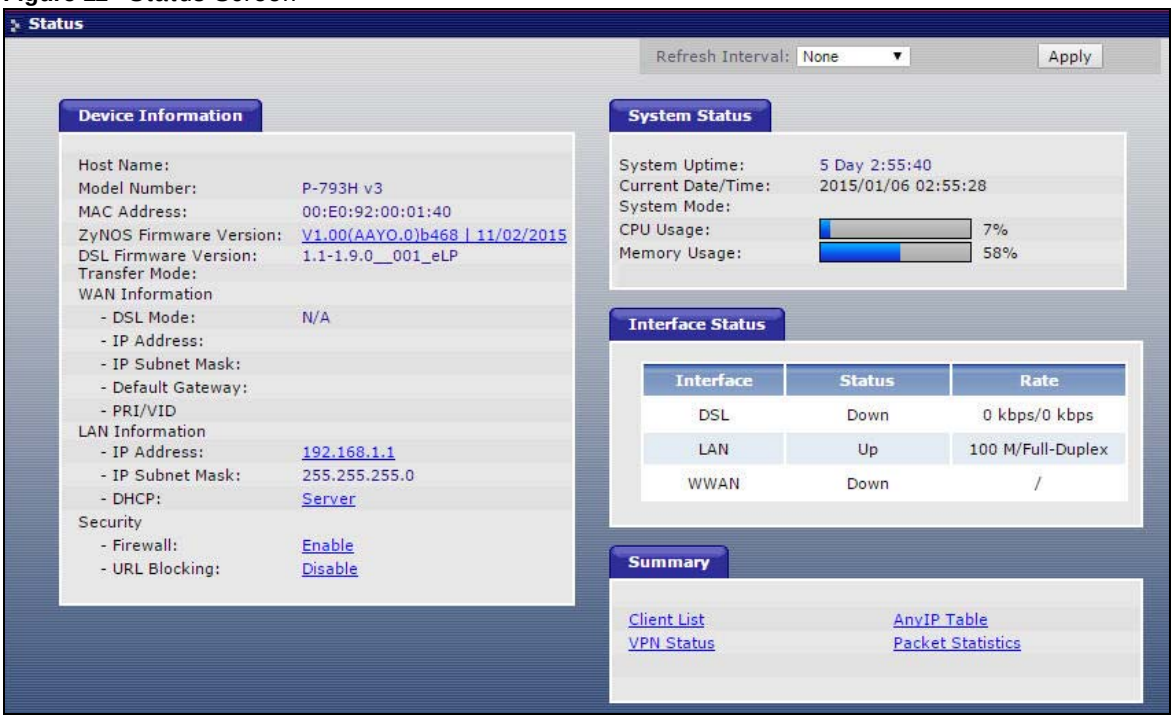
3.1 Overview

Use the **Status** screens to look at the current status of the device, system resources, and interfaces (LAN and WAN). The **Status** screen also provides detailed information of client list, Any IP, VPN and packet statistics.

3.2 The Status Screen

Use this screen to view the status of the P-79X. Click **Status** to open this screen.

Figure 11 Status Screen



Each field is described in the following table.

Table 7 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the P-79X to update this screen.
Apply	Click this to update this screen immediately.
Device Information	

Table 7 Status Screen

LABEL	DESCRIPTION
Host Name	This field displays the P-79X system name. It is used for identification. You can change this in the **Maintenance > System > General** screen's **System Name** field.
Model Number	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your P-79X.
ZyNOS Firmware Version	This is the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
DSL Firmware Version	This is the current version of the device's DSL modem code.
WAN Information	
DSL Mode	This is the DSL standard that your P-79X is using.
IP Address	This is the current IP address of the P-79X in the WAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This is the current subnet mask in the WAN.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the wizard or **WAN** screen.
LAN Information	
IP Address	This is the current IP address of the P-79X in the LAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This is the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the P-79X is providing to the LAN. Choices are: **Server** - The P-79X is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The P-79X acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The P-79X is not providing any DHCP services to the LAN. Click this to go to the screen where you can change it.
Security	
Firewall	This displays whether or not the P-79X's firewall is activated. Click this to go to the screen where you can change it.
URL Blocking	This displays whether or not the P-79X's URL Blocking is activated. Click this to go to the screen where you can change it.
System Status	
System Uptime	This field displays how long the P-79X has been running since it last started up. The P-79X starts up when you plug it in, when you restart it (**Maintenance > Tools > Restart**), or when you reset it.
Current Date/ Time	This field displays the current date and time in the P-79X. You can change this in **Maintenance > System > Time Setting**.
System Mode	This displays whether the P-79X is functioning as a router or a bridge.

Table 7 Status Screen

LABEL	DESCRIPTION
CPU Usage	This field displays what percentage of the P-79X's processing ability is currently used. When this percentage is close to 100%, the P-79X is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 17 on page 167).
Memory Usage	This field displays what percentage of the P-79X's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the P-79X is probably becoming unstable, and you should restart the device. See Section 23.4 on page 228, or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the P-79X has.
Status	This field indicates whether or not the P-79X is using the interface. For the DSL interface, this field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation. For the LAN interface, this field displays **Up** when the P-79X is using the interface and **Down** when the P-79X is not using the interface.
Rate	For the LAN interface, this displays the port speed and duplex setting. For the DSL interface, it displays the downstream and upstream transmission rate.
Summary	
Client List	Click this link to view current DHCP client information. See Section 8.4 on page 80.
VPN Status	Click this link to view the status of any VPN tunnels the P-79X has negotiated. See Section 3.4 on page 27.
AnyIP Table	Click this link to view a list of IP addresses and MAC addresses of computers, which are not in the same subnet as the P-79X. See Section 3.5 on page 28.
Packet Statistics	Click this link to view port status and packet specific statistics. See Section 3.6 on page 28.

3.3 Client List

See Section 8.4 on page 80 for information on this screen.

3.4 Status: VPN Status

See Section Figure 80 on page 139 for information on this screen.

3.5 Any IP Table

Click **Status > AnyIP Table** to access this screen. Use this screen to view the IP address and MAC address of each computer that is using the P-79X but is in a different subnet than the P-79X.

Figure 12 Any IP Table

Each field is described in the following table.

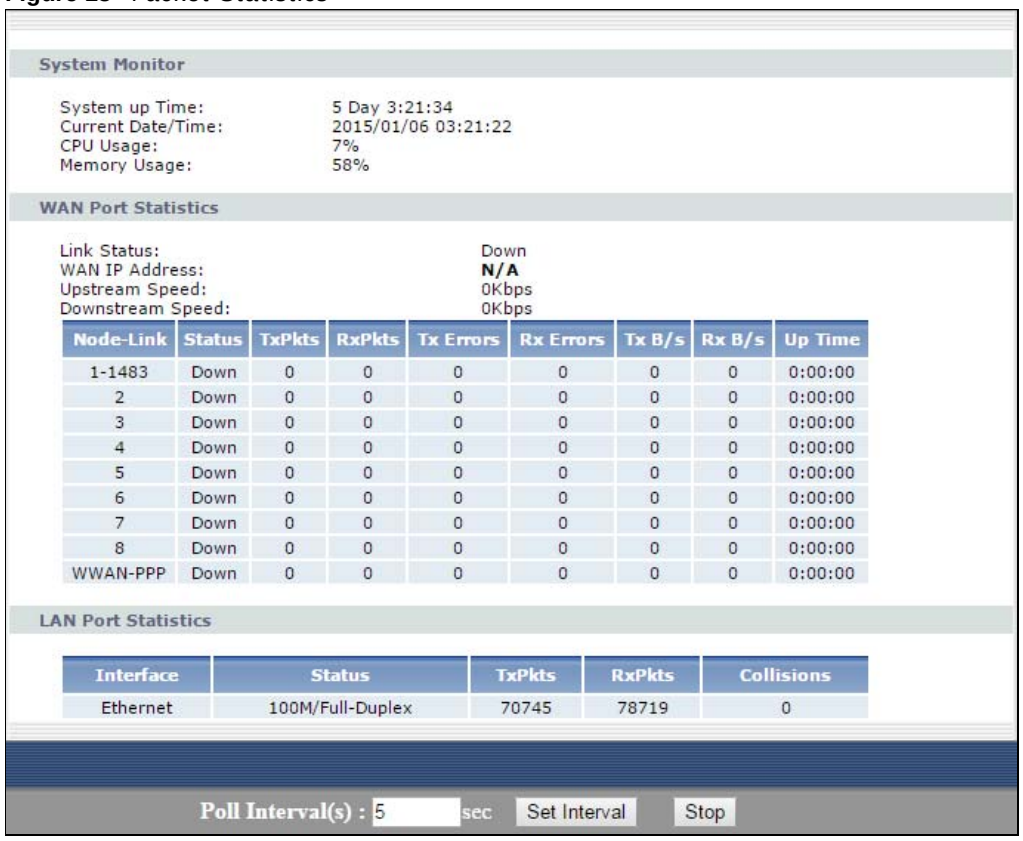
Table 8 Any IP Table

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with a specific entry.
IP Address	This field displays the IP address of each computer that is using the P-79X but is in a different subnet than the P-79X.
MAC Address	This field displays the MAC address of the computer that is using the P-79X but is in a different subnet than the P-79X.
Refresh	Click this to update this screen.

3.6 Packet Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable. Click **Status > Packet Statistics** to access this screen.

Figure 13 Packet Statistics



The following table describes the fields in this screen.

Table 9 Packet Statistics

LABEL	DESCRIPTION
System Monitor	
System up Time	This is the elapsed time the system has been up.
Current Date/Time	This field displays your P-79X's present date and time.
CPU Usage	This field specifies the percentage of CPU utilization.
Memory Usage	This field specifies the percentage of memory utilization.
WAN Port Statistics	
Link Status	This is the status of your WAN link.
WAN IP Address	This is the IP address of the P-79X's WAN port.
Upstream Speed	This is the upstream speed of your P-79X.
Downstream Speed	This is the downstream speed of your P-79X.
Node-Link	This field displays the remote node index number and link type. Link types are ENET ENCAP (RFC 1483) and PPPoE.
Status	This field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Tx Errors	This field displays the number of error packets transmitted on this port.

Table 9 Packet Statistics (continued)

LABEL	DESCRIPTION
Rx Errors	This field displays the number of error packets received on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
LAN Port Statistics	
Interface	This field displays **Ethernet** (LAN ports).
Status	For the LAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected).
TxPkts	This field displays the number of packets transmitted on this interface.
RxPkts	This field displays the number of packets received on this interface.
Collisions	This is the number of collisions on this interfaces.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this to apply the new poll interval you entered in the **Poll Interval** field above.
Stop	Click this to halt the refreshing of the system statistics.

4

Internet Setup Wizard

4.1 Overview

Use the wizard setup screens to configure your system for Internet access with the information given to you by your ISP.

Note: See the advanced menu chapters for background information on these fields.

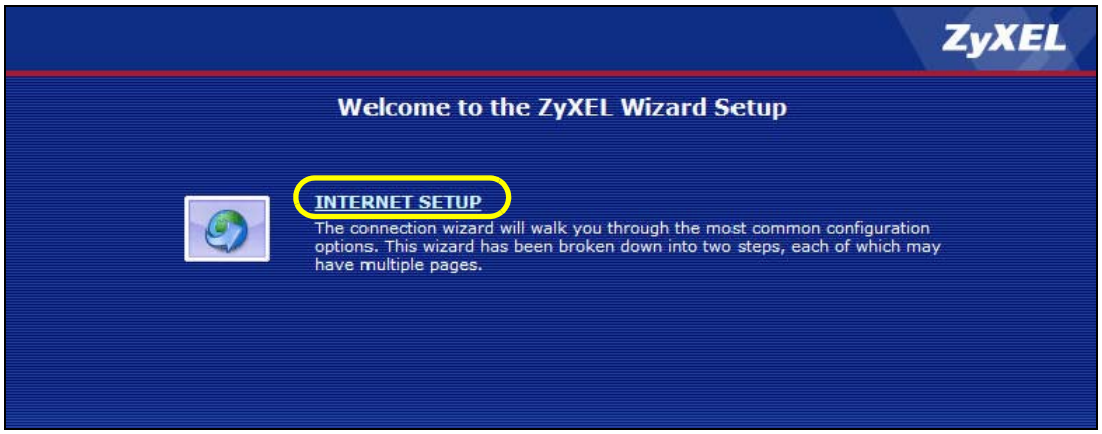
4.2 Internet Access Wizard Setup

1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon ( ) in the top right corner of the web configurator to go to the wizards.

Figure 14 Select a Mode

2 Click **INTERNET SETUP** to configure the system for Internet access.

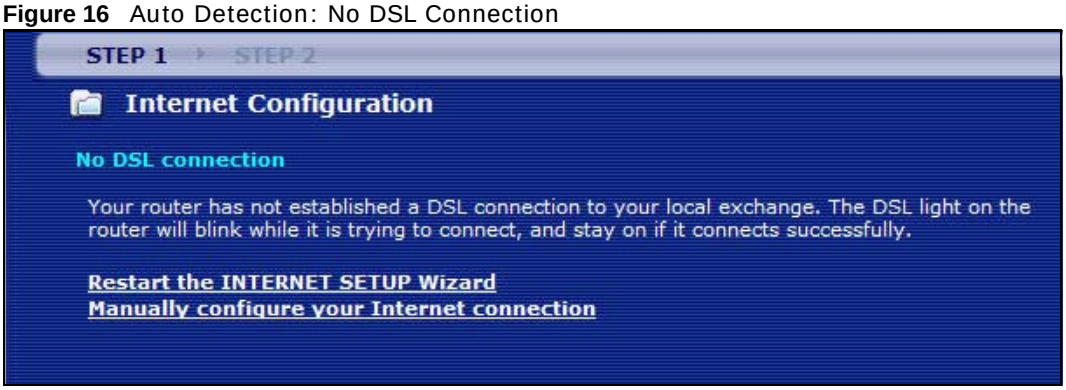
Figure 15 Wizard Welcome



3 Your P-79X attempts to detect your DSL connection and your connection type.

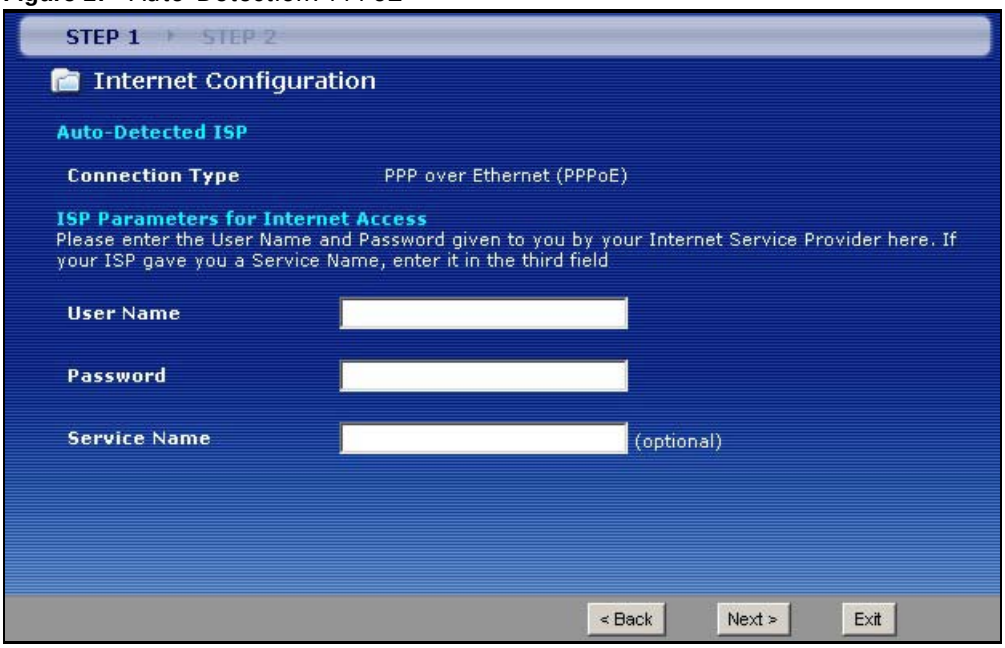
3a The following screen appears if a connection is not detected. Check your hardware connections and click **Restart the INTERNET SETUP Wizard** to return to the wizard welcome screen. If you still cannot connect, click **Manually configure your Internet connection**. Follow the directions in the wizard and enter your Internet setup information as provided to you by your ISP. See Section 4.2.1 on page 33 for more details.

Figure 16 Auto Detection: No DSL Connection



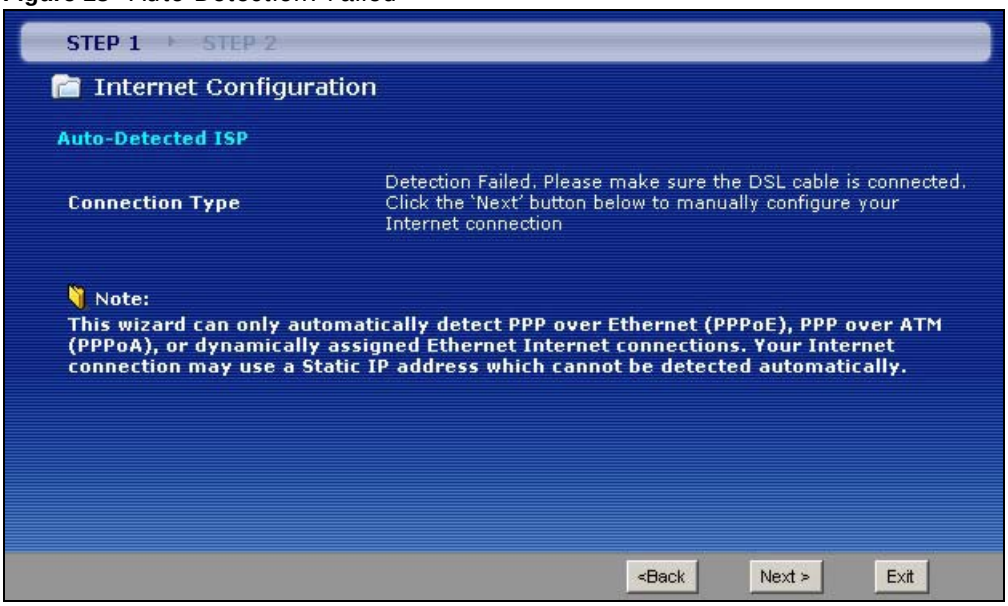
3b The following screen displays if a PPPoE connection is detected. Enter your Internet account information (username, password and/or service name) exactly as provided by your ISP. Then click **Next**.

Figure 17 Auto-Detection: PPPoE



3c The following screen appears if the ZyXEL device detects a connection but not the connection type. Click **Next** and refer to Section 4.2.1 on page 33 on how to manually configure the P-79X for Internet access.

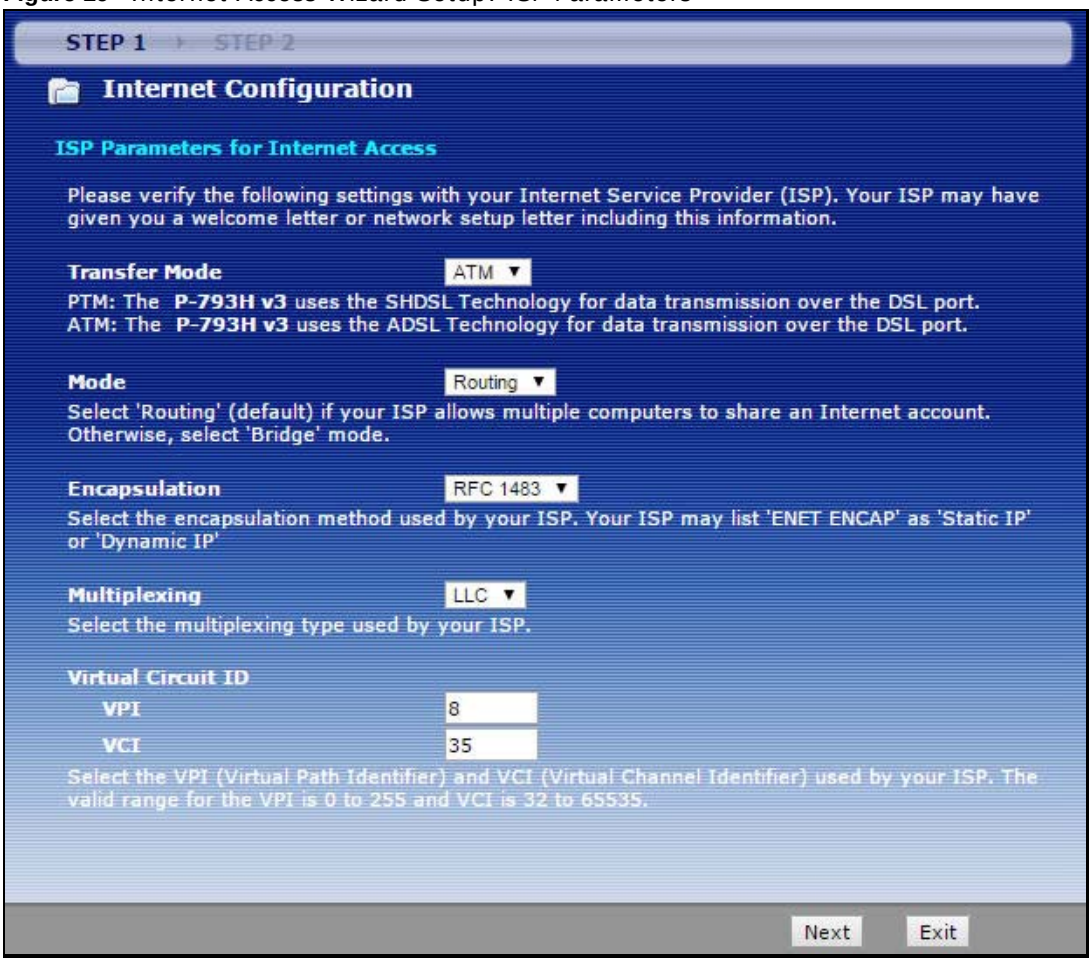
Figure 18 Auto Detection: Failed



4.2.1 Manual Configuration

1 If the P-79X fails to detect your DSL connection type but the physical line is connected, enter your Internet access information in the wizard screen exactly as your service provider gave it to you. Leave the defaults in any fields for which you were not given information.

Figure 19 Internet Access Wizard Setup: ISP Parameters



The following table describes the fields in this screen.

Table 10 Internet Access Wizard Setup: ISP Parameters

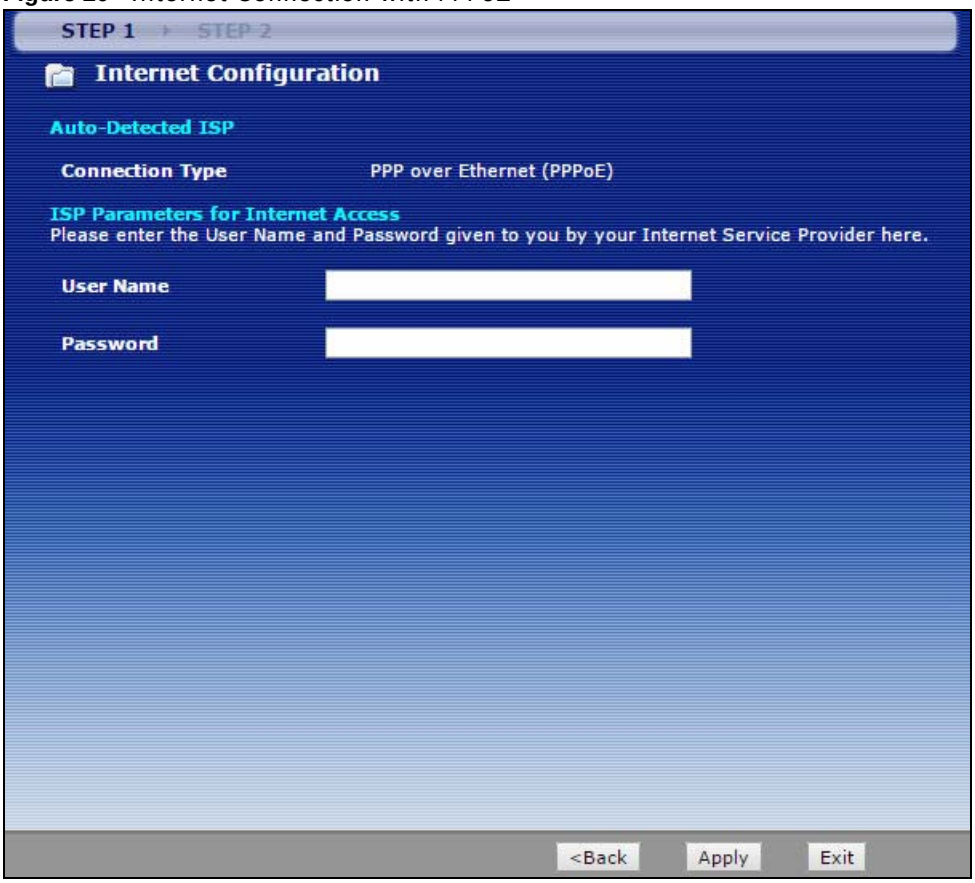
LABEL	DESCRIPTION
Transfer Mode	Select the transfer mode you want to use. **PTM** (Packet Transfer Mode): The P-79X uses the SHDSL technology for data transmission over the DSL port. **ATM** (Asynchronous Transfer Mode): The P-79X uses the ADSL technology for data transmission over the DSL port. Select **Auto** if the P-79X uses the SHDSL or the ADSL technology for data transmission over the DSL port.
Mode	Select **Routing** (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account. Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use Firewall, DHCP server and NAT on the P-79X.
Encapsulation	Select the encapsulation type your ISP uses from the **Encapsulation** drop-down list box. Choices vary depending on what you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select **RFC 1483**. If you select **Routing** in the **Mode** field, select **RFC 1483** or **PPPoE**.

Table 10 Internet Access Wizard Setup: ISP Parameters

LABEL	DESCRIPTION
Multiplexing	Select the multiplexing method used by your ISP from the **Multiplex** drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Next	Click this to continue to the next wizard screen. The next wizard screen you see depends on what protocol you chose above.
Exit	Click this to close the wizard screen without saving.

2 The next wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue.

Figure 20 Internet Connection with PPPoE



The following table describes the fields in this screen.

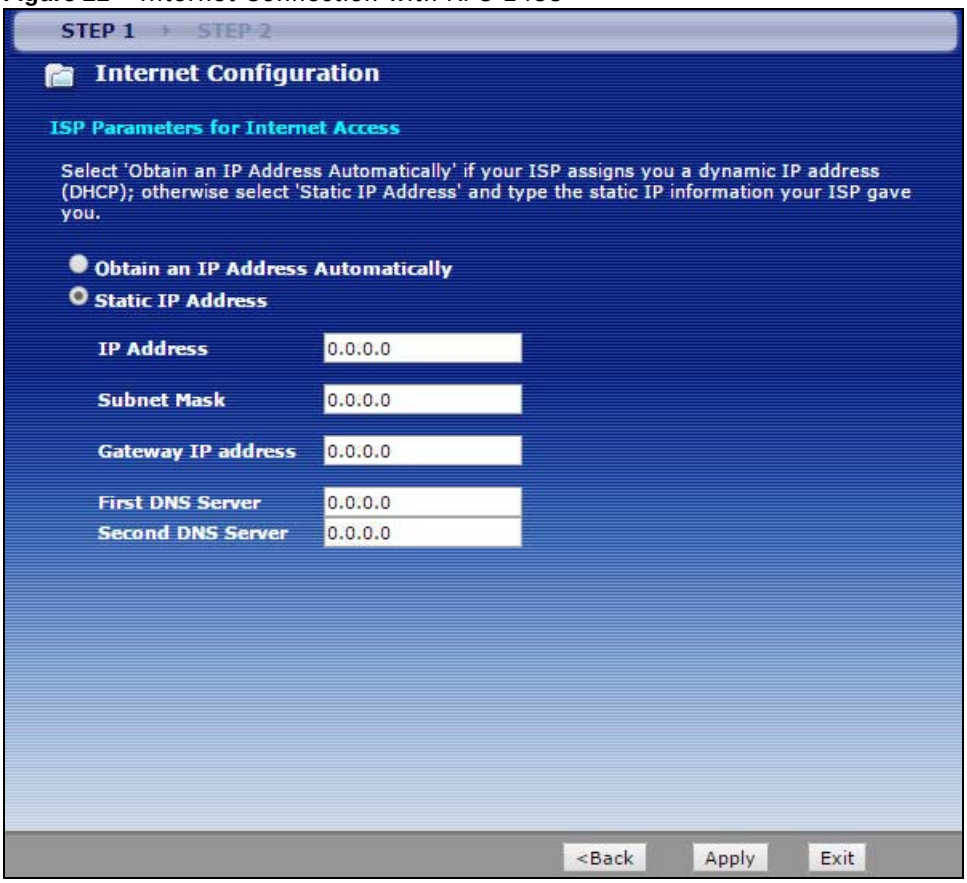
Table 11 Internet Connection with PPPoE

LABEL	DESCRIPTION
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.

Table 11 Internet Connection with PPPoE (continued)

LABEL	DESCRIPTION
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Exit	Click this to close the wizard screen without saving.

Figure 21 Internet Connection with RFC 1483



The following table describes the fields in this screen.

Table 12 Internet Connection with RFC 1483

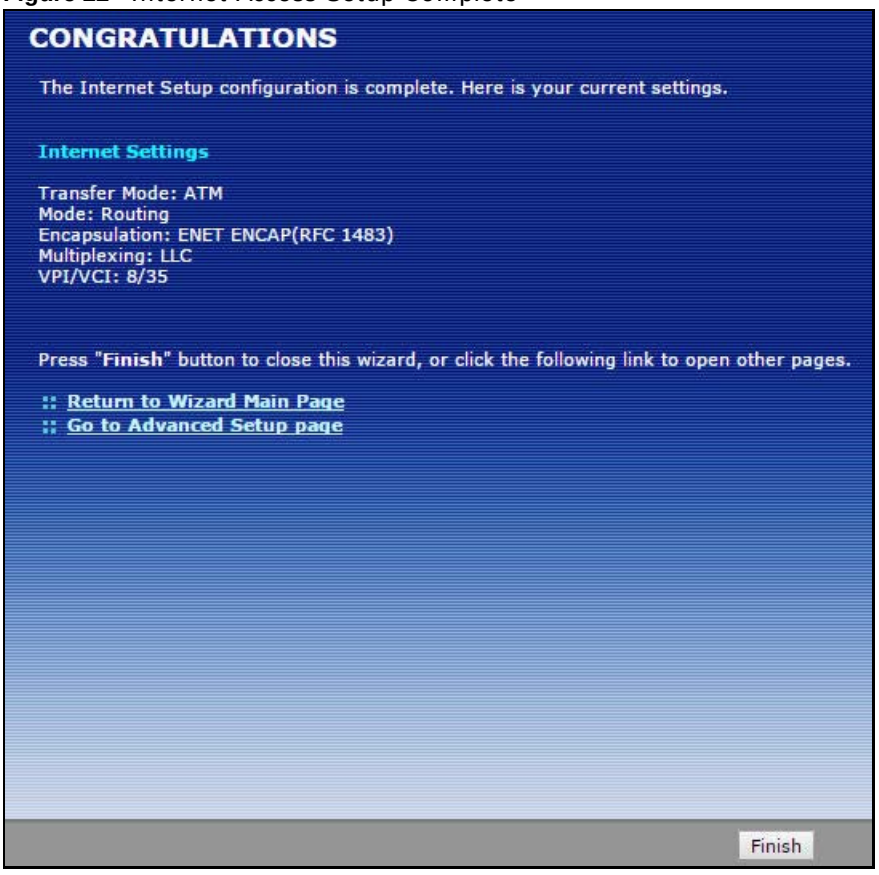
LABEL	DESCRIPTION
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select **Obtain an IP Address Automatically** if you have a dynamic IP address.
Static IP Address	Select **Static IP Address** if your ISP gave you an IP address to use.
IP Address	Enter your ISP assigned IP address.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendix to calculate a subnet mask If you are implementing subnetting.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you use **ENET ENCAP** in the **Encapsulation** field in the previous screen.

Table 12 Internet Connection with RFC 1483 (continued)

LABEL	DESCRIPTION
First DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Second DNS Server	As above.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Exit	Click this to close the wizard screen without saving.

3 Use the read-only summary table to check whether what you have configured is correct. Click **Finish** to complete and save the wizard setup.

Figure 22 Internet Access Setup Complete



4 Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the rest of this guide for more detailed information on the complete range of P-79X features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the wizard setup are correct.

5

Tutorials

5.1 Overview

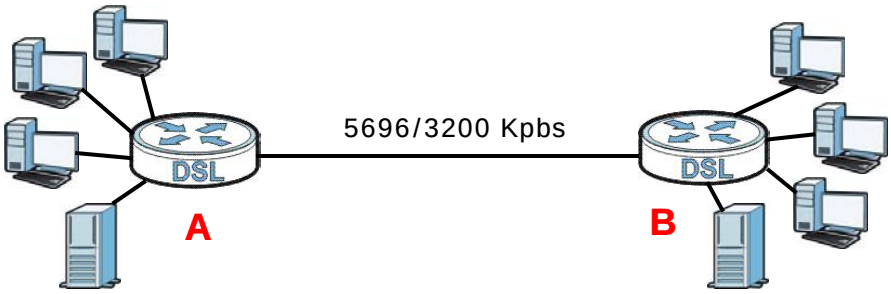
This chapter describes:

- Configuring Point-to-point Connection, see page 38
- Configuring a Point-to-2points Connection, see page 40

Note: The tutorials featured in this chapter require a basic understanding of connecting to and using the Web Configurator on your P-79X. For details, see the included Quick Start Guide. For field descriptions of individual screens, see the related technical reference in this User's Guide.

5.2 Configuring Point-to-point Connection

In this scenario, Company **A** wants to set up a point-to-point connection with its branch office **B** by using two P-79Xs. The two P-79Xs are directly connected together through their DSL ports. The P-79X on **A**'s side is the server and the P-79X on **B**'s side is the client. The maximum transfer rate for the DSL connection between **A** and **B** is **5696** Kbps and the minimum transfer rate is **3200** Kbps.



To set up the point-to-point connection between **A** and **B**, you need to:

1 Set Up the Server.

2 Set Up the Client.

3 Connect the P-79Xs.

5.2.1 Set Up the Server

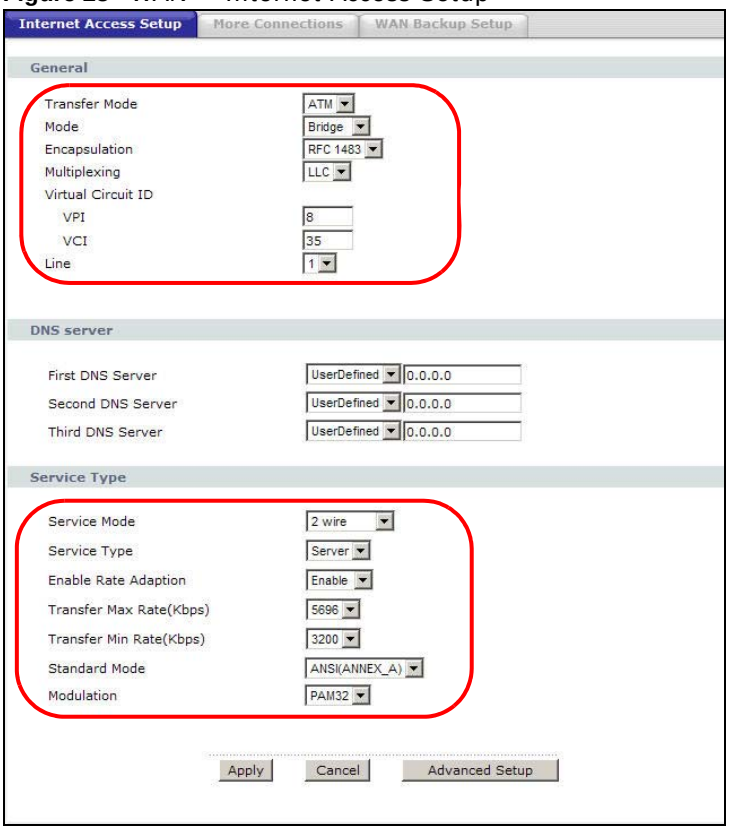
1 Log in to the server P-79X of Company **A**.

2 Click **Network > WAN > Internet Access Setup**.

3 Configure the **Internet Access Setup** screen as the following. Select **ATM** as the **Transfer Mode**. Select **Bridge** as the **Mode**. Configure the **Multiplexing**, **Encapsulation, VPI**, and **VCI** fields for the point-to-point connection. Select **1** in the **Line** field as the DSL line you want the P-79X to use as a default for outgoing traffic.

4 Then configure the **Service Type** section. Select **2 wire** in the **Service Mode** field. In the **Service Type** field, select **Server**. Select **5696** as the **Transfer Max Rate** and **3200** as the **Transfer Min Rate**. Leave the rest of the fields set to their default settings. Click **Apply**.

Figure 23 WAN > Internet Access Setup



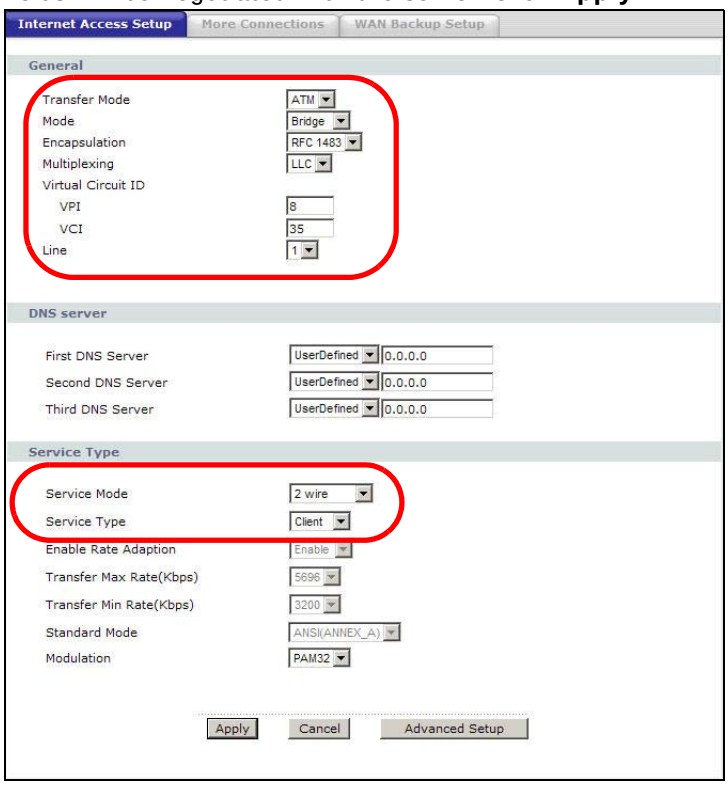
5.2.2 Set Up the Client

1 Log in to the client P-79X of branch office **B**.

2 Click **Network > WAN > Internet Access Setup**.

3 Select **ATM** as the **Transfer Mode**. Select **Bridge** as the **Mode**. Set the **Multiplexing**, **Encapsulation, VPI**, and **VCI** to the same values you set in the server. Select **1** in the **Line** field as the DSL line you want the P-79X to use as a default for outgoing traffic.

4 Scroll down to the **Service Type** section. In the **Service Mode** field, select **2 wire**, the same type of connection you selected for the server. In the **Service Type** field, select **Client**. The rest of the fields will be negotiated with the server. Click **Apply**.

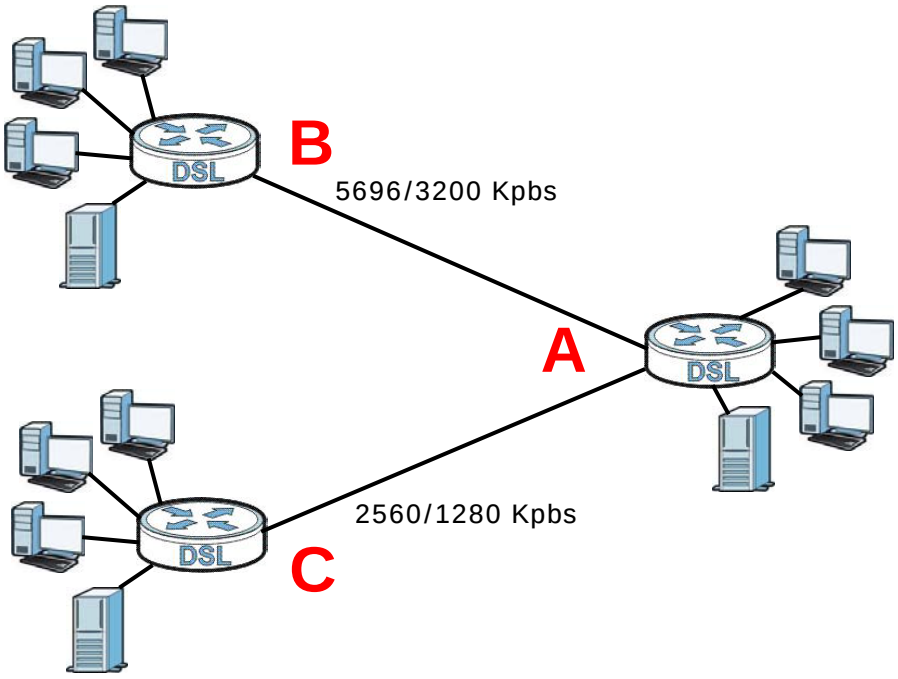


5.2.3 Connect the P-79Xs

Connect the **DSL** ports on the P-79Xs together, and wait while the P-79Xs automatically establish the connection. When the connection is established, the **DSL1**, **DSL2**, and **INTERNET** lights are on. It takes up to half a minute to establish the connection. If the P-79Xs do not establish the connection, verify that the settings (except the **Service Type**) match.

5.3 Configuring a Point-to-2points Connection

Now Company **A** has another branch office, **C** and wants to set up a point-to-2points connection between a server P-79X on **A**'s side and client P-79Xs at **B** and **C**. The maximum transfer rate for the DSL connection between **A** and **B** is **5696** Kbps and the minimum transfer rate is **3200** Kbps. The maximum transfer rate for the DSL connection between **A** and **C** is **2560** Kbps and minimum transfer rate is **1280** Kbps.



To set up the point-to-2 point connection between **A**, **B** and **C** you need to:

1 Set up the Server.

2 Set up the Clients.

3 Connect the P-79Xs.

5.3.1 Set up the Server

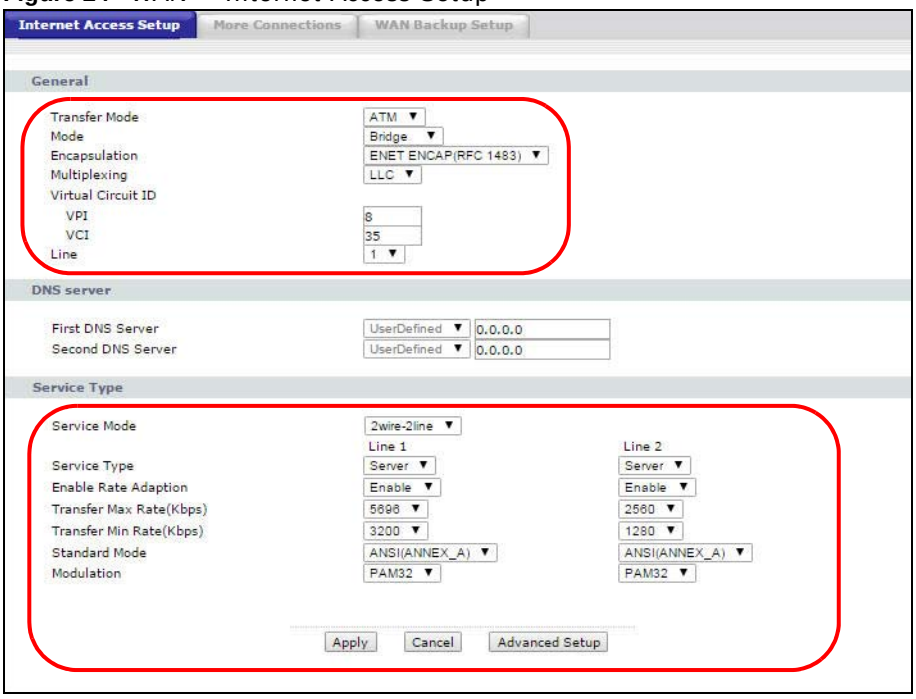
1 Log in to the server P-79X of Company **A**.

2 Click **Network > WAN > Internet Access Setup**.

3 Configure the **Internet Access Setup** screen as the following. Select **ATM** as the **Transfer Mode**. Select **Bridge** as the **Mode**. Configure the **Multiplexing**, **Encapsulation, VPI**, and **VCI** fields for the point-to-point connection. Select **1** in the **Line** field as the DSL line you want the P-79X to use as a default for outgoing traffic.

4 Then configure the **Service Type** section. Select **2 wire-2 line** in the **Service Mode** field. In the **Service Type** field, select **Server**. For Line1 configuration, select **5696** as the **Transfer Max Rate** and **3200** as the **Transfer Min Rate**. For Line2 configuration, select **2560** as the **Transfer Max Rate** and **1280** as the **Transfer Min Rate**. Leave the rest of the fields to their default settings. Click **Apply**.

Figure 24 WAN > Internet Access Setup



5.3.2 Set up the Clients

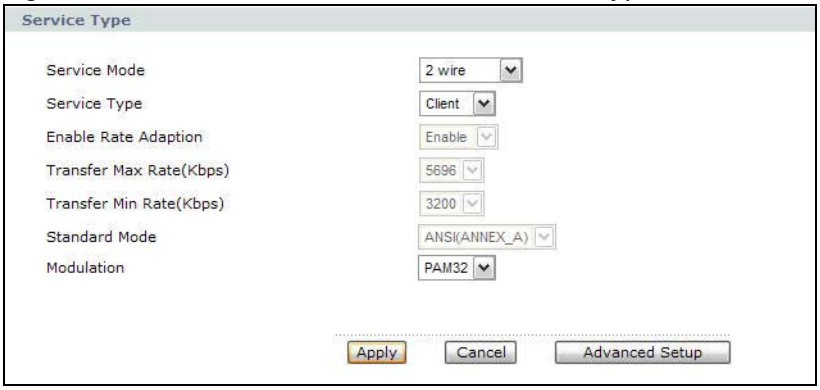
1 Log in to the client P-79X of branch office **B**.

2 Click **Network > WAN > Internet Access Setup**.

3 Select **ATM** as the **Transfer Mode**. Set the **VPI**, **VCI**, **Multiplexing**, and **Encapsulation** to the same values you set in the server.

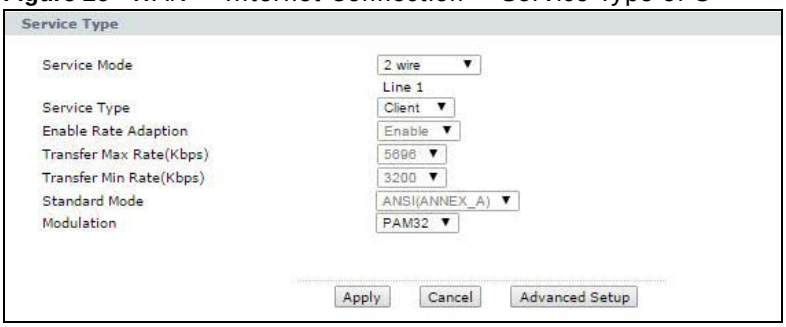
4 Scroll down to the **Service Type** section. In the **Service Mode** field, select **2 wire**. In the **Service Type** field, select **Client**. The rest of the fields will be negotiated with the server. Click **Apply**.

Figure 25 WAN > Internet Connection > Service Type of **B**



5 Repeat the above steps 1 to 4 for the second client P-79X on **C**'s side. The **Service Type** should look like the following.

Figure 26 WAN > Internet Connection > Service Type of **C**



5.3.3 Connect the P-79Xs

Connect the **DSL** ports on the P-79Xs together, and wait while the P-79Xs automatically establish the connection. Make sure that the Y-cable is connected to the proper DSL outlets. The Y-cable connector marked **DSL1** must be connected to the outgoing DSL 1 telephone jack and the Y-cable connector marked **DSL2** must be connected to the outgoing DSL 2 telephone jack.

When the connection is established, the **DSL1**, **DSL2**, and **INTERNET** lights turn on. It takes up to half a minute to establish the connection. If the P-79Xs do not establish the connection, verify that the settings are correct.

PART II
Technical Reference

6

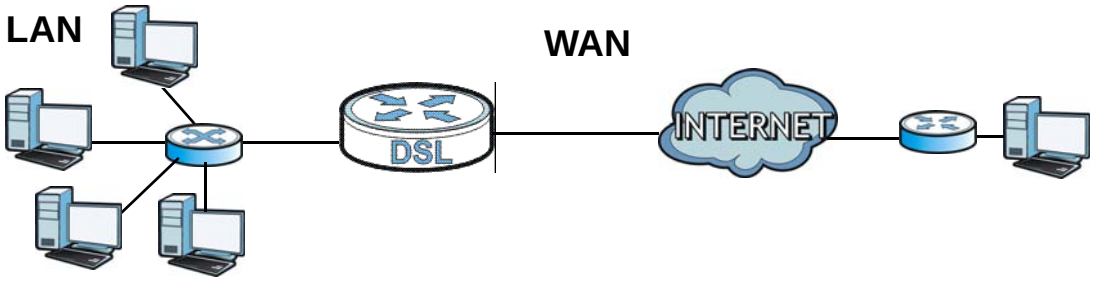
WAN Setup

6.1 Overview

This chapter describes how to configure WAN settings from the **WAN** screens. Use these screens to configure your P-79X for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks (such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 27 LAN and WAN



6.1.1 What You Can Do in the WAN Screens

- Use the **Internet Access Setup** screen (Section 6.2 on page 46) to configure the WAN settings on the P-79X for Internet access.
- Use the **More Connections** screen (Section 6.3 on page 53) to set up additional Internet access connections.
- Use the **WAN Backup Setup** screen (Section 6.4 on page 57) to set up a backup gateway that helps forward traffic to its destination when the default WAN connection is down.

6.1.2 What You Need to Know About WAN

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the P-79X, which makes it accessible from an outside network. It is used by the P-79X to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the P-79X tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

ATM

Asynchronous Transfer Mode (ATM) is a LAN and WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells.

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

Multicast

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

IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 and 3 are improvements over version 1, but IGMP version 1 and 2 are still in wide use.

Finding Out More

See Section 6.5 on page 59 for technical background information on WAN.

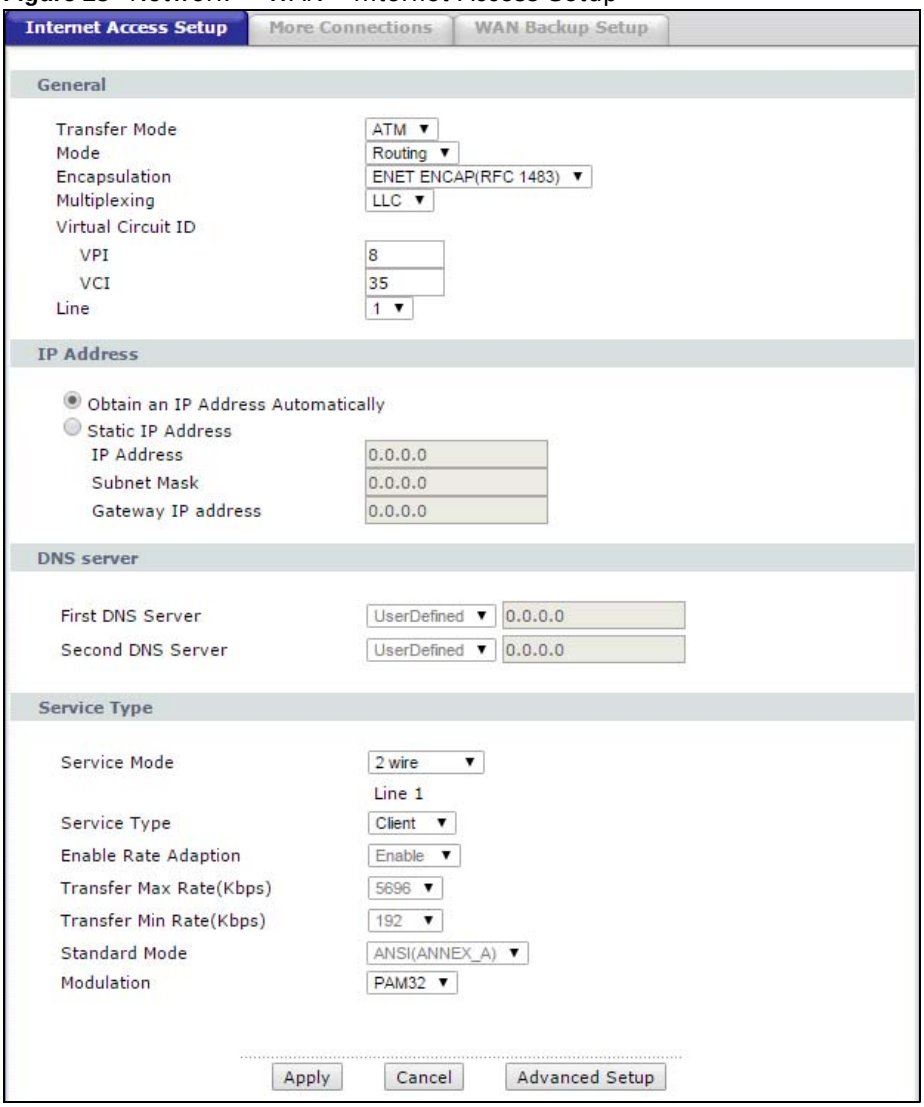
6.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

6.2 The Internet Access Setup Screen

Use this screen to change your P-79X's WAN settings. Click **Network > WAN > Internet Access Setup**. The screen differs by the WAN type and encapsulation you select.

Figure 28 Network > WAN >Internet Access Setup



The following table describes the labels in this screen.

Table 13 Network > WAN > Internet Access Setup

LABEL	DESCRIPTION
General	
Transfer Mode	Select the transfer mode you want to use. **PTM** (Packet Transfer Mode): The P-79X uses the SHDSL technology for data transmission over the DSL port. **ATM** (Asynchronous Transfer Mode): The P-79X uses the ADSL technology for data transmission over the DSL port. Select **Auto** if the P-79X uses the SHDSL or the ADSL technology for data transmission over the DSL port.

Table 13 Network > WAN > Internet Access Setup (continued)

LABEL	DESCRIPTION
Mode	Select **Routing** (default) from the drop-down list box if your ISP gives you one IP address only and you want multiple computers to share an Internet account. Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use Firewall, DHCP server and NAT on the P-79X.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select **ENET ENCAP (RFC 1483)**. If you select **Routing** in the **Mode** field, select **ENET ENCAP (RFC 1483)** or **PPPoE**. If you set up a point-to-point or a point-to-2points connection, select either **ENET ENCAP (RFC 1483)**.
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**. This is available only when you select **ATM** in the **Transfer Mode** field.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information. This is available only when you select **ATM** in the **Transfer Mode** field.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
Tag VLAN ID for egress packets	Select this option to add the VLAN tag (specified below) to the outgoing traffic through this connection. This is available only when you select **PTM** in the **Transfer Mode** field.
Enter 802.1P Priority	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
Enter 802.1Q VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
Line	Select the DSL line you want the P-79X to use as a default for outgoing traffic (remote node 1).
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below.

Table 13 Network > WAN > Internet Access Setup (continued)

LABEL	DESCRIPTION
Subnet Mask	This option is available if you select **ENET ENCAP** in the **Encapsulation** field. Enter a subnet mask in dotted decimal notation.
Gateway IP address	This option is available if you select **ENET ENCAP** in the **Encapsulation** field. Specify a gateway IP address (supplied by your ISP).
DNS Server	
First DNS Server Second DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the P-79X's WAN IP address) and you select **Obtain an IP Address Automatically**. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. You must have another DNS server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Connection (PPPoE encapsulation only)	
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The P-79X will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Service Type	
Service Mode	Select **2-wire**, **4-wire** or **2wire-2line** mode for the DSL connection. This is depends on the network configuration you want to set up and the phone lines you use. Service mode affects the maximum speed of the connection. In **2-wire** mode, the maximum data rate is up to 5.69 Mbps, while in **4-wire** mode, the maximum data rate is up to 11.38 Mbps. In **2wire-2line** mode the maximum data rate is 5.69 Mbps for each line. See Section 6.2.1 on page 50 for more information on configuring **2wire-2line** mode.
Service Type	Indicate whether the P-79X is the server or the client in the DSL connection. Select **Server** if this P-79X is the server in a point-to-point application. Otherwise, select **Client**. This field is not configurable if you select **2wire-2line** mode because the ZyXEL Device is automatically set to **Server**.
Enable Rate Adaption	This field is enabled if **Service Type** is **Server**. Indicate whether or not the P-79X can adjust the speed of its connection to that of the other device.
Transfer Max Rate (Kbps)	This field is enabled if **Service Type** is **Server**. Set the maximum rate at which the P-79X sends and receives information. The actual transfer rate will be between this value and the minimum transfer rate you configure. When you select **4-wire** in the **Service Mode** field, then the transfer rate you set here is doubled. For example, select 5696 Kbps to configure a maximum transfer rate of 11392 Kbps.

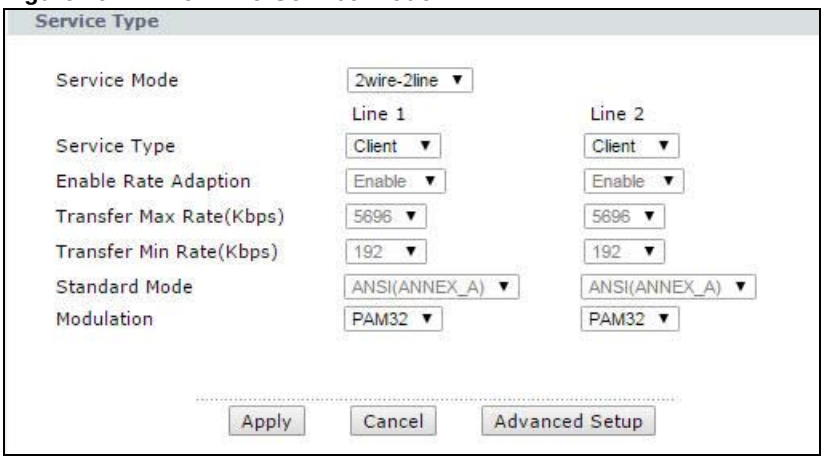
Table 13 Network > WAN > Internet Access Setup (continued)

LABEL	DESCRIPTION
Transfer Min Rate (Kbps)	This field is enabled if **Service Type** is **Server**. Set the minimum rate at which the P-79X sends and receives information. The actual transfer rate will be between this value and the maximum transfer rate you configure. When you select **4-wire** in the **Service Mode** field, then the transfer rate you set here is doubled. For example, select 192 Kbps to configure a minimum transfer rate of 384 Kbps.
Standard Mode	This field is enabled if **Service Type** is **Server**. Select the operational mode the P-79X uses in the DSL connection. ANSI (ANNEX_A) refers to connections over POTS and ETSI (ANNEX_B) refers to connections over ISDN lines.
Modulation	Select the modulation supported by your ISP.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the **Advanced WAN Setup** screen and edit more details of your WAN setup.

6.2.1 2Wire-2Line Service Mode

The **Service Mode** section of the **Internet Connection** screen allows you to set up two DSL connections when you select **2wire-2line** mode. This allows you to create a point-to-2points configuration.

Figure 29 2wire-2line Service Mode



The following table describes the labels in this screen.

Table 14 2wire-2line Service Mode

LABEL	DESCRIPTION
Service Type	
Service Mode	Select **2wire-2line** mode for the DSL connection. This means that the P-79X is going to be a server connected to two client P-79Xs.
Service Type	When you select **2wire-2line** mode this field automatically changes to **Server** or **Client**.
Line1 / Line 2	You can configure different connection rate settings for **Line 1** and **Line 2** DSL connections.

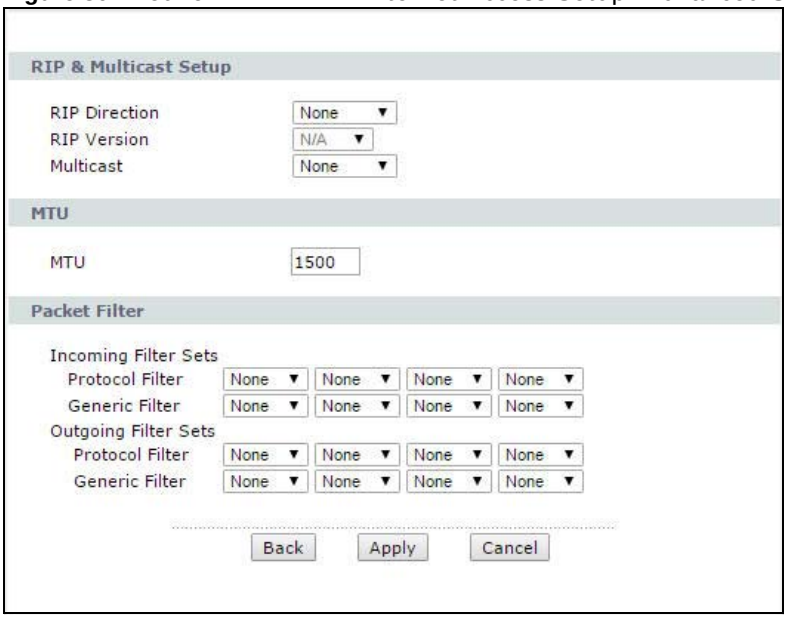
Table 14 2wire-2line Service Mode (continued)

LABEL	DESCRIPTION
Enable Rate Adaption	Indicate whether or not the P-79X can adjust the speed of its connection to that of the other device.
Transfer Max Rate (Kbps)	This field is enabled if **Service Type** is **Server**. Set the maximum rate at which the P-79X sends and receives information. The actual transfer rate will be between this value and the minimum transfer rate you configure.
Transfer Min Rate (Kbps)	This field is enabled if **Service Type** is **Server**. Set the minimum rate at which the P-79X sends and receives information. The actual transfer rate will be between this value and the maximum transfer rate you configure.
Standard Mode	Select the operational mode the P-79X uses in the DSL connection. Annex A refers to connections over POTS and Annex B refers to connections over ISDN lines.
Modulation	Select the modulation supported by your ISP.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Advanced Setup	Click this button to display the **Advanced WAN Setup** screen and edit more details of your WAN setup.

6.2.2 Advanced Internet Access Setup

Use this screen to edit your P-79X's advanced WAN settings. Click the **Advanced Setup** button in the **Internet Access Setup** screen. The screen appears as shown.

Figure 30 Network > WAN > Internet Access Setup: Advanced Setup



The following table describes the labels in this screen.

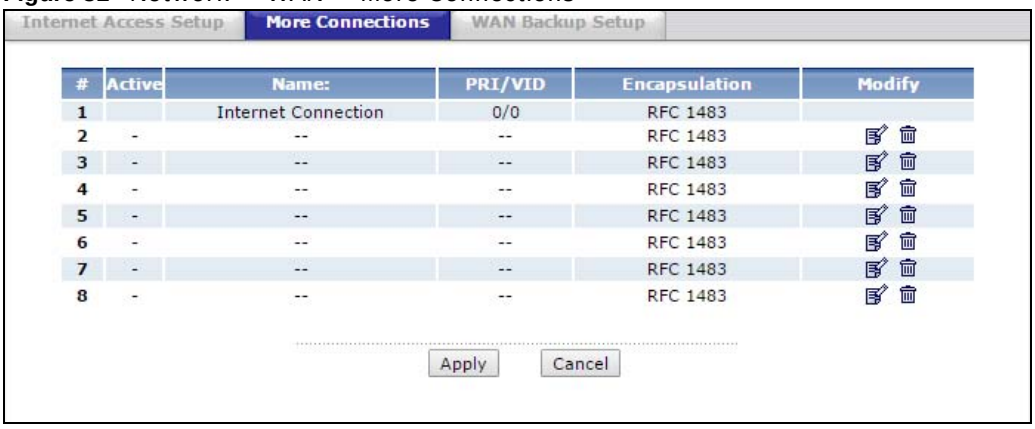
Table 15 Network > WAN > Internet Access Setup: Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	This section is not available when you configure the P-79X to be in bridge mode.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Use this field to control how much routing information the P-79X sends and receives on the subnet. Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	This field is not configurable if you select **None** in the **RIP Direction** field. Select the RIP version from **RIP-1** and **RIP-2**.
Multicast	Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer). Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a multicast group. The P-79X supports **IGMP-v1**, **IGMP-v2, IGMP-v3** and **IGMP-all**. Select **None** to disable it.
MTU	
MTU	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field. For ENET ENCAP, the MTU value is 1500. For PPPoE, the MTU value is 1492. For PPPoA and RFC 1483, the MTU is 65535.
Packet Filter	
Incoming Filter Sets	
Protocol Filter	Select the protocol filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure packet filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.
Generic Filter	Select the generic filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.
Outgoing Filter Sets	
Protocol Filter	Select the protocol filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure protocol filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.
Generic Filter	Select the generic filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

6.3 The More Connections Screen

The P-79X allows you to configure more than one Internet access connection. To configure additional Internet access connections click **Network > WAN > More Connections**. The screen differs by the encapsulation you select. When you use the **WAN > Internet Access Setup** screen to set up Internet access, you are configuring the first WAN connection.

Figure 31 Network > WAN > More Connections



The following table describes the labels in this screen.

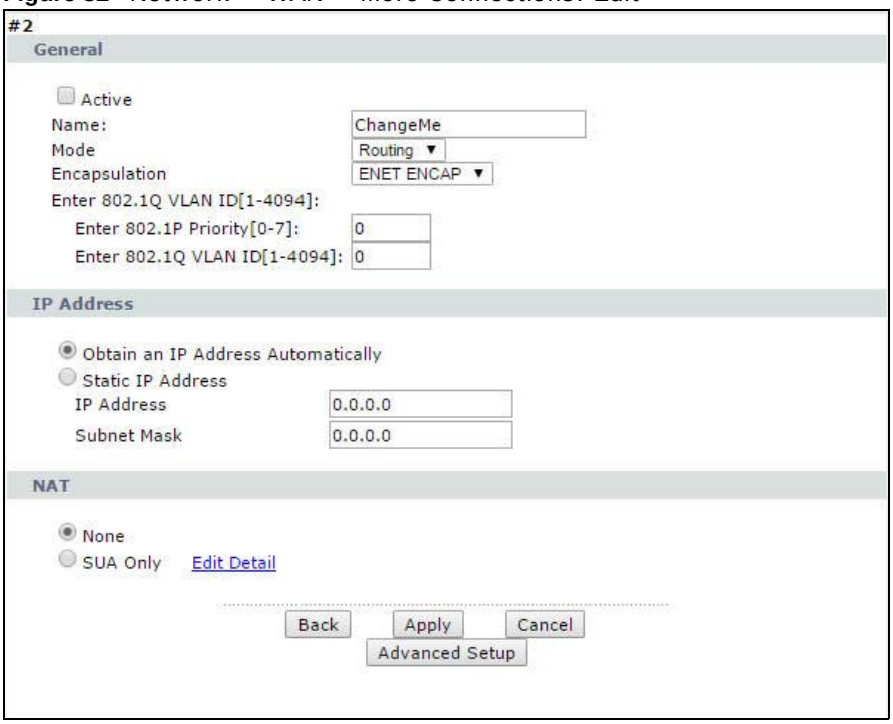
Table 16 Network > WAN > More Connections

LABEL	DESCRIPTION
#	This is an index number indicating the number of the corresponding connection.
Active	This field indicates whether the connection is active or not.
Name	This is the name you gave to the Internet connection.
PRI/VID	**PRI** indicates the 802.1P priority level assigned to traffic sent through this connection. This displays **-** when there is no priority level assigned. **VID** indicates the 802.1Q VLAN ID number assigned to traffic sent through this connection. This displays **-** when there is no VLAN ID number assigned.
Encapsulation	This field indicates the encapsulation method of the Internet connection.
Modify	The first (ISP) connection is read-only in this screen. Use the **WAN > Internet Access Setup** screen to edit it. Click the Edit icon to edit the Internet connection settings. Click this icon on an empty configuration to add a new Internet access setup. Click the Remove icon to delete the Internet access setup from your connection list.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

6.3.1 More Connections Edit

Use this screen to configure a connection. Click the edit icon in the **More Connections** screen to display the following screen.

Figure 32 Network > WAN > More Connections: Edit



The following table describes the labels in this screen.

Table 17 Network > WAN > More Connections: Edit

LABEL	DESCRIPTION
#	This is the index number of the WAN connections.
General	
Active	Select the check box to activate or clear the check box to deactivate this connection.
Name	Enter a unique, descriptive name of up to 13 ASCII characters for this connection.
Mode	Select **Routing** from the drop-down list box if your ISP allows multiple computers to share an Internet account. If you select **Bridge**, the P-79X will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select **ENET ENCAP**. If you select **Routing** in the **Mode** field, select **ENET ENCAP** or **PPPoE**. If you set up a point-to-point connection, select **ENET ENCAP**.
User Name	(PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoE encapsulation only) Enter the password associated with the user name above.
Enter 802.1P Priority[0-7]	Specify a priority level (between 0 and 7). "0" is the lowest priority level and "7" is the highest.

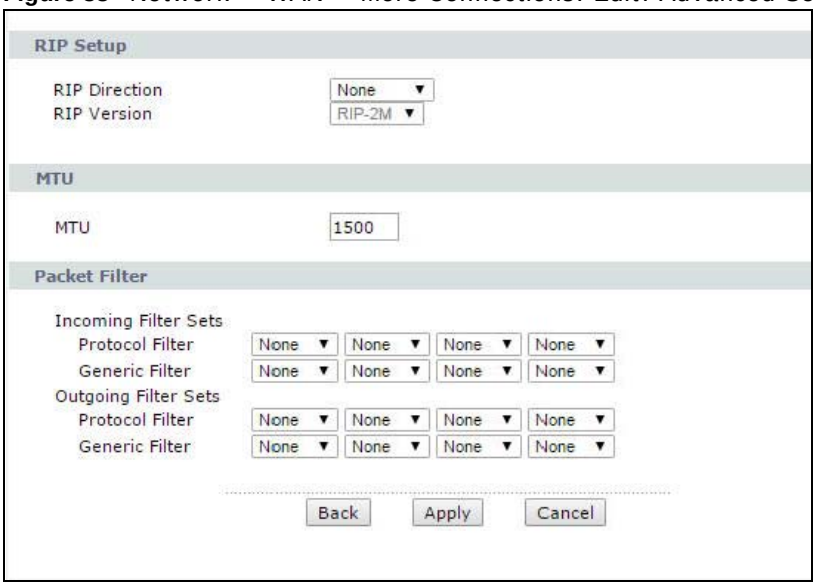
Table 17 Network > WAN > More Connections: Edit (continued)

LABEL	DESCRIPTION
Enter 802.1Q VLAN ID[1-4094]	Specify a VLAN ID number.
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. If you use the encapsulation type except **ENET ENCAP**, select **Obtain an IP Address Automatically** when you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below. If you use **ENET ENCAP**, enter the IP address given by your ISP in the **IP Address** field.
Subnet Mask	Enter a subnet mask in dotted decimal notation.
Connection	
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The P-79X will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
NAT	**SUA only** is available only when you select **Routing** in the **Mode** field. Select **SUA Only** if you have one public IP address and want to use NAT. Click **Edit Detail** to go to the **Port Forwarding** screen to edit a server mapping set. Otherwise, select **None** to disable NAT.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the **More Connections Advanced Setup** screen and edit more details of your WAN setup.

6.3.2 Configuring More Connections Advanced Setup

Use this screen to edit your P-79X's advanced WAN settings. Click the **Advanced Setup** button in the **More Connections Edit** screen. The screen appears as shown.

Figure 33 Network > WAN > More Connections: Edit: Advanced Setup



The following table describes the labels in this screen.

Table 18 Network > WAN > More Connections: Edit: Advanced Setup

LABEL	DESCRIPTION
RIP Setup	This section is not available when you configure the P-79X to be in bridge mode.
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
MTU	
MTU	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field. For ENET ENCAP, the MTU value is 1500. For PPPoE, the MTU value is 1492. For PPPoA and RFC, the MTU is 65535.
Packet Filter	
Incoming Filter Sets	
Protocol Filter	Select the protocol filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure packet filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.
Generic Filter	Select the generic filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.
Outgoing Filter Sets	
Protocol Filter	Select the protocol filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure protocol filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.

Table 18 Network > WAN > More Connections: Edit: Advanced Setup (continued)

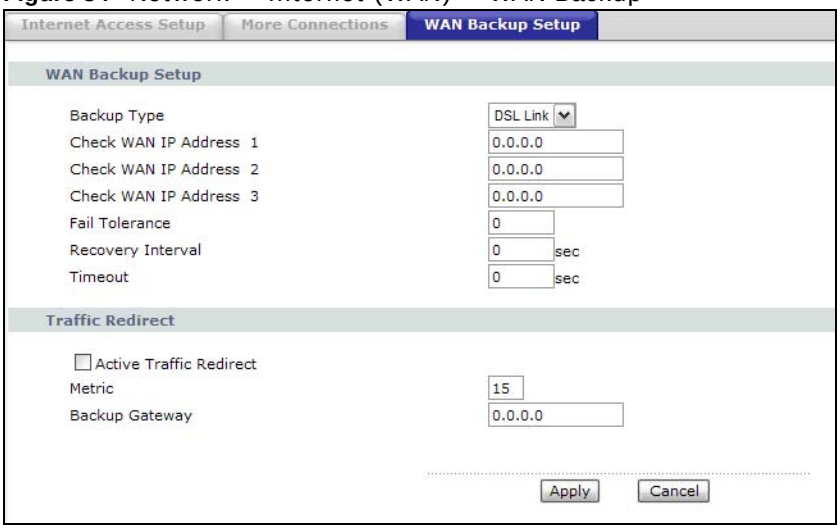
LABEL	DESCRIPTION
Generic Filter	Select the generic filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

6.4 The WAN Backup Setup Screen

Use this screen to configure your P-79X's WAN backup. Click **Network > WAN > WAN Backup Setup**. This screen is not available if you set the WAN type to **Ethernet** in the **Internet Access Setup** screen.

Note: This screen is not available when you use the P-791R v3 device.

Figure 34 Network > Internet (WAN) > WAN Backup



The following table describes the labels in this screen.

Table 19 Network > Internet (WAN) > WAN Backup

LABEL	DESCRIPTION
Backup Type	Select the method that the P-79X uses to check the DSL connection. Select **DSL Link** to have the P-79X check if the connection to the DSLAM is up. Select **ICMP** to have the P-79X periodically ping the IP addresses configured in the **Check WAN IP Address** fields.
Check WAN IP Address1-3	Configure this field to test your P-79X's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the P-79X periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your P-79X may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	When the P-79X is using a lower priority connection (usually a WAN backup connection), it periodically checks whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the P-79X to wait between checks. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds (3 recommended) for your P-79X to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** field before timing out the request. The WAN connection is considered "down" after the P-79X times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	Traffic redirect forwards traffic to a backup gateway when the P-79X cannot connect to the Internet.
Active Traffic Redirect	Select this check box to have the P-79X use traffic redirect if the normal WAN connection goes down. Note: If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the P-79X uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The P-79X automatically forwards traffic to this IP address if the P-79X's Internet connection terminates.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.5 WAN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

6.5.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The P-79X supports the following methods.

6.5.1.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **Gateway IP Address** field in the wizard or WAN screen. You can get this information from your ISP.

6.5.1.2 PPP over Ethernet

The P-79X supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The PPPoE option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

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

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

By implementing PPPoE directly on the P-79X (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the P-79X does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

6.5.1.3 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

6.5.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

6.5.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

6.5.4 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

IP Assignment with PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **Gateway IP Address** fields are not applicable (N/A). If you have a static IP, then you only need to fill in the **IP Address** field and not the **Gateway IP Address** field.

IP Assignment with RFC 1483 Encapsulation

In this case the IP address assignment must be static.

IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **Gateway IP Address** fields as supplied by your ISP. However for a dynamic IP, the P-79X acts as a DHCP client on the WAN port and so the **IP Address** and **Gateway IP Address** fields are not applicable (N/A) as the DHCP server assigns them to the P-79X.

6.5.5 Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The P-79X does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the P-79X will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

6.5.6 NAT

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

6.6 Metric

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

The metric sets the priority for the P-79X's routes to the Internet. If any two of the default routes have the same metric, the P-79X uses the following pre-defined priorities:

- Normal route: designated by the ISP (see Section 6.2 on page 46)
- Traffic-redirect route (see Section 6.7 on page 61)

For example, if the normal route has a of "1" and the traffic-redirect route has a metric of "2", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the P-79X tries the traffic-redirect route next.

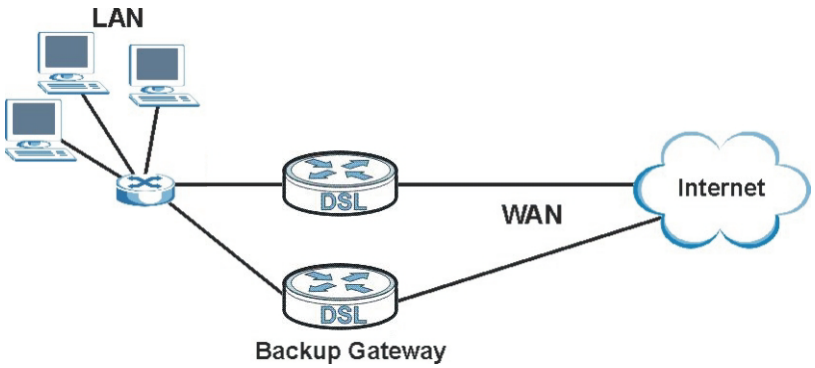
If you want the traffic-redirect route route to take priority over the normal route, all you need to do is set the traffic-redirect route's metric to "1" and the normal route to "2".

IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above.

6.7 Traffic Redirect

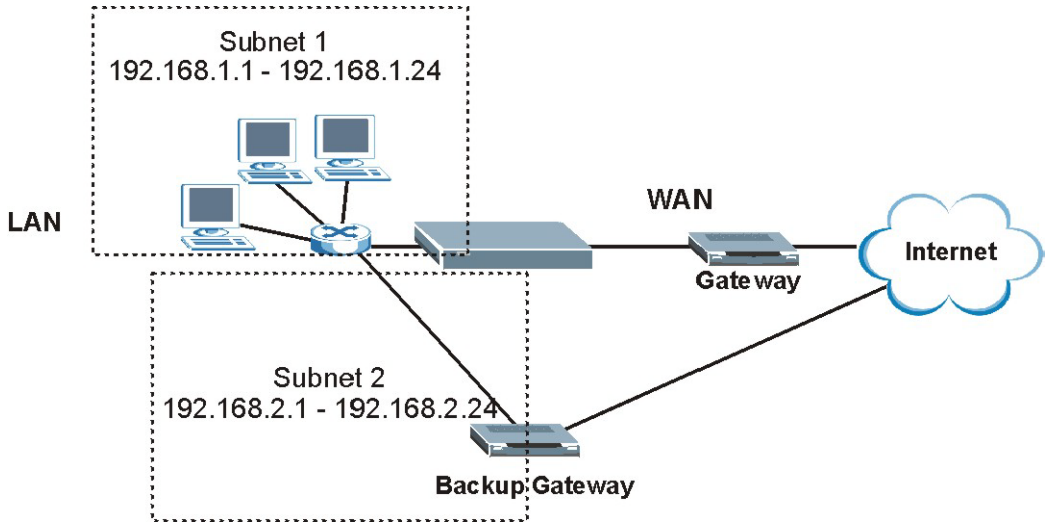
Traffic redirect forwards traffic to a backup gateway when the P-79X cannot connect to the Internet. An example is shown in the figure below.

Figure 35 Traffic Redirect Example



The following network topology allows you to avoid triangle route security issues when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the P-79X itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure filters that allow packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

Figure 36 Traffic Redirect LAN Setup



6.8 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

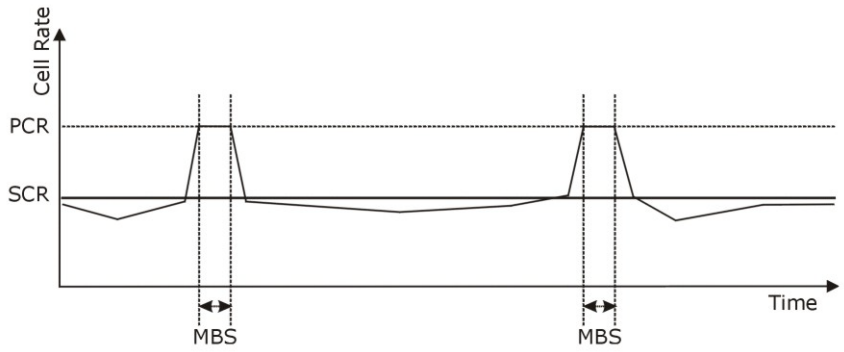
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 37 Example of Traffic Shaping



6.8.1 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

7

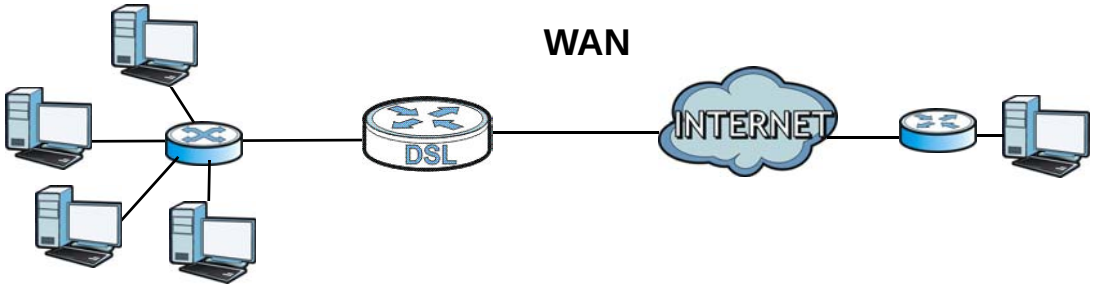
WWAN

7.1 Overview

This chapter discusses the P-79X's **WWAN** screens. Use these screens to configure your P-79X for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

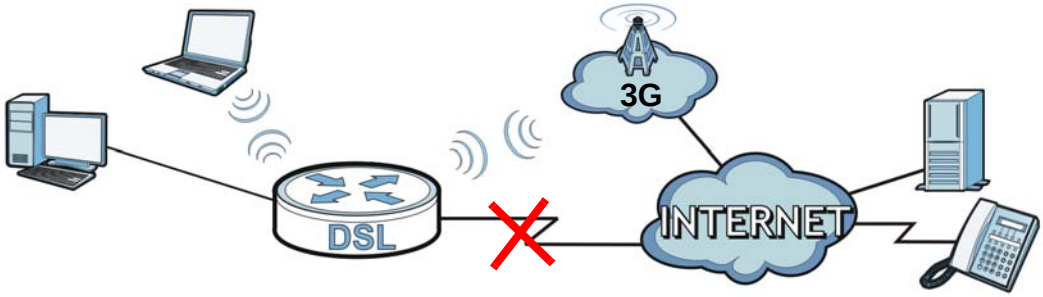
Figure 38 LAN and WAN



3G standards for the sending and receiving of voice, video, and data in a mobile environment.

You can attach a 3G wireless adapter to the USB port and set the P-79X to use this 3G connection as your WAN or a backup when the wired WAN connection fails.

Figure 39 3G WAN Connection



7.1.1 What You Can Do in this Chapter

- Use the **3G WAN Setup** screen to configure 3G WAN connection (Section 7.2 on page 67).

Table 20 WAN Setup Overview

LAYER-2 INTERFACE		INTERNET CONNECTION		
CONNECTION	**DSL LINK TYPE**	**MODE**	**ENCAPSULATION**	**CONNECTION SETTINGS**
ADSL/VDSL over PTM	N/A	Routing	PPPoE	PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
			IPoE	IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		Bridge	N/A	VLAN and QoS
ADSL over ATM	EoA	Routing	PPPoE	ATM PVC configuration, PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
			IPoE/IPoA	ATM PVC configuration, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		Bridge	N/A	ATM PVC configuration, and QoS
Ethernet	N/A	Routing	PPPoE	PPP user name and password, WAN IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
			IPoE	WAN IPv4/IPv6 IP address, NAT, DNS server and routing feature
		Bridge	N/A	VLAN and QoS
GbE	N/A	Routing	IPoE/PPPoE	PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		Bridge	N/A	VLAN and QoS
3G	N/A	Nailed Up	PPP/IPoE	Dial string, APN (Access Point Name), IP address, DNS server
		On Demand	PPP/IPoE	Dial string, APN, Maximum idle time out, DNS server, IP address

7.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the P-79X, which makes it accessible from an outside network. It is used by the P-79X to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the P-79X tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

ATM

Asynchronous Transfer Mode (ATM) is a WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC) between Finding Out More

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

7.1.3 Before You Begin

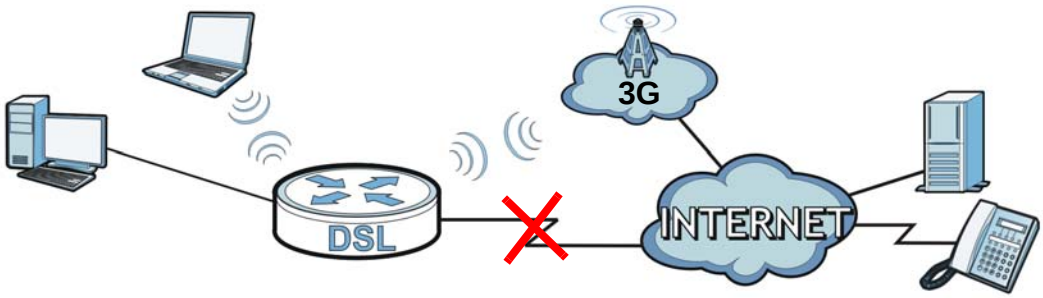
You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

7.2 The 3G WAN Setup Screen

The USB port (at the rear panel of the P-79X) allow you to attach a 3G dongle to wirelessly connect to a 3G network for Internet access. You can have the P-79X use the 3G WAN connection as a backup. Disconnect the DSL and Ethernet WAN ports to use the 3G dongle as your primary WAN connection. The P-79X automatically uses a wired WAN connection when available.

Note: This P-79X supports connecting one 3G dongle at a time.

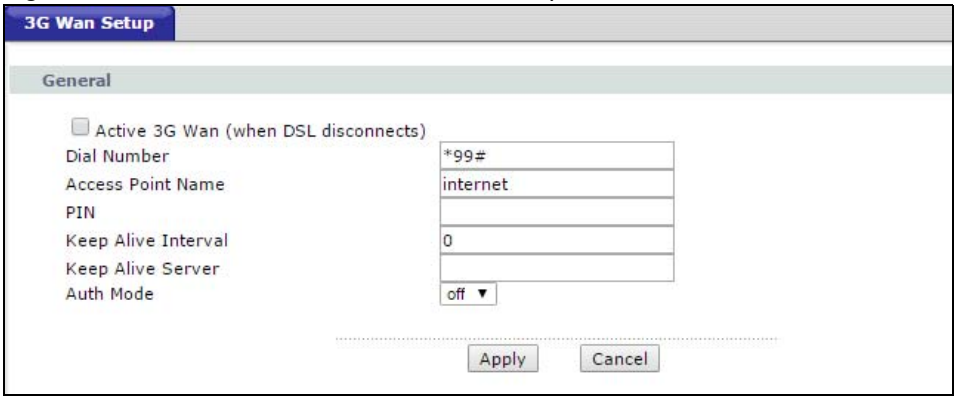
Figure 40 Internet Access Application: 3G WAN



Use this screen to configure your 3G settings. Click **Network > WWAN > 3G WAN Setup**.

Note: The actual data rate you obtain varies depending the 3G card you use, the signal strength to the service provider's base station, and so on.

Figure 41 Network > WWAN > 3G WAN Setup



The following table describes the labels in this screen.

Table 21 Network Setting > WWAN > 3G Backup

LABEL	DESCRIPTION
General	
Active 3G WAN	Select this check box to have the P-79X use the 3G connection as your WAN or a backup when the wired WAN connection fails.
Dial Number	Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number. For example, *99# is the dial string to establish a GPRS or 3G connection in Taiwan.
Access Point Name	Enter the Access Point Name (APN) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 32 ASCII printable characters. Spaces are allowed.

Table 21 Network Setting > WWAN > 3G Backup (continued)

LABEL	DESCRIPTION
PIN	A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card. If your ISP enabled PIN code authentication, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, leave this field blank.
Keep Alive Interval	Specify the time interval (in minutes) for checking whether the 3G connection is valid or not.
Keep Alive Server	Specify the DNS server address for checking the 3G connection status.
Auth Mode	Select **On** to enable the authentication. Otherwise, select **Off**.
Username	This is available only when you select **On** in the **Auth Mode** field. Type the user name (of up to 64 ASCII printable characters) given to you by your service provider.
Password	This is available only when you select **On** in the **Auth Mode** field. Type the password (of up to 64 ASCII printable characters) associated with the user name above.
Apply	Click **Apply** to save your changes back to the P-79X.
Cancel	Click **Cancel** to return to the previous configuration.

7.3 Technical Reference

The following section contains additional technical information about the P-79X features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The P-79X can work in bridge mode or routing mode. When the P-79X is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

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

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

By implementing PPPoE directly on the P-79X (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the P-79X does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

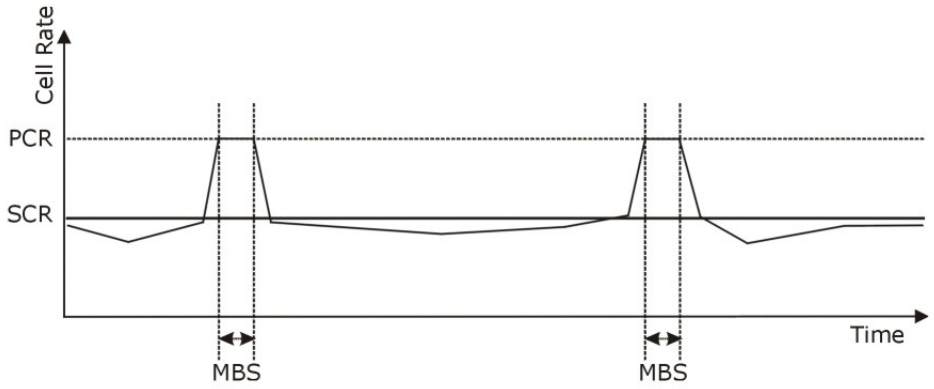
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 42 Example of Traffic Shaping



ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the

4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

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

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

At start up, the P-79X queries all directly connected networks to gather group membership. After that, the P-79X periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The P-79X can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the P-79X's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

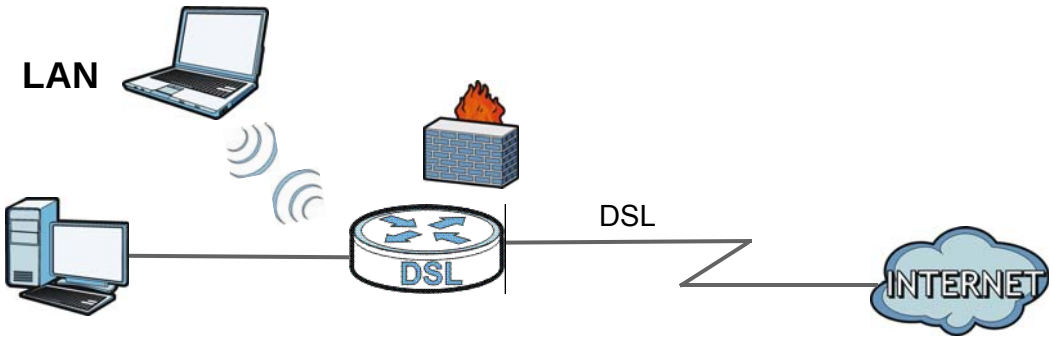
8

LAN Setup

8.1 Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one immediate area such as a building or floor of a building.

Use the LAN screens to help you configure a LAN DHCP server and manage IP addresses.



8.1.1 What You Can Do in the LAN Screens

- Use the **IP** screen (Section 8.2 on page 75) to set the LAN IP address and subnet mask of your ZyXEL device. You can also edit your P-79X's RIP, multicast, any IP and Windows Networking settings from this screen.
- Use the **DHCP Setup** screen (Section 8.3 on page 78) to configure the ZyXEL Device's DHCP settings.
- Use the **Client List** screen (Section 8.4 on page 80) to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.
- Use the **IP Alias** screen (Section 8.5 on page 81) to change your P-79X's IP alias settings.

8.1.2 What You Need To Know About LAN

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your P-79X an IP address, subnet mask, DNS and other routing information when it's turned on.

RIP

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.

Multicast

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

IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 and 3 are improvements over version 1, but IGMP version 1 is still in wide use.

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a networking device before you can access it.

Finding Out More

See Section 8.6 on page 83 for technical background information on LANs.

8.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

8.2 The IP Screen

Use this screen to set the Local Area Network IP address and subnet mask of your P-79X. Click **Network > LAN** to open the **IP** screen.

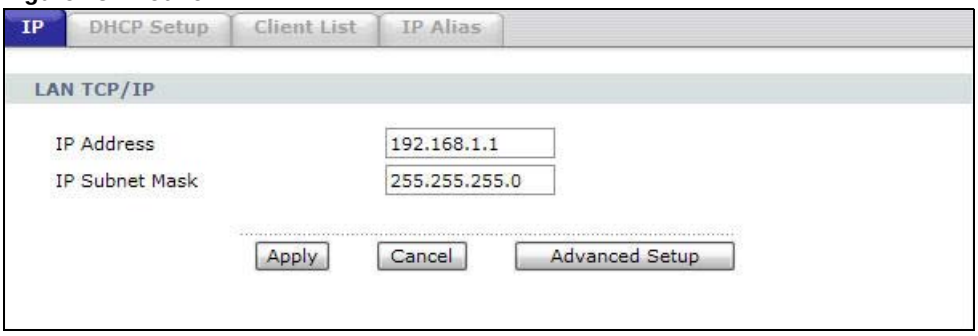
Follow these steps to configure your LAN settings.

1 Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your P-79X.

2 Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.

3 Click **Apply** to save your settings.

Figure 43 Network > LAN > IP



The following table describes the fields in this screen.

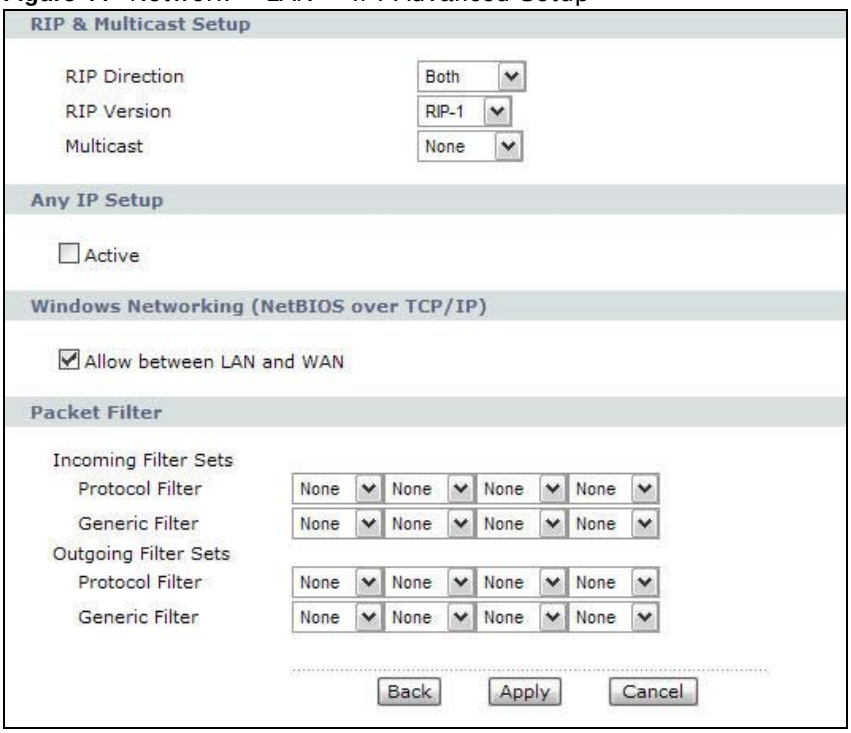
Table 22 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Enter the LAN IP address you want to assign to your P-79X in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your P-79X automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the **Advanced LAN Setup** screen and edit more details of your LAN setup.

8.2.1 The Advanced LAN IP Setup Screen

Use this screen to edit your P-79X's RIP, multicast, Any IP and Windows Networking settings. Click the **Advanced Setup** button in the **LAN IP** screen. The screen appears as shown.

Figure 44 Network > LAN > IP: Advanced Setup



The following table describes the labels in this screen.

Table 23 Network > LAN > IP: Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from **None**and **Both**.
RIP Version	Select the RIP version from **RIP-1**and **RIP-2**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The P-79X supports **IGMP-v1**, **IGMP-v2, IGMP-v3** and **IGMP-all**. Select **None** to disable it.
Any IP Setup	
Active	Select the **Active** check box to enable the Any IP feature. This allows a computer to access the Internet via the P-79X without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the P-79X are not in the same subnet. When you disable the Any IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the P-79X's LAN IP address can connect to the P-79X or access the Internet through the P-79X. Note: You must enable NAT/SUA in the **NAT** screen to use the Any IP feature on the P-79X
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.

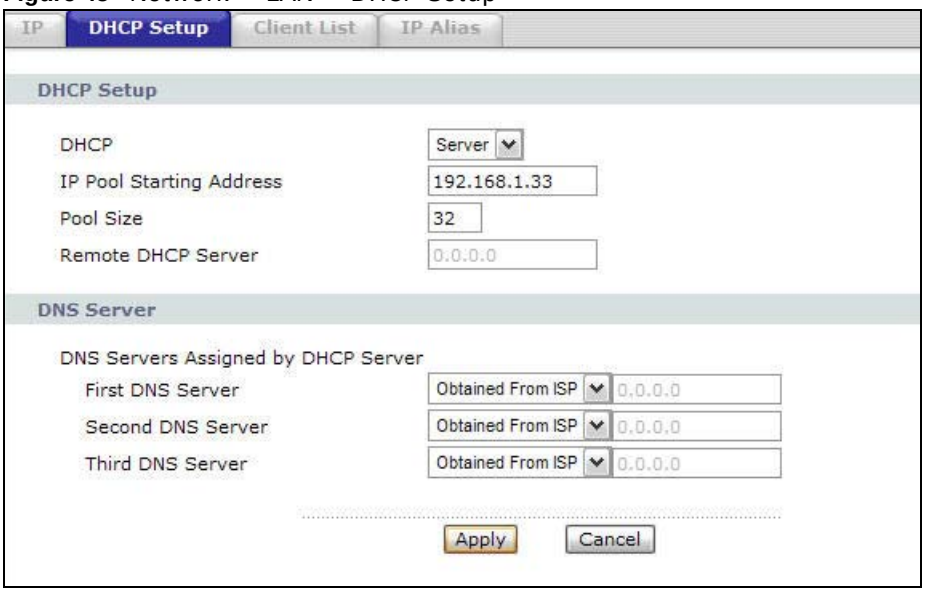
Table 23 Network > LAN > IP: Advanced Setup

LABEL	DESCRIPTION
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Packet Filter	
Incoming Filter Sets	
Protocol Filter	Select the protocol filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure packet filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.
Generic Filter	Select the generic filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.
Outgoing Filter Sets	
Protocol Filter	Select the protocol filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure protocol filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.
Generic Filter	Select the generic filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 12 on page 119 for more details.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

8.3 The DHCP Setup Screen

Use this screen to configure the DNS server information that the P-79X sends to the DHCP client devices on the LAN. Click **Network > DHCP Setup** to open this screen.

Figure 45 Network > LAN > DHCP Setup



The following table describes the labels in this screen.

Table 24 Network > LAN > DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
DHCP	If set to **Server**, your P-79X can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the P-79X acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** field in this case. When DHCP is used, the following items need to be set:
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.
DNS Server	
DNS Servers Assigned by DHCP Server	The P-79X passes a DNS (Domain Name System) server IP address to the DHCP clients.

Table 24 Network > LAN > DHCP Setup

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the P-79X's WAN IP address). Select **UserDefined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **UserDefined**, but leave the IP address set to 0.0.0.0, **UserDefined** changes to **None** after you click **Apply**. If you set a second choice to **UserDefined**, and enter the same IP address, the second **UserDefined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the P-79X act as a DNS proxy only when the ISP uses IPCP DNS server extensions. The P-79X's LAN IP address displays in the field to the right (read-only). The P-79X tells the DHCP clients on the LAN that the P-79X itself is the DNS server. When a computer on the LAN sends a DNS query to the P-79X, the P-79X forwards the query to the real DNS server learned through IPCP and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

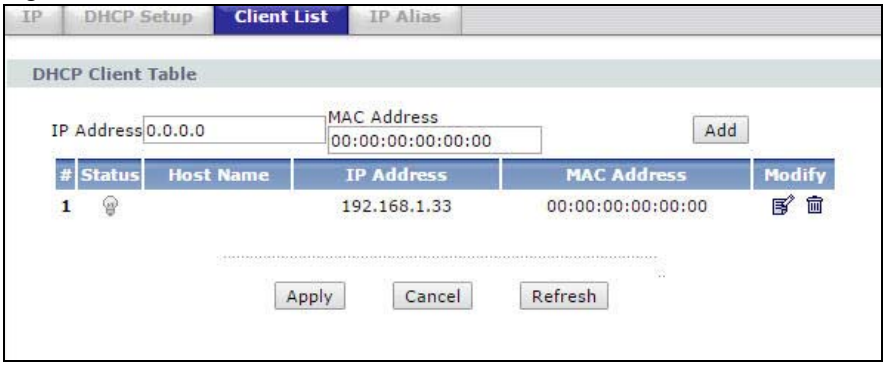
8.4 The Client List Screen

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

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

Use this screen to change your P-79X's static DHCP settings. Click **Network > LAN > Client List** to open the following screen.

Figure 46 Network > LAN > Client List



The following table describes the labels in this screen.

Table 25 Network > LAN > Client List

LABEL	DESCRIPTION
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click this to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the P-79X.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Modify	Click the modify icon to have the IP address field editable and change it.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Refresh	Click this to reload the DHCP table.

8.5 The IP Alias Screen

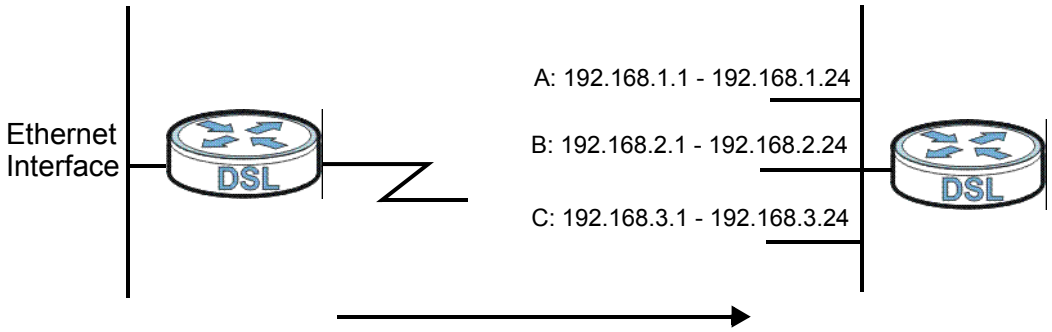
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The P-79X supports three logical LAN interfaces via its single physical Ethernet interface with the P-79X itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

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

The following figure shows a LAN divided into subnets A, B, and C.

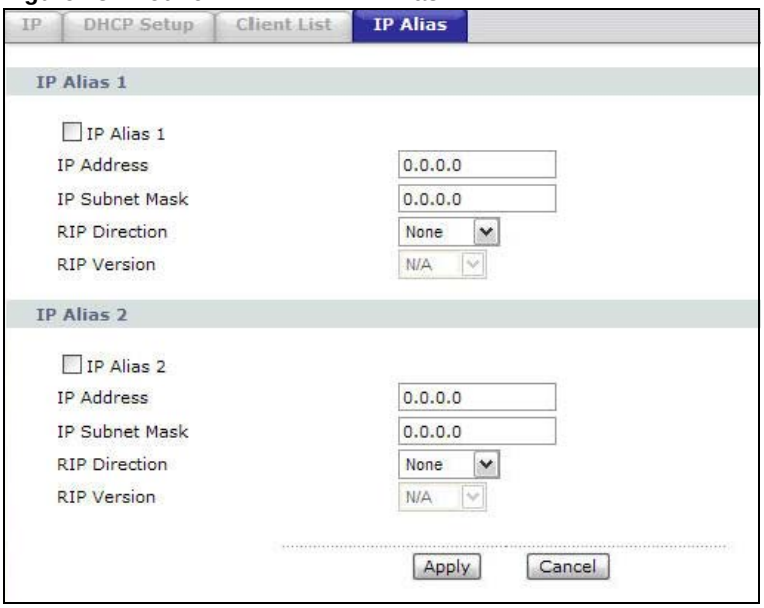
Figure 47 Physical Network & Partitioned Logical Networks



8.5.1 Configuring the LAN IP Alias Screen

Use this screen to change your P-79X's IP alias settings. Click **Network** > **LAN** > **IP Alias** to open the following screen.

Figure 48 Network > LAN > IP Alias



The following table describes the labels in this screen.

Table 26 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1, 2	Select the check box to configure another LAN network for the P-79X.
IP Address	Enter the IP address of your P-79X in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your P-79X will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the P-79X.
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both / In Only / Out Only / None**. When set to **Both** or **Out Only**, the P-79X will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the P-79X sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

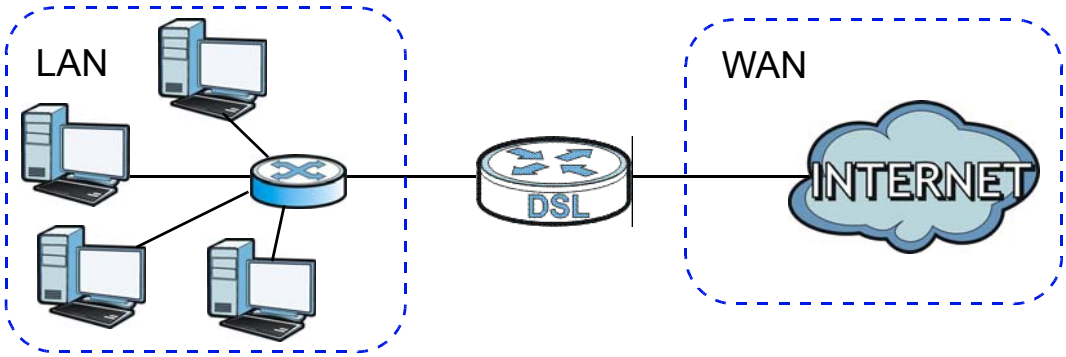
8.6 LAN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

8.6.1 LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the P-79X ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 49 LAN and WAN IP Addresses



8.6.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the P-79X as a DHCP server or disable it. When configured as a server, the P-79X provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The P-79X is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

8.6.3 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

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

- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The P-79X supports the IPCP DNS server extensions through the DNS proxy feature.

  If the **DNS Server** fields in the **DHCP Setup** screen are set to **DNS Relay**, the P-79X tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the P-79X, the P-79X acts as a DNS proxy and forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

  Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

8.6.4 LAN TCP/IP

The P-79X has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the P-79X. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your P-79X, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your P-79X will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the P-79X unless you are instructed to do otherwise.

Private IP Addresses

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

- 10.0.0.0 — 10.255.255.255

- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

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

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

8.6.5 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both -** the P-79X will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only -** the P-79X will not send any RIP packets but will accept all RIP packets received.
- **Out Only -** the P-79X will send out RIP packets but will not accept any RIP packets received.
- **None -** the P-79X will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the P-79X sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.

8.6.6 Multicast

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

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. IGMP version 3 supports source filtering, reporting or ignoring traffic from specific source address to a particular host on the network. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The P-79X supports IGMP version 1 (**IGMP-v1**), IGMP version 2 (**IGMP-v2**) and IGMP version 3 (**IGMP-v3**). At start up, the P-79X queries all directly connected networks to gather group membership. After that, the P-79X periodically updates this information. IP multicasting can be enabled/disabled on the P-79X LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

9

Network Address Translation (NAT)

9.1 Overview

This chapter discusses how to configure NAT on the P-79X. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

9.1.1 What You Can Do in the NAT Screens

- Use the **General** screen (Section 9.2 on page 88) to configure the NAT setup settings.
- Use the **Port Forwarding** screen (Section 9.3 on page 89) to configure forward incoming service requests to the server(s) on your local network.
- Use the **Address Mapping** screen (Section 9.4 on page 92) to change your P-79X's address mapping settings.
- Use the **ALG** screen (Section 9.5 on page 94) to enable and disable the SIP (VoIP) ALG in the P-79X.

9.1.2 What You Need To Know About NAT

Inside/Outside

Inside/outside denotes where a host is located relative to the P-79X, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

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

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

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

SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The P-79X also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in Table 34 on page 98.

- Choose **SUA Only** if you have just one public WAN IP address for your P-79X.
- Choose **Full Feature** if you have multiple public WAN IP addresses for your P-79X.

Finding Out More

See Section 9.6 on page 95 for advanced technical information on NAT.

9.2 The NAT General Setup Screen

Use this screen to activate NAT. Click **Network > NAT** to open the following screen.

Note: You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the P-79X.

Figure 50 Network > NAT > General

The following table describes the labels in this screen.

Table 27 Network > NAT > General

LABEL	DESCRIPTION
Active Network Address Translation (NAT)	Select this check box to enable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your P-79X.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your P-79X.

Table 27 Network > NAT > General (continued)

LABEL	DESCRIPTION
Max NAT/Firewall Session Per User	When computers use peer to peer applications, such as file sharing applications, they need to establish NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/Firewall sessions client computers can establish through the P-79X. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is exhausting all of the available NAT sessions.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.3 The Port Forwarding Screen

Note: This screen is available only when you select **SUA only** in the **NAT > General** screen.

Use this screen to forward incoming service requests to the server(s) on your local network.

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

The most often used port numbers and services are shown in Appendix F on page 279. Please refer to RFC 1700 for further information about port numbers.

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

Default Server IP Address

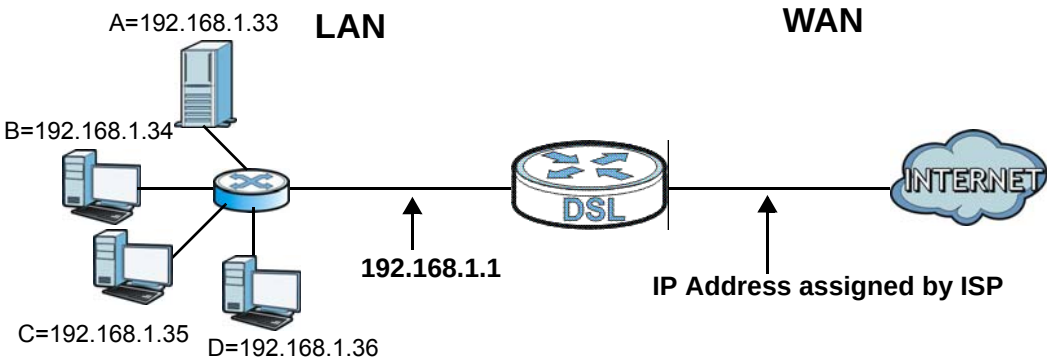
In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

Note: If you do not assign a **Default Server** IP address, the P-79X discards all packets received for ports that are not specified here or in the remote management setup.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 51 Multiple Servers Behind NAT Example

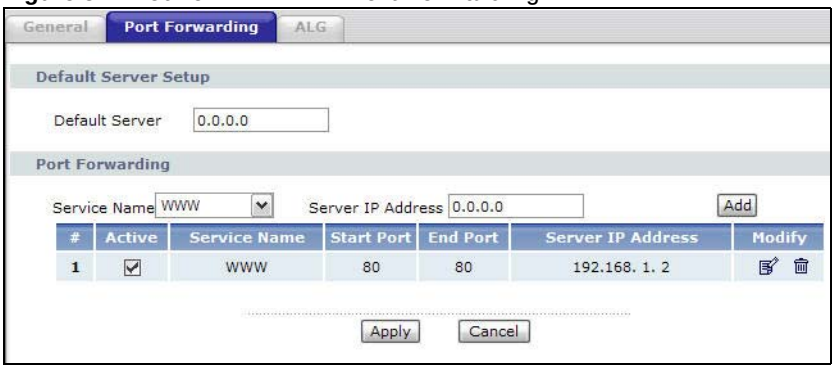


9.3.1 Configuring the Port Forwarding Screen

Click **Network > NAT > Port Forwarding** to open the following screen.

See Appendix F on page 279 for port numbers commonly used for particular services.

Figure 52 Network > NAT > Port Forwarding



The following table describes the fields in this screen.

Table 28 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a **Default Server** IP address, the P-79X discards all packets received for ports that are not specified here or in the remote management setup.
Port Forwarding	
Service Name	Select a service from the drop-down list box.

Table 28 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Server IP Address	Enter the IP address of the server for the specified service.
Add	Click this button to add a rule to the table below.
#	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	This is a service's name.
Start Port	This is the first port number that identifies a service.
End Port	This is the last port number that identifies a service.
Server IP Address	This is the server's IP address.
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule. Click the delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.3.2 The Port Forwarding Rule Edit Screen

Use this screen to edit a port forwarding rule. Click the rule's edit icon in the **Port Forwarding** screen to display the screen shown next.

Figure 53 Network > NAT > Port Forwarding: Edit

The following table describes the fields in this screen.

Table 29 Network > NAT > Port Forwarding: Edit

LABEL	DESCRIPTION
Active	Click this check box to enable the rule.
Service Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port** field.

Table 29 Network > NAT > Port Forwarding: Edit (continued)

LABEL	DESCRIPTION
End Port	Enter a port number in this field. To forward only one port, enter the port number again in the **Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above.
Server IP Address	Enter the inside IP address of the server here.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.

9.4 The Address Mapping Screen

Note: The **Address Mapping** screen is available only when you select **Full Feature** in the **NAT > General** screen.

Ordering your rules is important because the P-79X applies the rules in the order that you specify. When a rule matches the current packet, the P-79X takes the corresponding action and the remaining rules are ignored. To change your P-79X's address mapping settings, click **Network > NAT > Address Mapping** to open the following screen.

Figure 54 Network > NAT > Address Mapping

The following table describes the fields in this screen.

Table 30 Network > NAT > Address Mapping

LABEL	DESCRIPTION
#	This is the rule index number.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types.

Table 30 Network > NAT > Address Mapping (continued)

LABEL	DESCRIPTION
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types.
Type	**1-1**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **M-1**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. **M-M Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **MM No** (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

9.4.1 The Address Mapping Rule Edit Screen

Use this screen to edit an address mapping rule. Click the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 55 Network > NAT > Address Mapping: Edit

The following table describes the fields in this screen.

Table 31 Network > NAT > Address Mapping: Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **Many-to-Many No Overload**: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Server Mapping Set	Only available when **Type** is set to **Server**. Select a number from the drop-down menu to choose a port forwarding set.
Edit Details	Click this link to go to the **Port Forwarding** screen to edit a port forwarding set that you have selected in the **Server Mapping Set** field.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.5 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the P-79X registers with the SIP register server, the SIP ALG translates the P-79X's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your P-79X is behind a SIP ALG.

Use this screen to enable and disable the SIP (VoIP) ALG in the P-79X. To access this screen, click **Network > NAT > ALG**.

Figure 56 Network > NAT > ALG

The following table describes the fields in this screen.

Table 32 Network > NAT > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Select this to change the private ports or IP in SIP messages so that the VoIP client behind the P-79X can be found in RTP traffic.
Apply	Click this to save your changes.
Reset	Click this to restore your previously saved settings.

9.6 NAT Technical Reference

This chapter contains more information regarding NAT.

9.6.1 NAT Definitions

Inside/outside denotes where a host is located relative to the P-79X, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

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

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

Table 33 NAT Definitions

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

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

9.6.2 What NAT Does

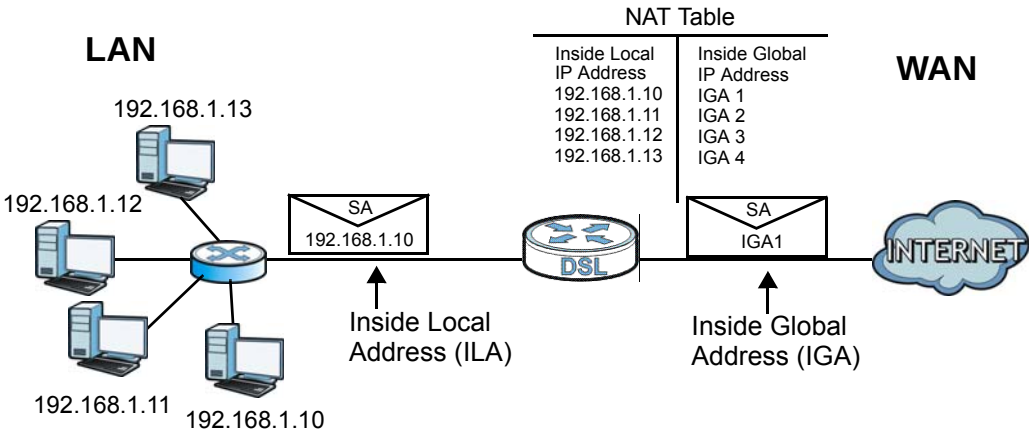
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see Table 34 on page 98), NAT offers the additional benefit of firewall protection. With no servers defined, your P-79X filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

9.6.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The P-79X keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

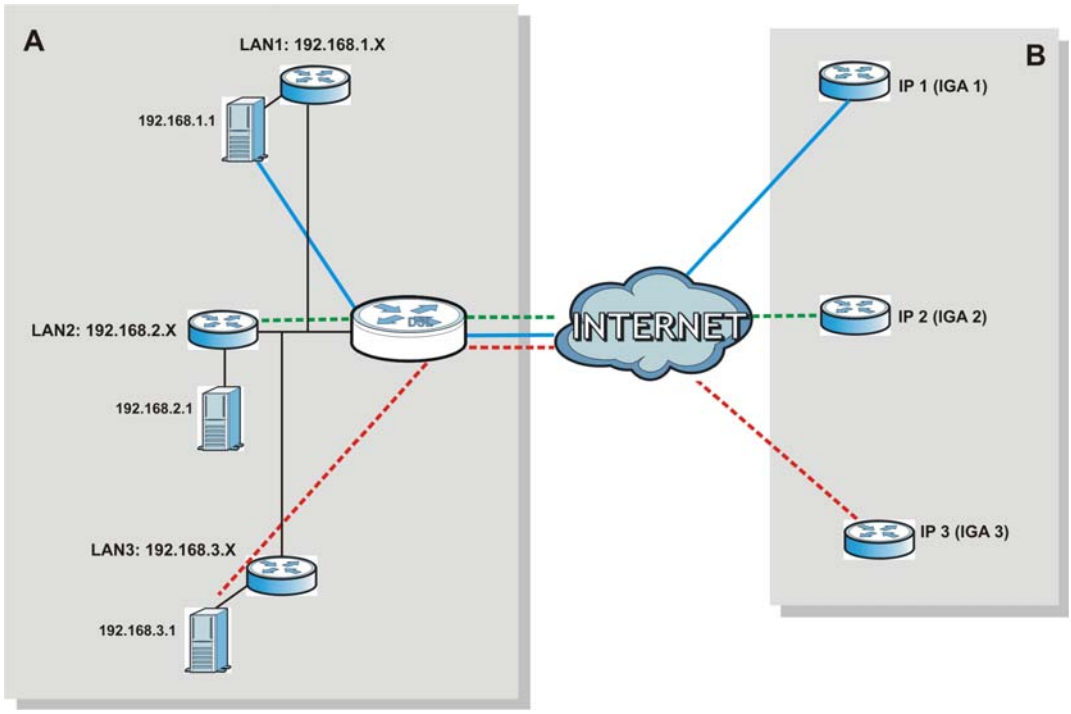
Figure 57 How NAT Works



9.6.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the P-79X can communicate with three distinct WAN networks.

Figure 58 NAT Application With IP Alias



9.6.5 NAT Mapping Types

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

- **One to One**: In One-to-One mode, the P-79X maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the P-79X maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
- **Many to Many Overload**: In Many-to-Many Overload mode, the P-79X maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the P-79X maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do NOT change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

Table 34 NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1←→ IGA1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 ...
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 ...
Many-to-Many No Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 ...
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1

10

Firewalls

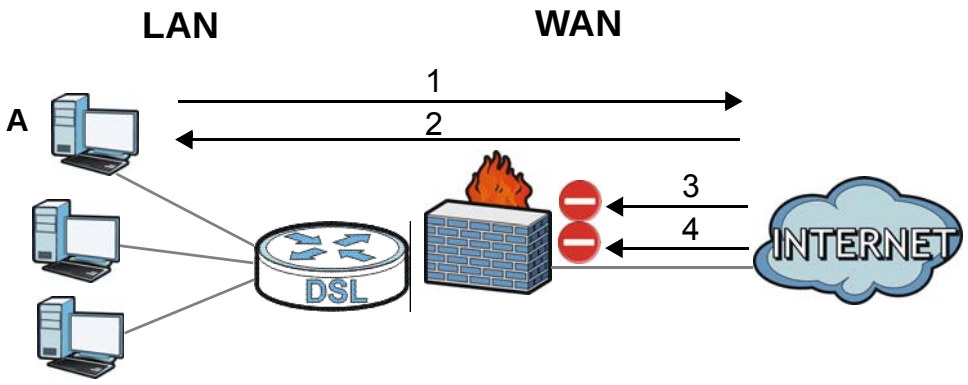
10.1 Overview

This chapter shows you how to enable and configure the P-79X firewall. Use these screens to enable and configure the firewall that protects your P-79X and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 59 Default Firewall Action



10.1.1 What You Can Do in the Firewall Screens

- Use the **General** screen (Section 10.2 on page 103) to enable firewall on the P-79X, and set the default action that the firewall takes on packets that do not match any of the firewall rules.
- Use the **Rules** screen (Section 10.3 on page 104) to view the configured firewall rules and add, edit or remove a firewall rule.
- Use the **Threshold** screen (Section 10.4 on page 107) to set the thresholds that the P-79X uses to determine when to start dropping sessions that do not become fully established (half-open sessions).

10.1.2 What You Need to Know About Firewall

DoS

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

Anti-Probing

If an outside user attempts to probe an unsupported port on your P-79X, an ICMP response packet is automatically returned. This allows the outside user to know the P-79X exists. The P-79X supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your P-79X when unsupported ports are probed.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

DoS Thresholds

For DoS attacks, the P-79X uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions. You can use the default threshold values, or you can change them to values more suitable to your security requirements.

Finding Out More

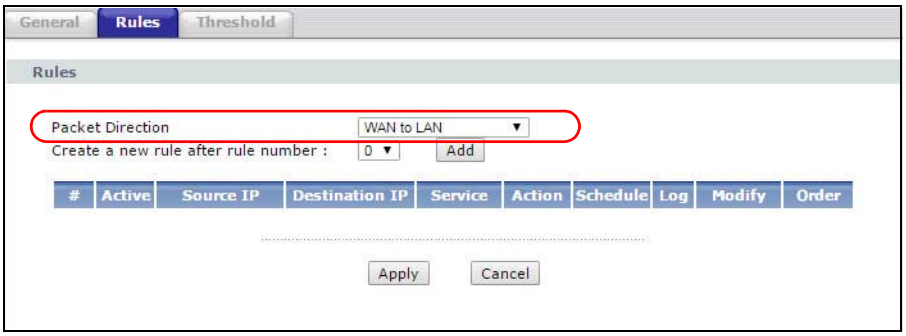
- See Section 10.1.3 on page 100 for an example of setting up a firewall.
- See Section 10.5 on page 110 for advanced technical information on firewall.

10.1.3 Firewall Rule Setup Example

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

1 Click **Security > Firewall** > **Rules**.

2 Select **WAN to LAN** in the **Packet Direction** field.

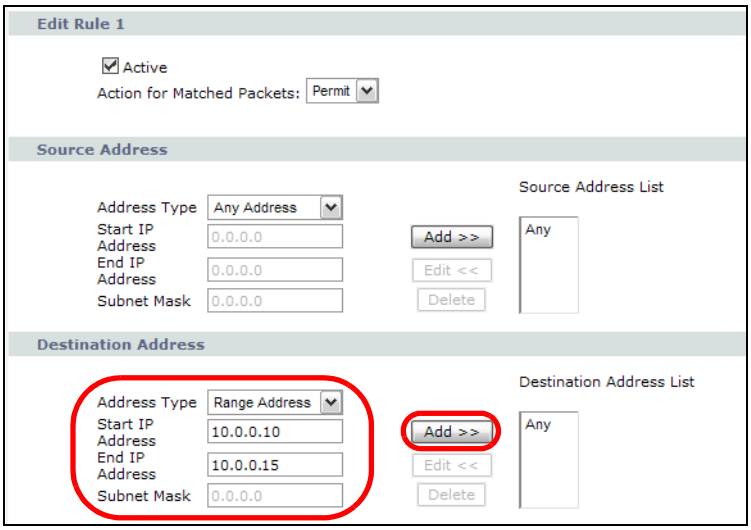


3 In the **Rules** screen, select the index number after that you want to add the rule. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.

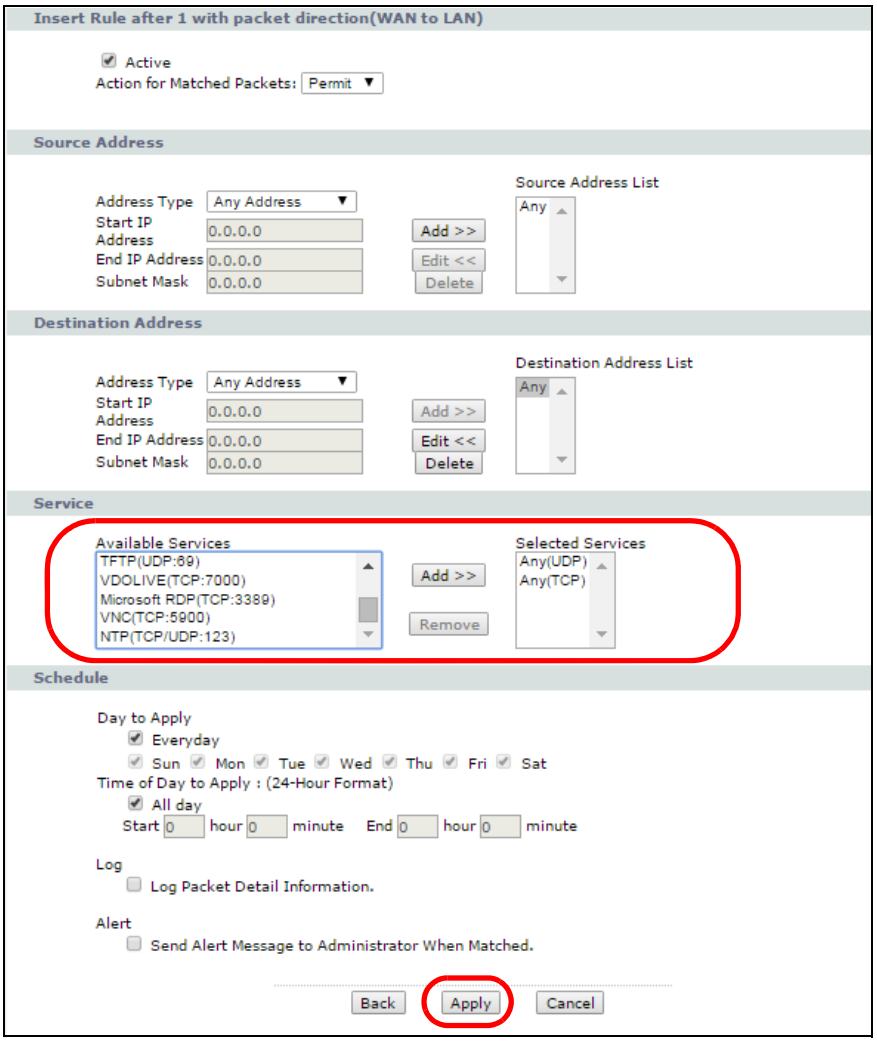
4 Click **Add** to display the firewall rule configuration screen.

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

6 Configure the destination address screen as follows and click **Add**.

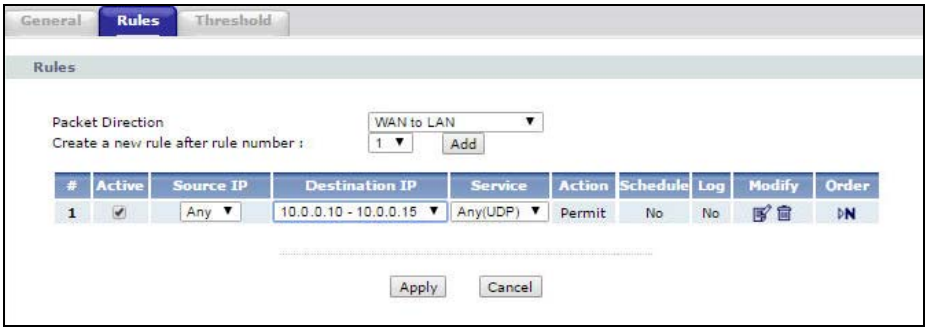


7 Use the **Add >>** and **Remove** buttons between **Available Services** and **Selected Services** list boxes to configure it as follows. Click **Apply** when you are done.



On completing the configuration procedure for this Internet firewall rule, the **Rules** screen should look like the following.

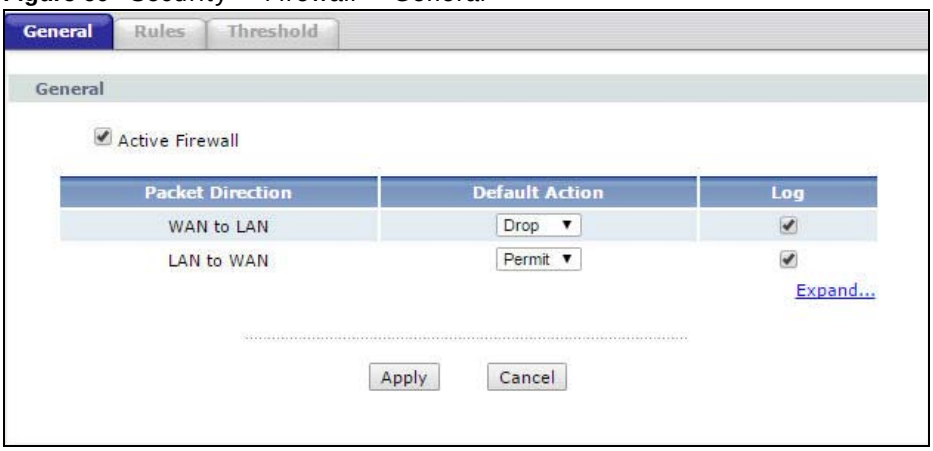
Rule 1 allows a connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.



10.2 The Firewall General Screen

Use this screen to configure the firewall settings. Click **Security > Firewall** to display the following screen.

Figure 60 Security > Firewall > General



The following table describes the labels in this screen.

Table 35 Security > Firewall > General

LABEL	DESCRIPTION
Active Firewall	Select this check box to activate the firewall. The P-79X performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Packet Direction	This is the direction of travel of packets (**LAN to LAN / Router**, **LAN to WAN**, **WAN to WAN / Router**, **WAN to LAN)**. Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, **LAN to LAN / Router** means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the P-79X or the P-79X itself.
Default Action	Use the drop-down list boxes to select the default action that the firewall is to take on packets that are traveling in the selected direction and do not match any of the firewall rules. Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select **Permit** to allow the passage of the packets.
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules.
Expand...	Click this to display more information.
Basic...	Click this to display less information.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

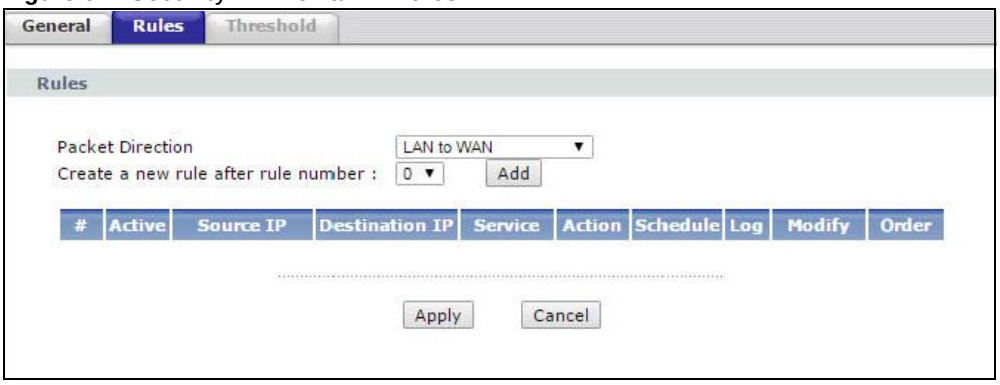
10.3 The Firewall Rule Screen

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

Refer to Section 10.5 on page 110 for more information.

Click **Security > Firewall > Rules** to bring up the following screen. This screen displays a list of the configured firewall rules. Note the order in which the rules are listed.

Figure 61 Security > Firewall > Rules



The following table describes the labels in this screen.

Table 36 Security > Firewall > Rules

LABEL	DESCRIPTION
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Create a new rule after rule number	Select an index number and click **Add** to add a new firewall rule after the selected index number. For example, if you select “6”, your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the **General** screen.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This field displays whether a firewall is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Destination IP	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Service	This drop-down list box displays the services to which this firewall rule applies. See Appendix F on page 279 for more information.
Action	This field displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**) or allows the passage of packets (**Permit**).
Schedule	This field tells you whether a schedule is specified (**Yes**) or not (**No**).

Table 36 Security > Firewall > Rules (continued)

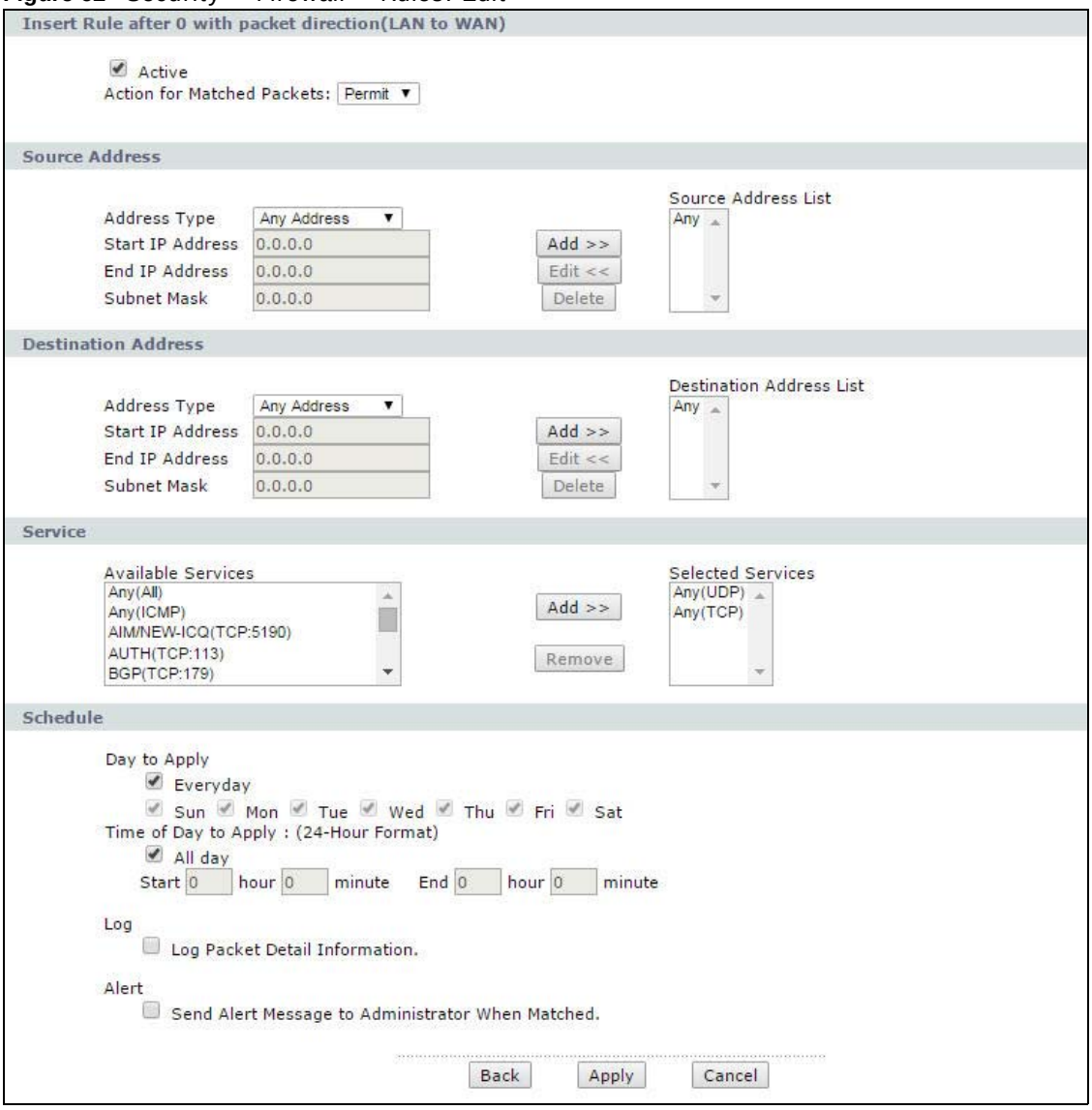
LABEL	DESCRIPTION
Log	This field shows you whether a log is created when packets match this rule (**Yes**) or not (**No**).
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Order	Click the Move icon to display the **Move the rule to** field. Type a number in the **Move the rule to** field and click the **Move** button to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

10.3.1 Configuring Firewall Rules

Refer to Section 10.1.2 on page 100 for more information.

Use this screen to configure firewall rules. In the **Rules** screen, select an index number and click **Add** or click a rule's **Edit** icon to display this screen and refer to the following table for information on the labels.

Figure 62 Security > Firewall > Rules: Edit



The following table describes the labels in this screen.

Table 37 Security > Firewall > Rules: Edit

LABEL	DESCRIPTION
Edit Rule	
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the drop-down list box to select whether to discard (**Drop**), deny and send an ICMP destination-unreachable message to the sender of (**Reject**) or allow the passage of (**Permit**) packets that match this rule.
Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for instance, 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here.

Table 37 Security > Firewall > Rules: Edit (continued)

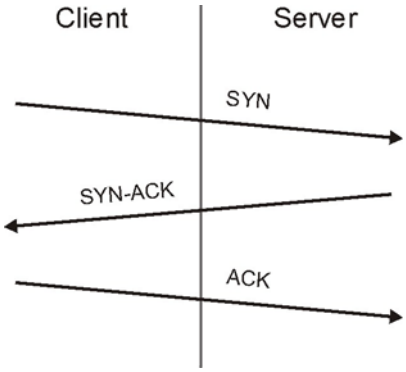
LABEL	DESCRIPTION
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add >>	Click **Add >>** to add a new address to the **Source** or **Destination Address** box. You can add multiple addresses, ranges of addresses, and/or subnets.
Edit <<	To edit an existing source or destination address, select it from the box and click **Edit <<**.
Delete	Highlight an existing source or destination address from the **Source** or **Destination Address** box above and click **Delete** to remove it.
Services	
Available/ Selected Services	Please see Appendix F on page 279 for more information on services available. Highlight a service from the **Available Services** box on the left, then click **Add >>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **Remove**.
Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select **All Day** or enter the start and end times in the hour-minute format to apply the rule.
Log	
Log Packet Detail Information	This field determines if a log for packets that match the rule is created or not. Go to the **Log Settings** page and select the **Access Control** logs category to have the P-79X record these logs.
Alert	
Send Alert Message to Administrator When Matched	Select the check box to have the P-79X generate an alert when the rule is matched.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

10.4 The Firewall Threshold Screen

For DoS attacks, the P-79X uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all sessions.

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed. Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

Figure 63 Three-Way Handshake



For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DOS attack.

10.4.1 Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you believe the P-79X has been receiving DoS attacks that are not recorded in the logs or the logs show that the P-79X is classifying normal traffic as DoS attacks. Factors influencing choices for threshold values are:

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

Reduce the threshold values if your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy).

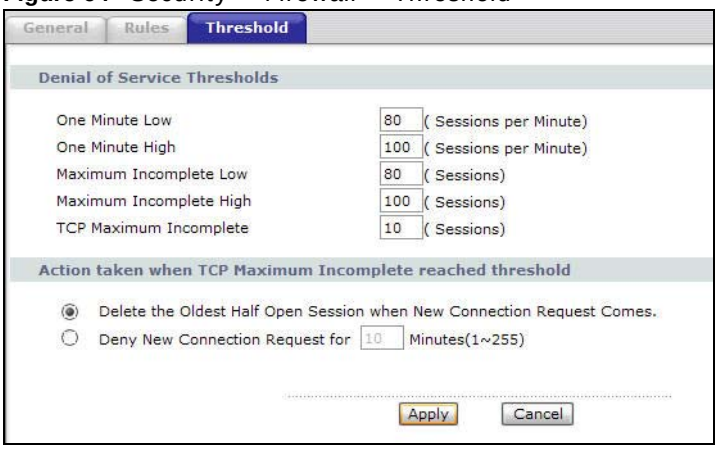
- If you often use P2P applications such as file sharing with eMule or eDonkey, it's recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the P-79X may classify them as DoS attacks.

10.4.2 Configuring Firewall Thresholds

The P-79X also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections.

Click **Firewall** > **Threshold** to bring up the next screen.

Figure 64 Security > Firewall > Threshold



The following table describes the labels in this screen.

Table 38 Security > Firewall > Threshold

LABEL	DESCRIPTION
Denial of Service Thresholds	The P-79X measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.
One Minute Low	This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The P-79X continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.
One Minute High	This is the rate of new half-open sessions per minute that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the P-79X deletes half-open sessions as required to accommodate new connection attempts. For example, if you set the one minute high to 100, the P-79X starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The P-79X continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the P-79X deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number. For example, if you set the maximum incomplete high to 100, the P-79X starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low.

Table 38 Security > Firewall > Threshold (continued)

LABEL	DESCRIPTION
TCP Maximum Incomplete	An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host. Specify the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth. The P-79X sends alerts whenever the **TCP Maximum Incomplete** is exceeded.
Action taken when TCP Maximum Incomplete reached threshold	Select the action that P-79X should take when the TCP maximum incomplete threshold is reached. You can have the P-79X either: Delete the oldest half open session when a new connection request comes. or Deny new connection requests for the number of minutes that you specify (between 1 and 255).
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

10.5 Firewall Technical Reference

This section provides some technical background information about the topics covered in this chapter.

10.5.1 Firewall Rules Overview

Your customized rules take precedence and override the P-79X's default settings. The P-79X checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the P-79X takes the action specified in the rule.

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

- LAN to LAN/ Router
- LAN to WAN
- WAN to LAN
- WAN to WAN/ Router

By default, the P-79X's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ Router

  These rules specify which computers on the LAN can manage the P-79X (remote management) and communicate between networks or subnets connected to the LAN interface (IP alias).

Note: You can also configure the remote management settings to allow only a specific computer to manage the P-79X.

- LAN to WAN

  These rules specify which computers on the LAN can access which computers or services on the WAN.

By default, the P-79X's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN

  These rules specify which computers on the WAN can access which computers or services on the LAN.

Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

- WAN to WAN/ Router

  By default the P-79X stops computers on the WAN from managing the P-79X or using the P-79X as a gateway to communicate with other computers on the WAN. You could configure one of these rules to allow a WAN computer to manage the P-79X.

Note: You also need to configure the remote management settings to allow a WAN computer to manage the P-79X.

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

For example, you may create rules to:

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

These custom rules work by comparing the source IP address, destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the P-79X's default rules.

10.5.2 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way.
3. Limit who can access your router.
4. Don't enable any local service (such as telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

6 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

10.5.3 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the P-79X and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?

2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.

4 Does this rule conflict with any existing rules?

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

11

URL Blocking

11.1 Overview

Internet content filtering allows you to block web sites based on keywords in the URL.

See Section 11.1.4 on page 113 for an example of setting up content filtering.

11.1.1 What You Can Do in the URL Blocking Screens

- Use the **Keyword** screen (Section 11.2 on page 115) to block web sites based on a keyword in the URL.
- Use the **Schedule** screen (Section 11.3 on page 116) to specify the days and times keyword blocking is active.
- Use the **Trusted** screen (Section 11.4 on page 117) to exclude computers and other devices on your LAN from the keyword blocking filter.

11.1.2 What You Need to Know About URL Blocking

URL

The URL (Uniform Resource Locator) identifies and helps locates resources on a network. On the Internet the URL is the web address that you type in the address bar of your Internet browser, for example “http://www.zyxel.com”.

11.1.3 Before You Begin

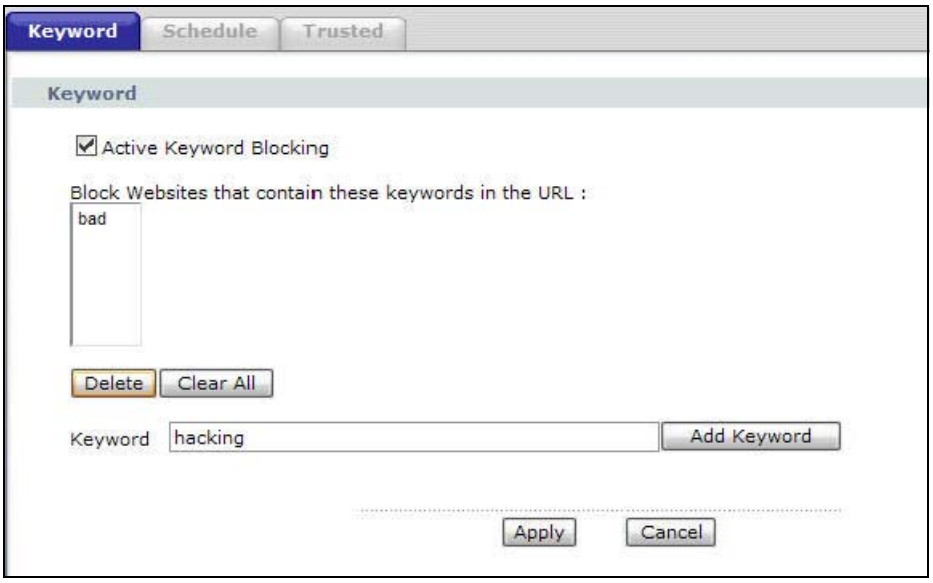
To use the **Trusted** screen, you need the IP addresses of devices on your network. See the **LAN** section (Section 11.4 on page 117) for more information.

11.1.4 URL Blocking Example

The following shows the steps required for a parent (Bob) to set up content filtering on a home network in order to limit his children’s access to certain web sites. In the following example, all URLs containing the word ‘bad’ are blocked.

1. Click **Security > URL Blocking** to display the following screen.
2. Select **Active Keyword Blocking**.
3. In the **Keyword** field type keywords to identify websites to be blocked.
4. Click **Add Keyword** for each keyword to be entered.

5 Click **Apply**.



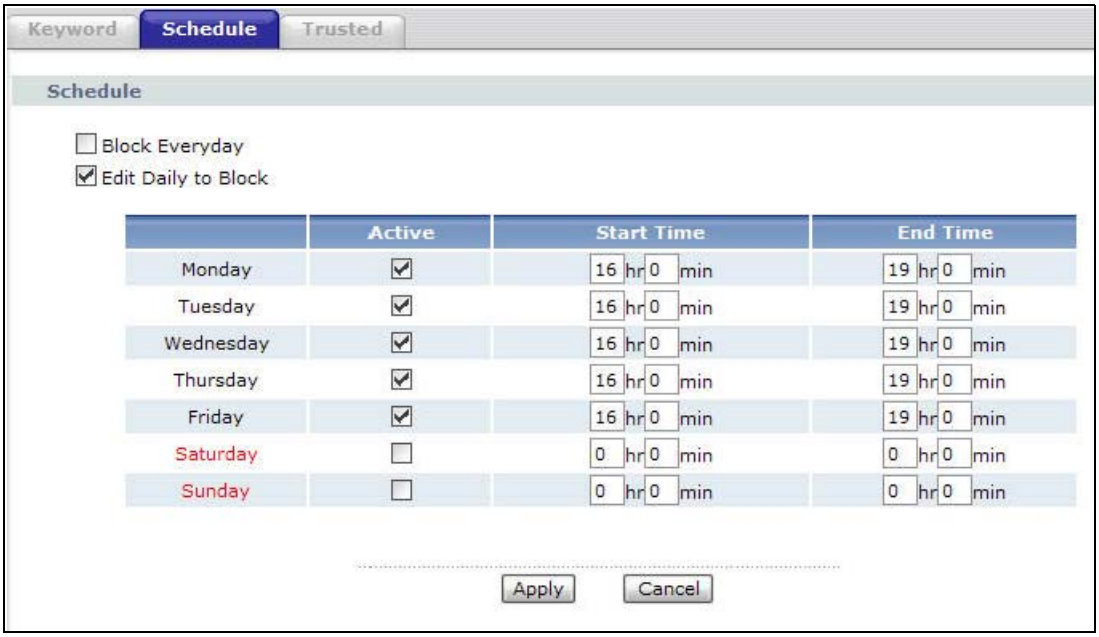
Bob's son arrives home from school at four, while his parents arrive later, at about 7pm. So keyword blocking is enabled for these times on weekdays and not on the weekend when the parents are at home.

1 Click **Security > URL Blocking > Schedule**.

2 Click **Edit Daily to Block** and select all weekdays.

3 Under **Start Time** and **End Time**, type the times for blocking to begin and end (16:00 ~ 17:00 in this example).

4 Click **Apply**.



The children can access the family computer in the living room, while only the parents use another computer in the study room. So keyword blocking is only needed on the family computer and the study computer can be excluded from keyword blocking. Bob's home network is on the domain "192.168.1.xxx". Bob gave his home computer a static IP address of 192.168.1.2 and the study computer a static IP address of 192.168.1.3. To exclude the study computer from keyword blocking he follows these steps.

1 Click **Security > URL Blocking** > **Trusted**.

2 In the **Start IP Address** and **End IP Address** fields, type 192.168.1.3.

3 Click **Apply**.

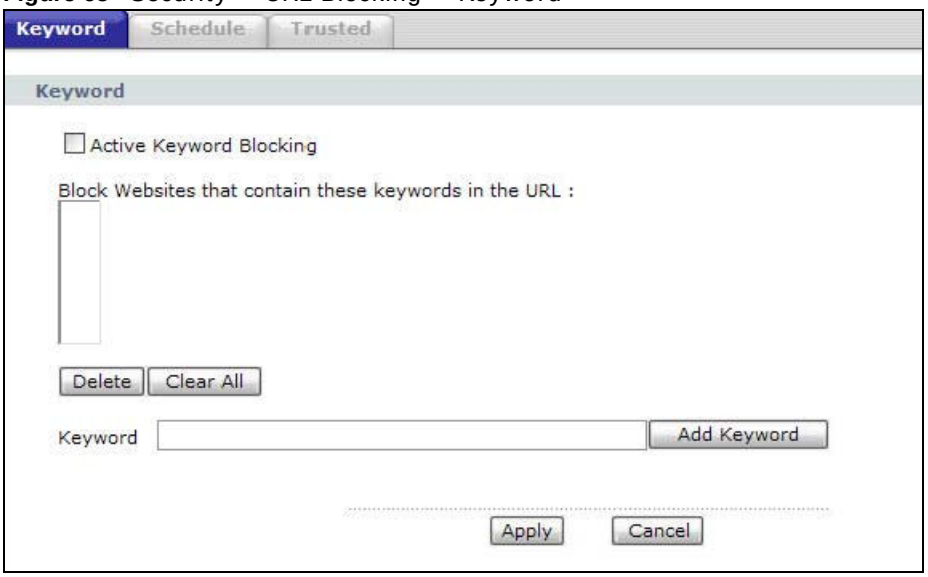
That finishes setting up keyword blocking on the home computer.

11.2 The Keyword Screen

Use this screen to block sites containing certain keywords in the URL. For example, if you enable the keyword "bad", the P-79X blocks all sites containing this keyword including the URL http://www.example.com/bad.html.

To have your P-79X block websites containing keywords in their URLs, click **Security > URL Blocking**. The screen appears as shown.

Figure 65 Security > URL Blocking > Keyword



The following table describes the labels in this screen.

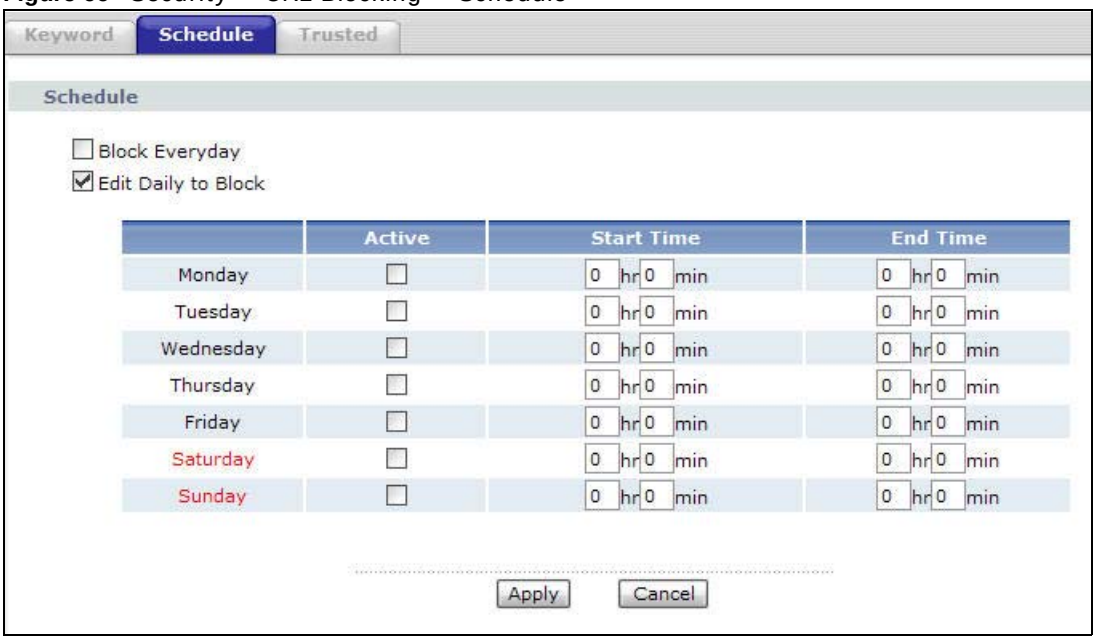
Table 39 Security > URL Blocking > Keyword

LABEL	DESCRIPTION
Active Keyword Blocking	Select this check box to enable this feature.
Block Websites that contain these keywords in the URL:	This box contains the list of all the keywords that you have configured the P-79X to block.
Delete	Highlight a keyword in the box and click this to remove it.
Clear All	Click this to remove all of the keywords from the list.
Keyword	Type a keyword in this field. You may use any character (up to 127 characters). Wildcards are not allowed.
Add Keyword	Click this after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

11.3 The Schedule Screen

Use this screen to set the days and times for the P-79X to perform content filtering. Click **Security > URL Blocking** > **Schedule**. The screen appears as shown.

Figure 66 Security > URL Blocking > Schedule



The following table describes the labels in this screen.

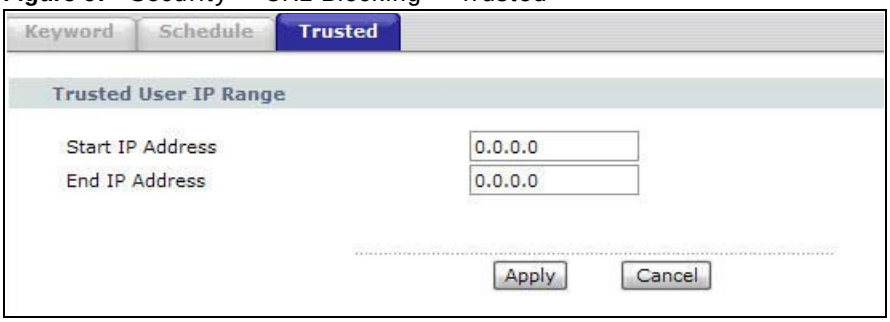
Table 40 Security > URL Blocking > Schedule

LABEL	DESCRIPTION
Schedule	Select **Block Everyday** to make the content filtering active everyday. Otherwise, select **Edit Daily to Block** and configure which days of the week (or everyday) and which time of the day you want the content filtering to be active.
Active	Select the check box to have the content filtering to be active on the selected day.
Start TIme	Enter the time when you want the content filtering to take effect in hour-minute format.
End Time	Enter the time when you want the content filtering to stop in hour-minute format.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

11.4 The Trusted Screen

Use this screen to exclude a range of users on the LAN from content filtering on your P-79X. Click **Security > URL Blocking** > **Trusted**. The screen appears as shown.

Figure 67 Security > URL Blocking > Trusted



The following table describes the labels in this screen.

Table 41 Security > URL Blocking > Trusted

LABEL	DESCRIPTION
Start IP Address	Type the IP address of a computer (or the beginning IP address of a specific range of computers) on the LAN that you want to exclude from content filtering.
End IP Address	Type the ending IP address of a specific range of users on your LAN that you want to exclude from content filtering. Leave this field blank if you want to exclude an individual computer.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

12

Packet Filter

12.1 Overview

Your P-79X uses filters to decide whether to allow passage of traffic. This chapter discusses how to create and apply filters.

12.1.1 What You Can Do in the Packet Filter Screen

Use the **Packet Filter** screens (Section 12.2 on page 119) to display the filter sets and configure the rules for protocol and generic filters.

12.1.2 What You Need to Know About the Packet Filter

Filters

Your P-79X uses filters to decide whether to allow passage of a data packet. Filters are subdivided into generic and protocol filters. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on IP packets.

Filter Structure

A filter set consists of one or more filter rules. The P-79X allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix generic filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

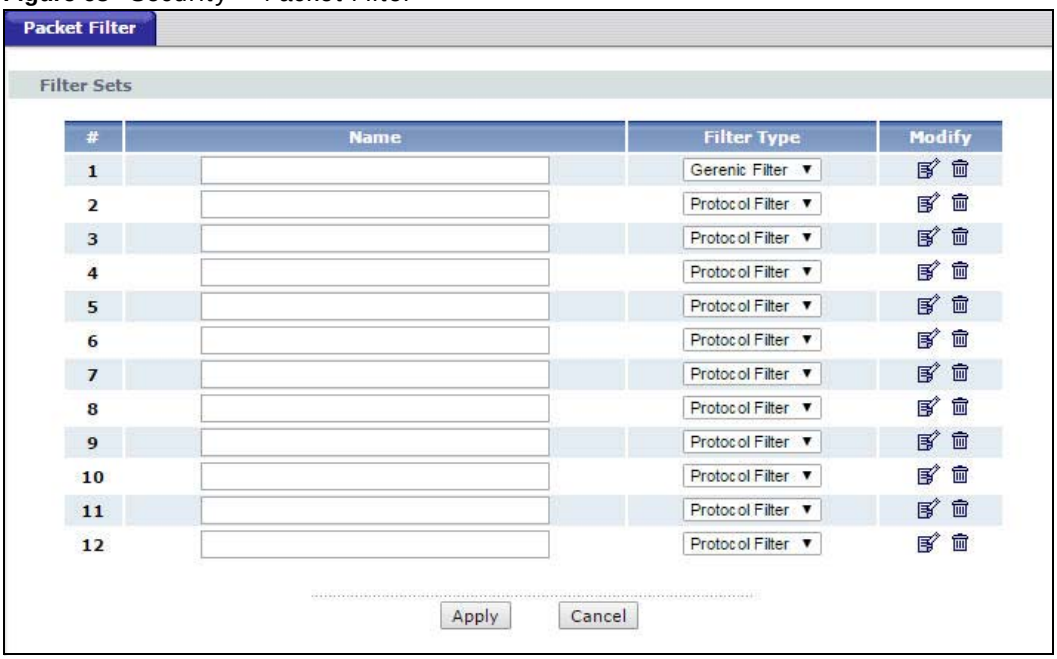
Finding Out More

See Section 12.3 on page 125 for technical background information on packet filters.

12.2 The Packet Filter Screen

Use this screen to set up packet filters on your P-79X. Click **Security > Packet Filter** to display the following screen.

Figure 68 Security > Packet Filter



The following table describes the labels in this screen.

Table 42 Security > Packet Filter

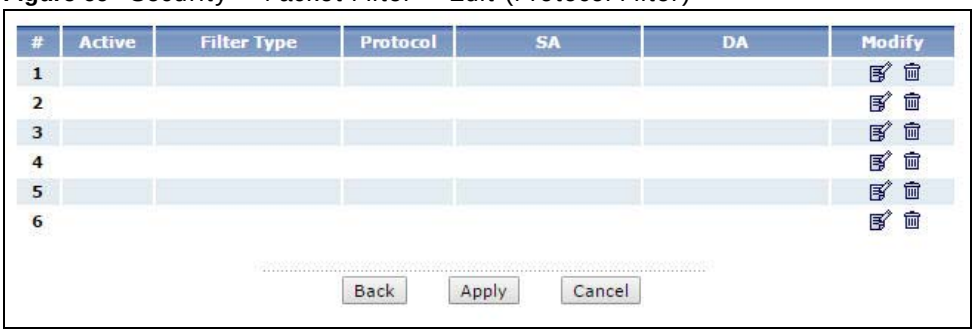
LABEL	DESCRIPTION
#	This field displays the index number of the filter set.
Name	Enter a name for the filter set. The text may consist of up to 16 letters, numerals and any printable character found on a typical English language keyboard.
Filter Type	Select **Protocol Filter** or **Generic Filter** for your filter set. Protocol filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.
Modify	Click the **Edit** icon to configure a filter set. For a new filter set, you must enter a name for the filter set and then click **Edit** to configure it. Click the **Remove** icon to delete a filter set.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

12.2.1 Editing Protocol Filters

Use this screen to display a protocol filter set on your P-79X. Protocol rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

In the **Packet Filter** screen, select **Protocol Filter** from the **Filter Type** field. Then click the **Edit** icon from the **Modify** field to display the following screen.

Figure 69 Security > Packet Filter > Edit (Protocol Filter)



The following table describes the labels in this screen.

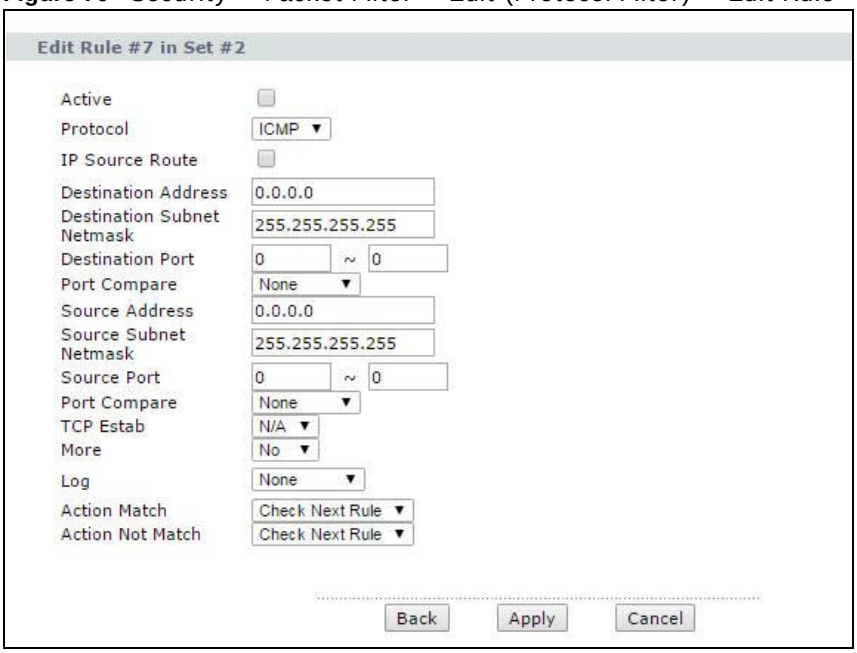
Table 43 Security > Packet Filter > Edit (Protocol Filter)

LABEL	DESCRIPTION
#	This is the index number of the rules in a filter set.
Active	Use the check box to turn a filter rule on or off.
Filter Type	This field displays whether the filter type is a protocol filter or generic filter.
Protocol	This field displays the upper layer protocol.
SA	This field displays the source IP address.
DA	This field displays the destination IP address.
Modify	Click the **Edit** icon to configure a filter rule. Click the **Remove** icon to delete a filter rule.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

12.2.2 Configuring Protocol Filter Rules

Use this screen to configure protocol filter rules. In the **Edit (Protocol Filter)** screen, click an **Edit** icon to display the following screen.

Figure 70 Security > Packet Filter > Edit (Protocol Filter) > Edit Rule



The following table describes the labels in this screen.

Table 44 Security > Packet Filter > Edit (Protocol Filter) > Edit Rule

LABEL	DESCRIPTION
Active	Select the check box to enable the filter rule.
Protocol	Select **ICMP**, **TCP** or **UDP** for the upper layer protocol.
IP Source Route	Select the check box to apply the filter rule to packets with an IP source route option. The majority of IP packets do not have source route.
Destination Address	Enter the destination IP address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
Destination Subnet Netmask	Enter the IP subnet mask for the destination IP address.
Destination Port	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port Compare	Select the comparison to apply to the destination port in the packet against the value given in the **Destination Port** field. Options are **None**, **Equal** and **Not Equal**.
Source Address	Enter the source IP address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
Source Subnet Netmask	Enter the IP subnet mask for the source IP address
Source Port	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port Compare	Select the comparison to apply to the source port in the packet against the value given in the **Source Port** field. Options are **None**, **Equal** and **Not Equal**.
TCP Estab	This field is only available when you select **TCP** in the **Protocol** field. Select **Yes** to have the rule match packets that want to establish a TCP connection. This field is ignored if you select **No**.

Table 44 Security > Packet Filter > Edit (Protocol Filter) > Edit Rule (continued)

LABEL	DESCRIPTION
More	Select **Yes** to pass a matching packet to the next filter rule before an action is taken. Select **No** to act upon the packet according to the action fields.
Log	Select a logging option from the following: **None** – No packets will be logged. **Match** - Only packets that match the rule parameters will be logged. **Not Match** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Match	Select the action for a matching packet. Options are **Check Next Rule**, **Forward** and **Drop**.
Action Not Match	Select the action for a packet not matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

12.2.3 Editing Generic Filters

Use this screen to display a generic filter set on your P-79X. The purpose of generic rules is to allow you to filter non-IP packets. For IP packets, it is generally easier to use the IP rules directly.

For generic rules, the P-79X treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The P-79X applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4 bytes, the value in either field will take 8 digits, for example, FFFFFFFF.

In the **Packet Filter** screen, select **Generic Filter** from the **Filter Type** field. Then click the **Edit** button from the **Modify** field to display the following screen.

Figure 71 Security > Packet Filter > Edit (Generic Filter)

The following table describes the labels in this screen.

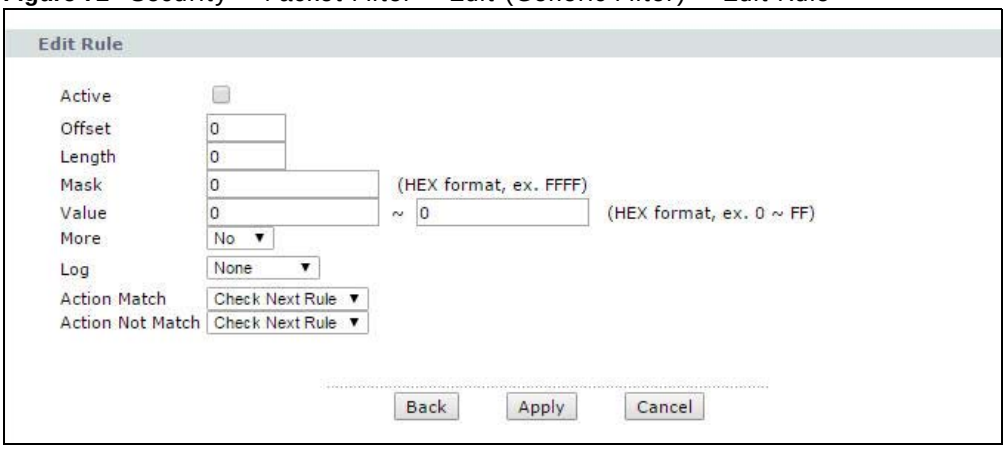
Table 45 Security > Packet Filter > Edit (Generic Filter)

LABEL	DESCRIPTION
#	This is the index number of the rules in a filter set.
Active	Use the check box to turn on or off a filter rule.
Filter Type	This field displays whether the filter type is a protocol filter or generic filter.
Offset	This field displays the offset value.
Length	This field displays the length value.
Mask	This field displays the mask value.
Value	This field displays the value.
Modify	Click the **Edit** icon to configure a filter rule. Click the **Remove** icon to delete a filter rule.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

12.2.4 Configuring Generic Packet Rules

Use this screen to configure generic filter rules. In the **Edit (Generic Filter)** screen, click the **Edit** button from the **Modify** field to display the following screen.

Figure 72 Security > Packet Filter > Edit (Generic Filter) > Edit Rule



The following table describes the labels in this screen.

Table 46 Security > Packet Filter > Edit (Generic Filter) > Edit Rule

LABEL	DESCRIPTION
Active	Select the check box to enable the filter rule.
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.
Mask	Enter the mask (in hexadecimal notation) to apply to the data portion before comparison.

Table 46 Security > Packet Filter > Edit (Generic Filter) > Edit Rule (continued)

LABEL	DESCRIPTION
Value	Enter the value (in hexadecimal notation) to compare with the data portion.
More	Select **Yes** to pass a matching packet to the next filter rule before an action is taken. Select **No** to act upon the packet according to the action fields.
Log	Select a logging option from the following: **None** – No packets will be logged. **Match** - Only packets that match the rule parameters will be logged. **Not Match** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Match	Select the action for a matching packet. Options are **Check Next Rule**, **Forward** and **Drop**.
Action Not Match	Select the action for a packet not matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

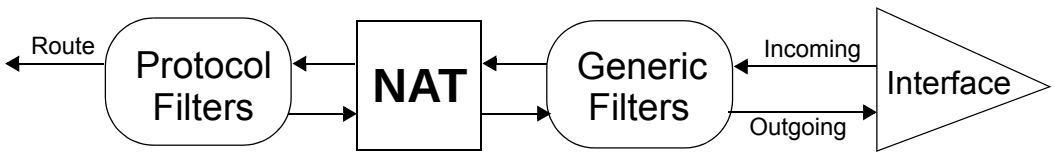
12.3 Packet Filter Technical Reference

This section provides some technical background information about the topics covered in this chapter.

12.3.1 Filter Types and NAT

There are two classes of filter rules, generic filter rules and protocol filter rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the P-79X applies the protocol filters to the “native” IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic filters are applied to the raw packets that appear on the wire. They are applied at the point when the P-79X is receiving and sending the packets; that is the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

Figure 73 Protocol and Generic Filter Sets



12.3.2 Firewall Versus Filters

Below are some comparisons between the P-79X's filtering and firewall functions.

Packet Filtering

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

When To Use Filtering

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

Firewall

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

When To Use The Firewall

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

5 Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.

6 The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

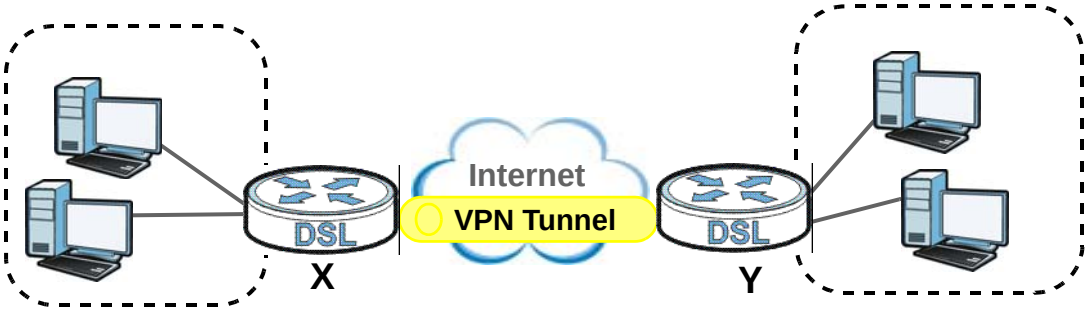
13 VPN

13.1 Overview

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

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

Figure 74 VPN: Example



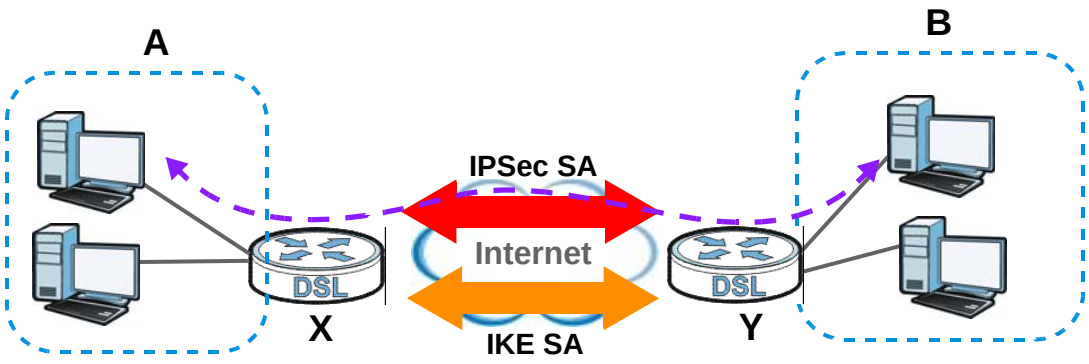
13.1.1 What You Can Do in the VPN Screens

- Use the **Setup** screen (Section 13.2 on page 130) to view the configured VPN policies and add, edit or remove a VPN policy.
- Use the **Monitor** screen (Section 13.5 on page 138) to display and manage the current active VPN connections.

13.1.2 What You Need to Know About IPSec VPN

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the P-79X and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the P-79X and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the P-79X and remote IPSec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 75 VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

My IP Address

My IP Address is the WAN IP address of the P-79X. The P-79X has to rebuild the VPN tunnel if **My IP Address** changes after setup.

The following applies if this field is configured as **0.0.0.0**:

- The P-79X uses the current P-79X WAN IP address (static or dynamic) to set up the VPN tunnel.

Secure Gateway Address

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

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

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The P-79X has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

Dynamic Secure Gateway Address

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network (see Section 13.6.12 on page 147 for configuration examples).

The Secure Gateway IP Address may be configured as **0.0.0.0** only when using **IKE** key management and not **Manual** key management.

Finding Out More

See Section 13.6 on page 139 for advanced technical information on IPSec VPN.

13.1.3 Before You Begin

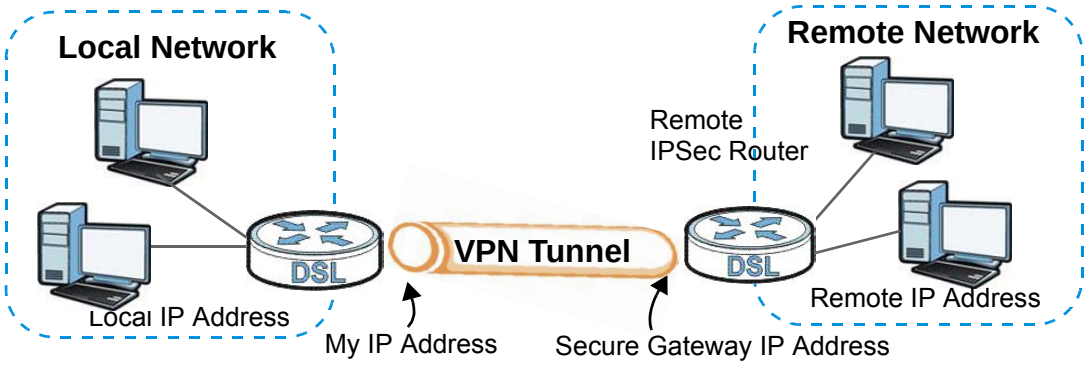
If a VPN tunnel uses Telnet, FTP, WWW, then you should configure remote management (**Remote MGMT**) to allow access for that service.

Note: This chapter is not available when you use the P-791R v3 device.

13.2 VPN Setup Screen

The following figure helps explain the main fields in the web configurator.

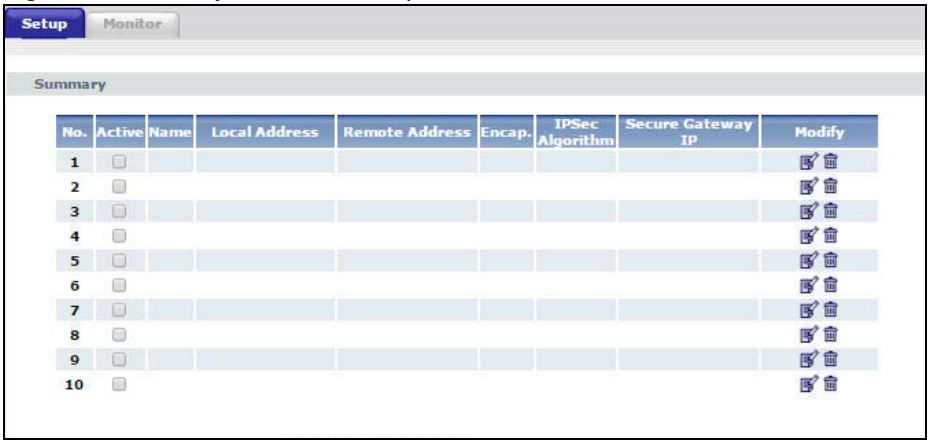
Figure 76 IPSec Summary Fields



Local and remote IP addresses must be static.

Click **Security** > **VPN** to open the **VPN Setup** screen. This is a menu of your IPSec rules (tunnels). The IPSec summary menu is read-only. Edit a VPN by selecting an index number and then configuring its associated submenus.

Figure 77 Security > VPN > Setup



The following table describes the fields in this screen.

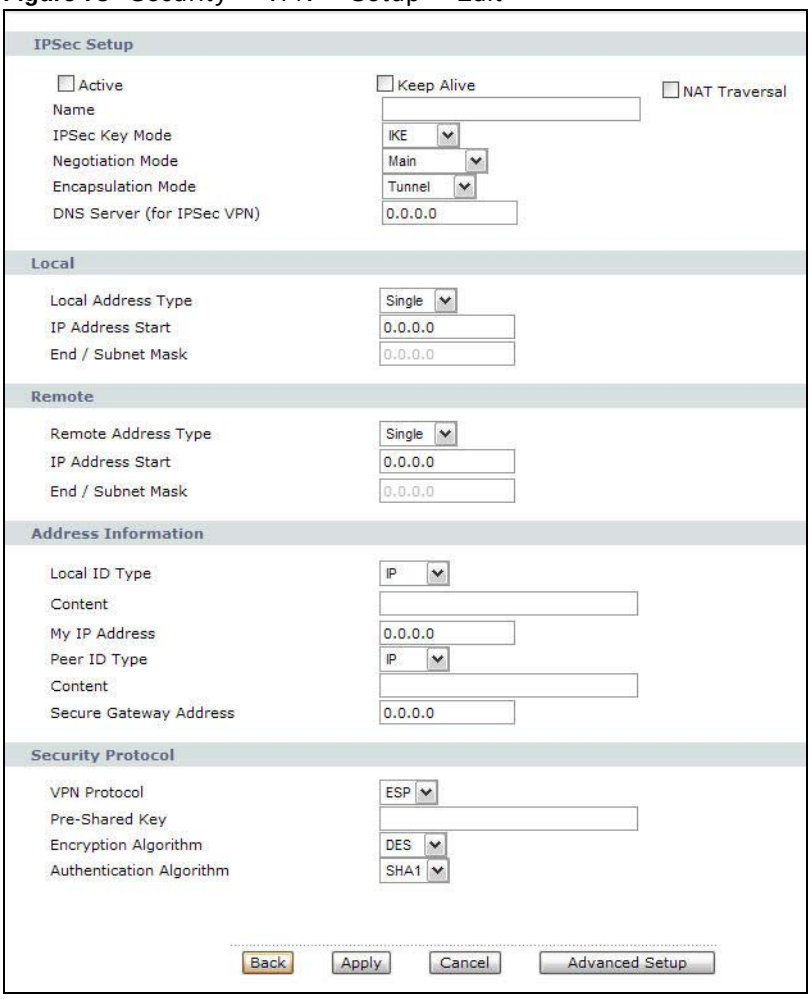
Table 47 Security > VPN > Setup

LABEL	DESCRIPTION
No.	This is the VPN policy index number. Click a number to edit VPN policies.
Active	This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active.
Name	This field displays the identification name for this VPN policy.
Local Address	This is the IP address(es) of computer(s) on your local network behind your P-79X. The same (static) IP address is displayed twice when the **Local Address Type** field in the **VPN Setup - Edit** screen is configured to **Single**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Address Type** field in the **VPN Setup - Edit** screen is configured to **Range**. A (static) IP address and a subnet mask are displayed when the **Local Address Type** field in the **VPN Setup - Edit** screen is configured to **Subnet**.
Remote Address	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router. This field displays **N/A** when the **Secure Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. The same (static) IP address is displayed twice when the **Remote Address Type** field in the **VPN Setup - Edit** screen is configured to **Single**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Address Type** field in the **VPN Setup - Edit** screen is configured to **Range**. A (static) IP address and a subnet mask are displayed when the **Remote Address Type** field in the **VPN Setup - Edit** screen is configured to **Subnet**.
Encap.	This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection).
IPSec Algorithm	This field displays the security protocols used for an SA. Both **AH** and **ESP** increase P-79X processing requirements and communications latency (delay).
Secure Gateway IP	This is the static WAN IP address or URL of the remote IPSec router. This field displays **0.0.0.0** when you configure the **Secure Gateway Address** field in the **VPN-IKE** screen to **0.0.0.0.**
Modify	Click the **Edit** icon to go to the screen where you can edit the VPN configuration. Click the **Remove** icon to remove an existing VPN configuration.
Apply	Click this to save your changes and apply them to the P-79X.
Cancel	Click this return your settings to their last saved values.

13.3 The VPN Edit Screen

Click an **Edit** icon in the **VPN Setup** screen to edit VPN policies.

Figure 78 Security > VPN > Setup > Edit



The following table describes the fields in this screen.

Table 48 Security > VPN > Setup > Edit

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy. This option determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Select either **Yes** or **No** from the drop-down list box. Select **Yes** to have the P-79X automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
NAT Traversal	This function is available if the **VPN Protocol** is **ESP**. Select this check box if you want to set up a VPN tunnel when there are NAT routers between the P-79X and remote IPSec router. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward UDP port 500 packets to the remote IPSec router behind the NAT router.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the P-79X drops trailing spaces.
IPSec Key Mode	Select **IKE** from the drop-down list box. **IKE** provides more protection so it is generally recommended.

Table 48 Security > VPN > Setup > Edit

LABEL	DESCRIPTION
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The P-79X assigns this additional DNS server to the P-79X's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local	Specify the IP addresses of the devices behind the P-79X that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Local Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** for a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Local Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind your P-79X. When the **Local Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your P-79X. When the **Local Address Type** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your P-79X.
End / Subnet Mask	When the **Local Address Type** field is configured to **Single**, this field is N/A. When the **Local Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your P-79X. When the **Local Address Type** field is configured to **Subnet**, this is a subnet mask on the LAN behind your P-79X.
Remote	Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** with a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Remote Address Type** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.
End / Subnet Mask	When the **Remote Address Type** field is configured to **Single**, this field is N/A. When the **Remote Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Address Information	

Table 48 Security > VPN > Setup > Edit

LABEL	DESCRIPTION
Local ID Type	Select **IP** to identify this P-79X by its IP address. Select **DNS** to identify this P-79X by a domain name. Select **E-mail** to identify this P-79X by an e-mail address.
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The P-79X automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations. When there is a NAT router between the two IPSec routers. When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this P-79X in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
My IP Address	Enter the WAN IP address of your P-79X. The VPN tunnel has to be rebuilt if this IP address changes. The following applies if this field is configured as **0.0.0.0**: The P-79X uses the current P-79X WAN IP address (static or dynamic) to set up the VPN tunnel.
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	The configuration of the peer content depends on the peer ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the P-79X will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description). For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations: When there is a NAT router between the two IPSec routers. When you want the P-79X to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.

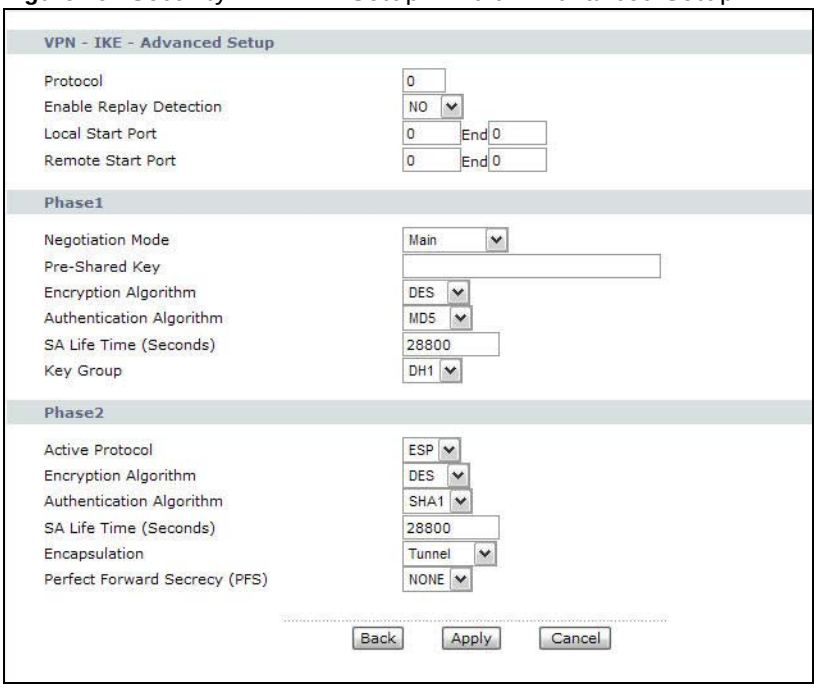
Table 48 Security > VPN > Setup > Edit

LABEL	DESCRIPTION
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **IPSec Key Mode** field must be set to **IKE**). In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Security Protocol	
VPN Protocol	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).
Pre-Shared Key	Click the button to use a pre-shared key for authentication, and type in your pre-shared key. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	Select **DES**, **3DES**, **AES** or **NULL** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key. Note: The **DES** encryption algorithm is not supported at the time of writing.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the P-79X.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Advanced Setup	Click **Advanced Setup** to configure more detailed settings of your IKE key management.

13.4 Configuring Advanced IKE Settings

Click **Advanced Setup** in the **VPN Setup-Edit** screen to open this screen.

Figure 79 Security > VPN > Setup > Edit > Advanced Setup



The following table describes the fields in this screen.

Table 49 Security > VPN > Setup > Edit > Advanced Setup

LABEL	DESCRIPTION
VPN - IKE - Advanced Setup	
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, and so on. 0 is the default and signifies any protocol.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select **YES** from the drop-down menu to enable replay detection, or select **NO** to disable it.
Local Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Local Start Port** is left at 0, **End** will also remain at 0.
Remote Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Remote Start Port** is left at 0, **End** will also remain at 0.
Phase 1	
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

Table 49 Security > VPN > Setup > Edit > Advanced Setup (continued)

LABEL	DESCRIPTION
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62-character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a “PYLD_MALFORMED” (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	Select **DES**, **3DES** or **AES** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. **AES** is faster than **3DES**. Note: The **DES** encryption algorithm is not supported at the time of writing.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
SA Life Time (Seconds)	Define the length of time before an IPSec SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	
Active Protocol	Use the drop-down list box to choose from **ESP** or **AH**.
Encryption Algorithm	This field is available when you select **ESP** in the **Active Protocol** field. Select **DES**, **3DES**, **AES** or **NULL** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key. Note: The **DES** encryption algorithm is not supported at the time of writing.

Table 49 Security > VPN > Setup > Edit > Advanced Setup (continued)

LABEL	DESCRIPTION
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Encapsulation	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**NONE**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose **DH1** or **DH2** from the drop-down list box to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the P-79X and return to the **VPN-IKE** screen.
Cancel	Click **Cancel** to return to the **VPN-IKE** screen without saving your changes.

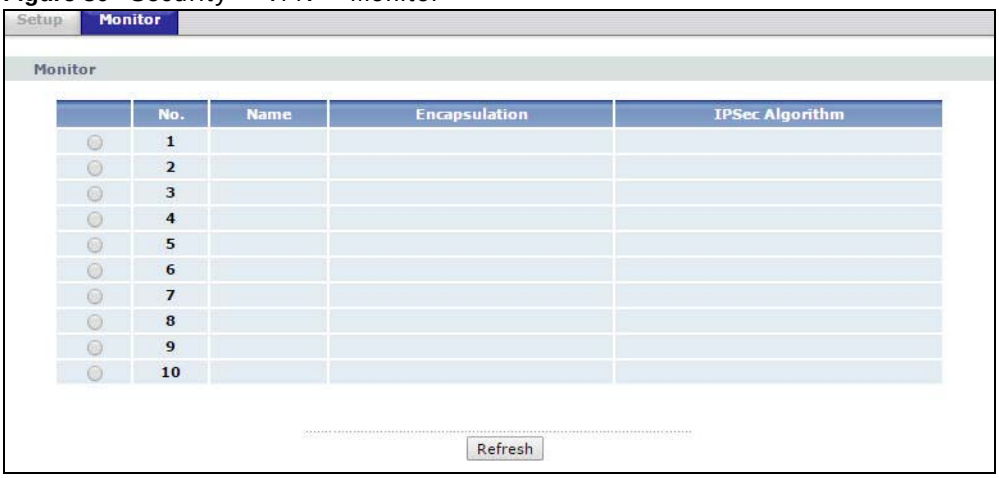
13.5 Viewing SA Monitor

Click **Security** > **VPN** > **Monitor** to open the screen as shown. Use this screen to display and manage active VPN connections.

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

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See Section 13.6.7 on page 144on keep alive to have the P-79X renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 80 Security > VPN > Monitor



The following table describes the fields in this screen.

Table 50 Security > VPN > Monitor

LABEL	DESCRIPTION
No	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocol, encryption algorithm, and authentication algorithm used in each VPN tunnel.
Refresh	Click **Refresh** to display the current active VPN connection(s).

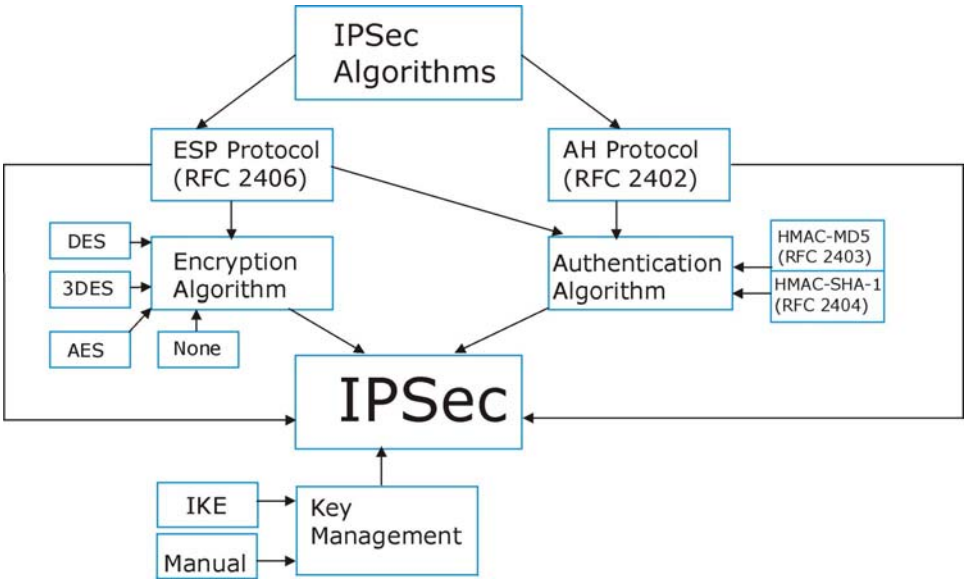
13.6 IPSec VPN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

13.6.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 81 IPSec Architecture



IPSec Algorithms

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

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms. The DES encryption algorithm is not supported at the time of writing.

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

Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

13.6.2 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the P-79X.

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

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

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

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 51 VPN and NAT

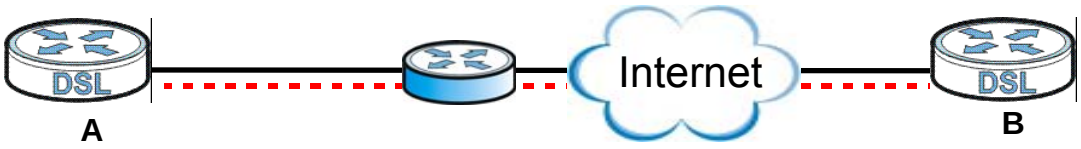
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

13.6.3 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the P-79X's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 82 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In Figure 82 on page 141, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

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

- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 52 VPN and NAT

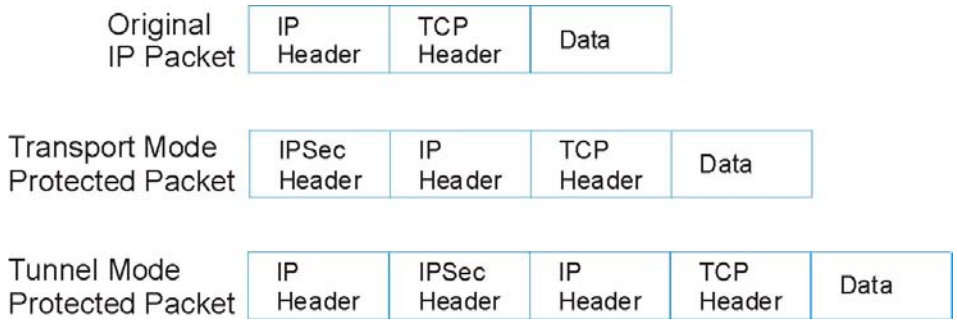
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

Y* - This is supported in the P-79X if you enable NAT traversal.

13.6.4 Encapsulation

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

Figure 83 Transport and Tunnel Mode IPSec Encapsulation



Transport Mode

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

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

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

Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP

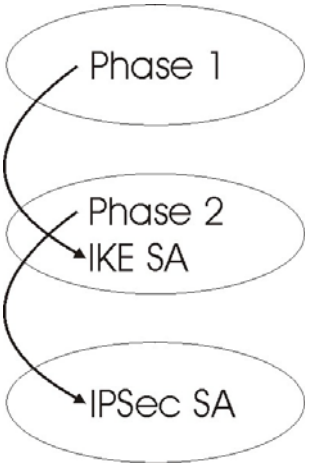
tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

13.6.5 IKE Phases

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

Figure 84 Two Phases to Set Up the IPSec SA



In phase 1 you must:

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

In phase 2 you must:

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

- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The P-79X automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The P-79X also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

13.6.6 Negotiation Mode

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

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

13.6.7 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the P-79X automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see Section 13.6.5 on page 143 for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Both IPSec routers must have a P-79X-compatible keep alive feature enabled in order for this feature to work.

If the P-79X has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the P-79X because the P-79X never drops the tunnels that are already connected.

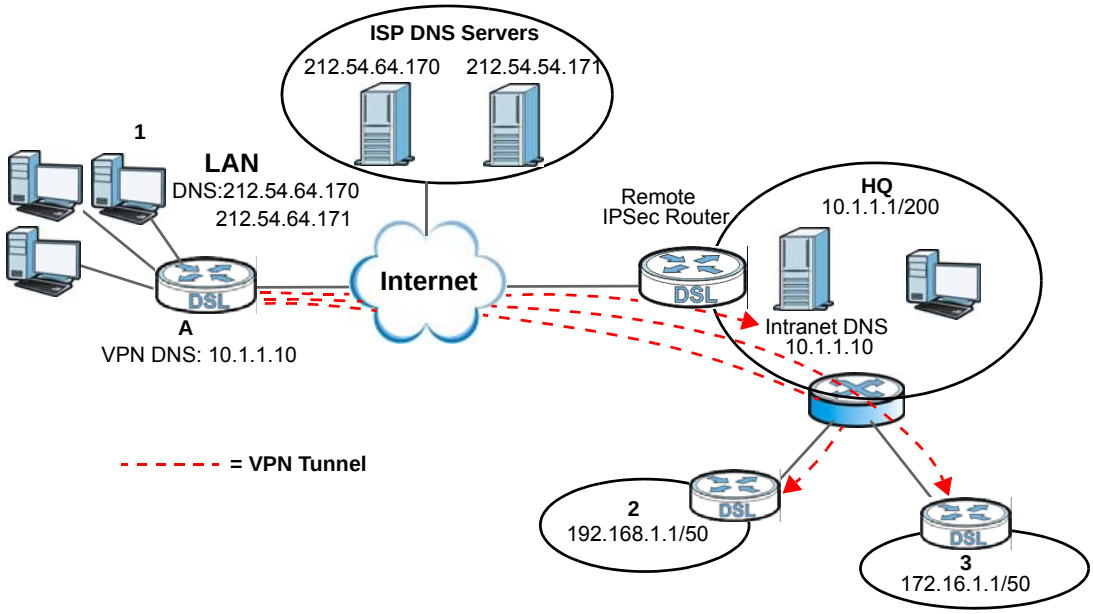
When there is outbound traffic with no inbound traffic, the P-79X automatically drops the tunnel after two minutes.

13.6.8 Remote DNS Server

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

The following figure depicts an example where three VPN tunnels are created from P-79X A; one to branch office 2, one to branch office 3 and another to headquarters. In order to access computers that use private domain names on the headquarters (HQ) network, the P-79X at branch office 1 uses the Intranet DNS server in headquarters. The DNS server feature for VPN does not work with Windows 2000 or Windows XP.

Figure 85 VPN Host using Intranet DNS Server Example



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

13.6.9 ID Type and Content

With aggressive negotiation mode (seeSection 13.6.6 on page 144), the P-79X identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the P-79X to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the P-79X from IPSec routers with dynamic IP addresses (seeSection 13.6.12 on page 147 for a telecommuter configuration example).

Regardless of the ID type and content configuration, the P-79X does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (seeSection 13.6.6 on page 144), the ID type and content are encrypted to provide identity protection. In this case the P-79X can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The P-79X can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (seeSection 13.4 on page 136). The ID type and content act as an extra level of identification for incoming SAs. The DES encryption algorithm is not supported at the time of writing.

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

Table 53 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer or leave the field blank to have the P-79X automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this P-79X.

Table 53 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
E-mail	Type an e-mail address (up to 31 characters) by which to identify this P-79X.
	The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

Table 54 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the P-79X automatically use the address in the **Secure Gateway Address** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
	The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Address** field below.

13.6.9.1 ID Type and Content Examples

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

The two P-79Xs in this example can complete negotiation and establish a VPN tunnel.

Table 55 Matching ID Type and Content Configuration Example

P-79X A	P-79X B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two P-79Xs in this example cannot complete their negotiation because P-79X B's **Local ID type** is **IP**, but P-79X A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 56 Mismatching ID Type and Content Configuration Example

P-79X A	P-79X B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

13.6.10 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 13.6.5 on page 143 for more on IKE phases). It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection.

13.6.11 Diffie-Hellman (DH) Key Groups

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

13.6.12 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single P-79X at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The P-79X at headquarters has a static public IP address.

13.6.12.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (**A**, **B** and **C** in the figure) to use one VPN rule to simultaneously access a P-79X at headquarters (**HQ** in the figure). The telecommuters do not have domain names mapped to the WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

Figure 86 Telecommuters Sharing One VPN Rule Example

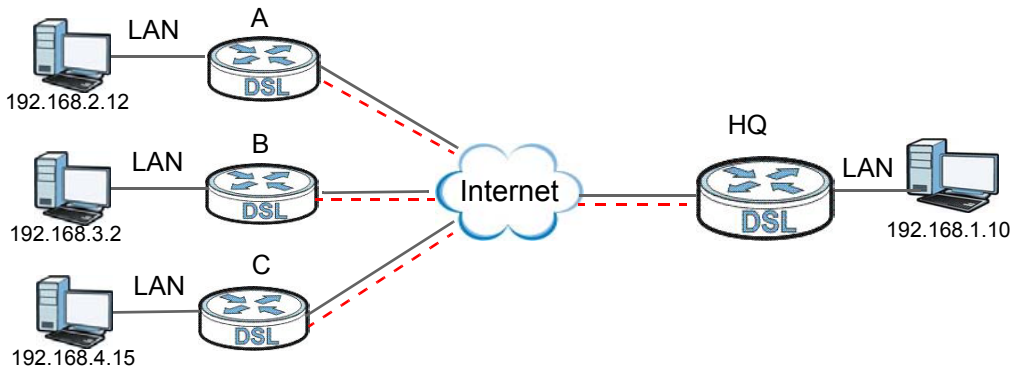


Table 57 Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
My IP Address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.

Table 57 Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
Local IP Address:	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15	192.168.1.10
Remote IP Address:	192.168.1.10	0.0.0.0 (N/A)

13.6.12.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (**A**, **B** and **C** in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see Section 13.6.6 on page 144), the P-79X can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a P-79X at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the P-79X at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a P-79X located at headquarters. The P-79X at headquarters (**HQ** in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The P-79X at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

Figure 87 Telecommuters Using Unique VPN Rules Example

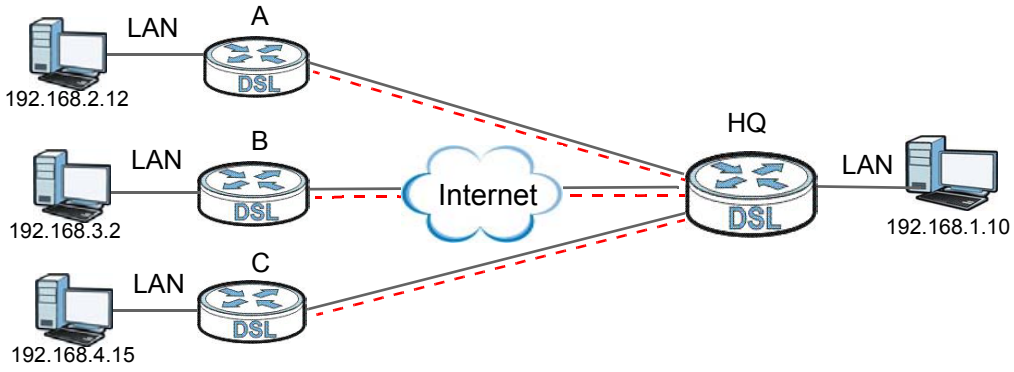


Table 58 Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
All Telecommuter Rules:	All Headquarters Rules:
My IP Address 0.0.0.0	My IP Address: bigcompanyhq.com
Secure Gateway Address: bigcompanyhq.com	Local IP Address: 192.168.1.10
Remote IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	

Table 58 Telecommuters Using Unique VPN Rules Example (continued)

TELECOMMUTERS	HEADQUARTERS
Telecommuter A (telecommutera.dydns.org)	Headquarters P-79X Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Secure Gateway Address: telecommuter1.com
	Remote Address 192.168.2.12
Telecommuter B (telecommuterb.dydns.org)	Headquarters P-79X Rule 2:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Secure Gateway Address: telecommuterb.com
	Remote Address 192.168.3.2
Telecommuter C (telecommuterc.dydns.org)	Headquarters P-79X Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Secure Gateway Address: telecommuterc.com
	Remote Address 192.168.4.15

14

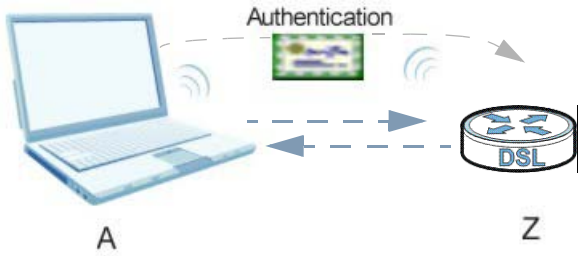
Certificates

14.1 Overview

This chapter describes how your P-79X can use certificates as a means of authenticating clients. It gives background information about public-key certificates and explains how to use them.

A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Figure 88 Certificates Example



In the figure above, the P-79X (**Z**) checks the identity of the notebook (**A**) using a certificate before granting it access to the network.

14.1.1 What You Need to Know About Certificates

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the P-79X to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

Certificate File Formats

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

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

Factory Default Certificate

The P-79X generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

14.1.2 Verifying a Certificate

Before you import a trusted certificate into the P-79X, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

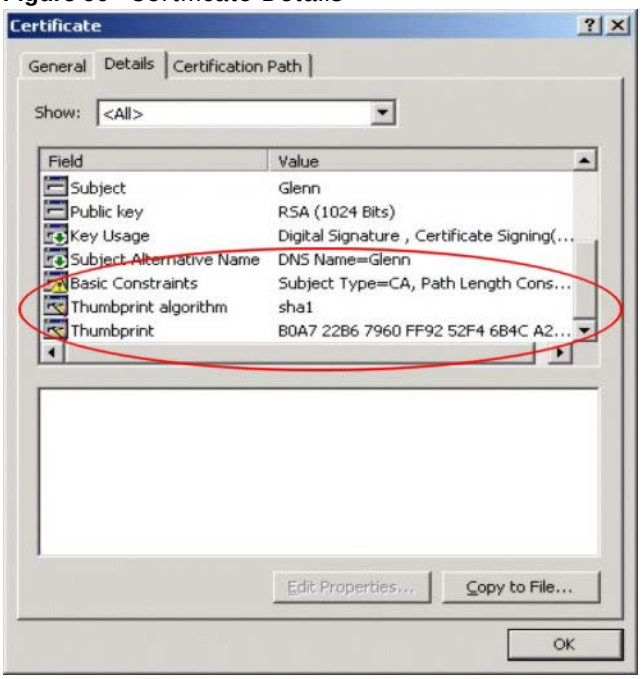
1 Browse to where you have the certificate saved on your computer.

2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 89 Remote Host Certificates

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

Figure 90 Certificate Details



4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

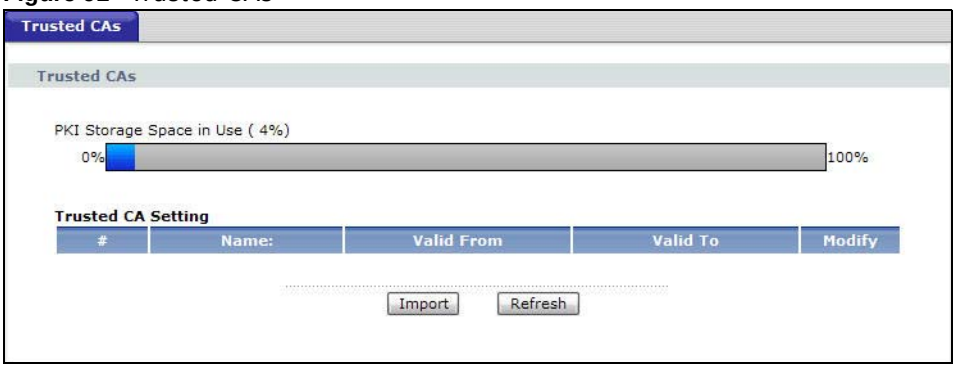
Finding Out More

See Section 14.3 on page 155 for technical background information on certificates.

14.2 The Trusted CAs Screen

This screen displays a summary list of certificates of the certification authorities that you have set the P-79X to accept as trusted. The P-79X accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities. Click **Security > Certificates > Trusted CAs** to open the following screen.

Figure 91 Trusted CAs



The following table describes the labels in this screen.

Table 59 Trusted CAs

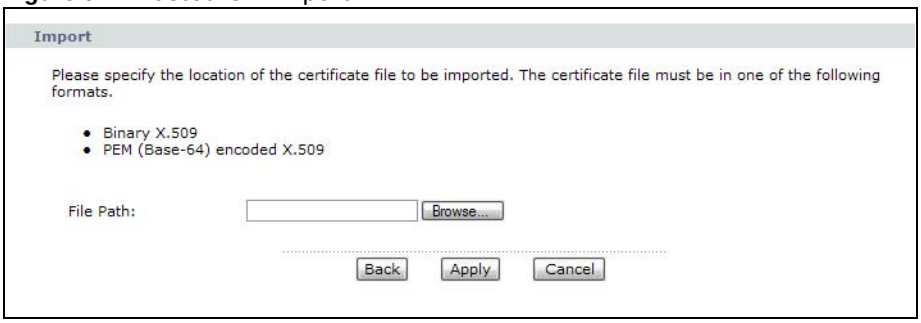
LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the P-79X's PKI storage space that is currently in use. The bar turns from blue to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the Edit icon to open a screen with an in-depth list of information about the certificate. Click the Remove icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Import	Click this to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the P-79X.
Refresh	Click this to display the current validity status of the certificates.

14.2.1 Trusted CA Import

Follow the instructions in this screen to save a trusted certification authority's certificate to the P-79X. Click **Security** > **Certificates** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen.

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

Figure 92 Trusted CA Import



The following table describes the labels in this screen.

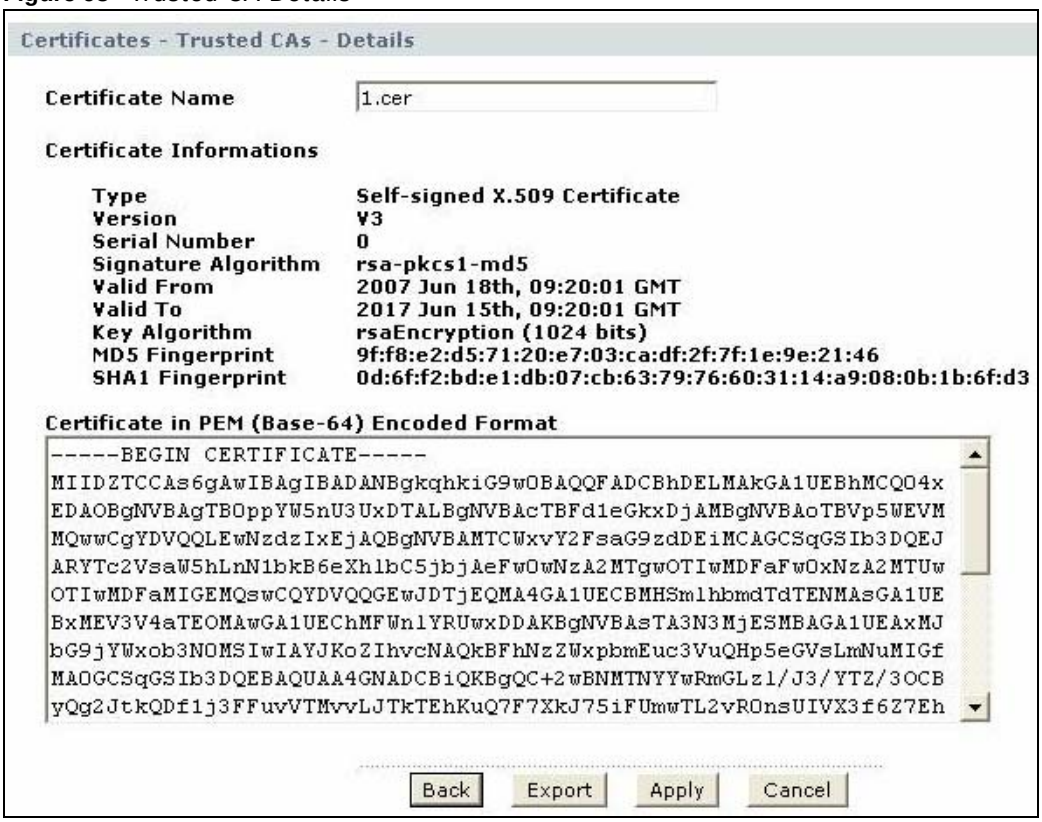
Table 60 Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click this to find the certificate file you want to upload.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save the certificate on the P-79X.
Cancel	Click this to restore your previously saved settings.

14.2.2 Trusted CA Details

Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the P-79X to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority. Click **Security** > **Certificates** > **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen.

Figure 93 Trusted CA Details



The following table describes the labels in this screen.

Table 61 Trusted CA Details

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.

Table 61 Trusted CA Details (continued)

LABEL	DESCRIPTION
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the P-79X uses RSA encryption) and the length of the key set in bits (1024 bits for example).
MD5 Fingerprint	This is the certificate's message digest that the P-79X calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the P-79X calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this to return to the previous screen without saving.
Export	Click this and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click this to save your changes. You can only change the name and/or set whether or not you want the P-79X to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click this to restore your previously saved settings.

14.3 Certificates Technical Reference

This section provides technical background information about the topics covered in this chapter.

14.3.1 Certificates Overview

The P-79X can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

The P-79X uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The

method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

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

Advantages of Certificates

Certificates offer the following benefits.

- The P-79X only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

14.3.2 Private-Public Certificates

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

1. Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
2. Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
3. Tim uses his private key to sign the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).
5. Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

15

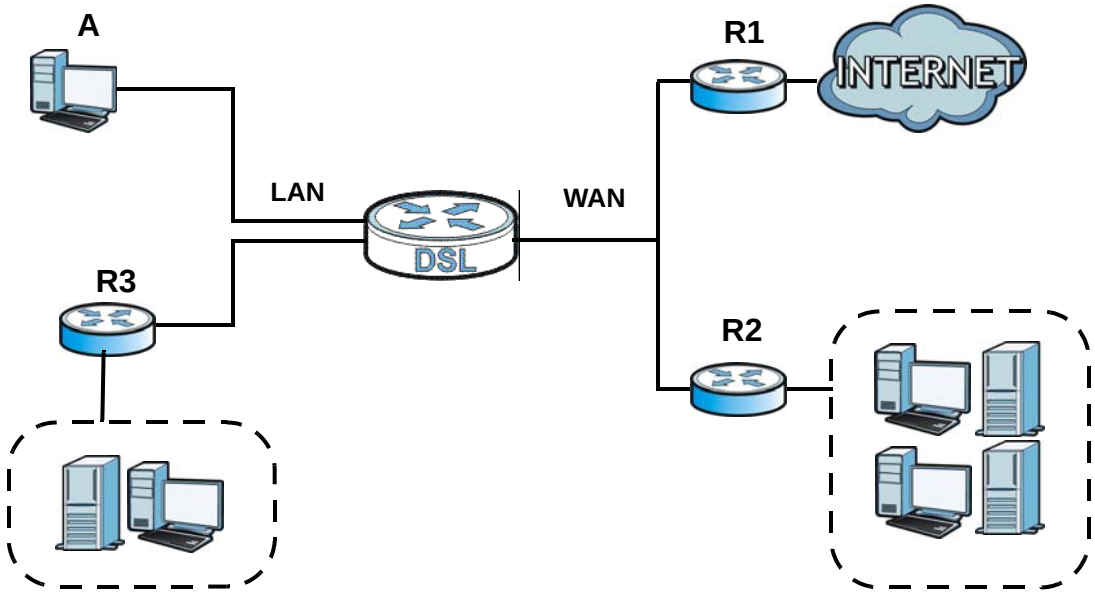
Static Route

15.1 Overview

The P-79X usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the P-79X send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the P-79X's LAN interface. The P-79X routes most traffic from **A** to the Internet through the P-79X's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

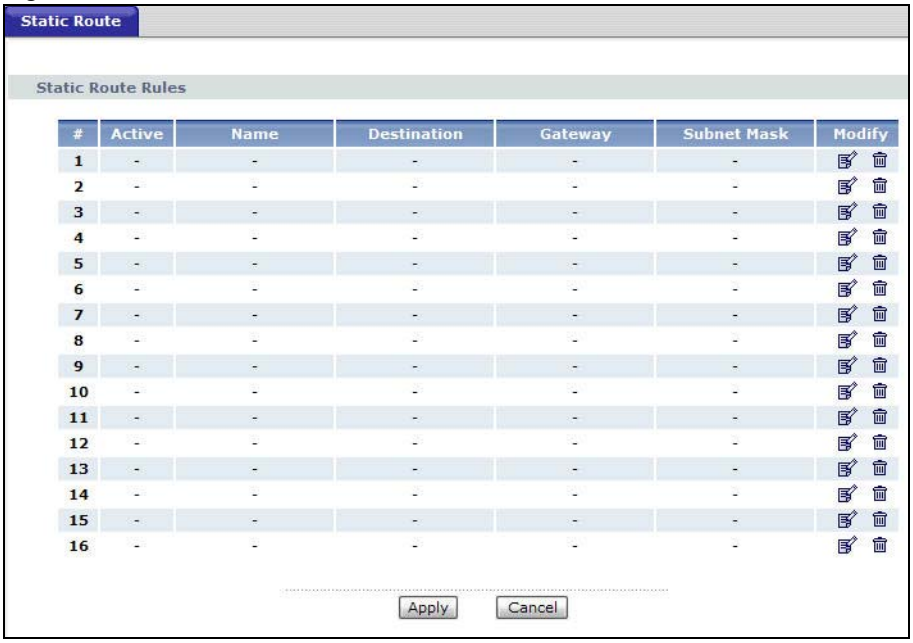
Figure 94 Example of Static Routing Topology



15.2 The Static Route Screen

Use this screen to view the static route rules. Click **Advanced > Static Route** to open the **Static Route** screen.

Figure 95 Advanced > Static Route



The following table describes the labels in this screen.

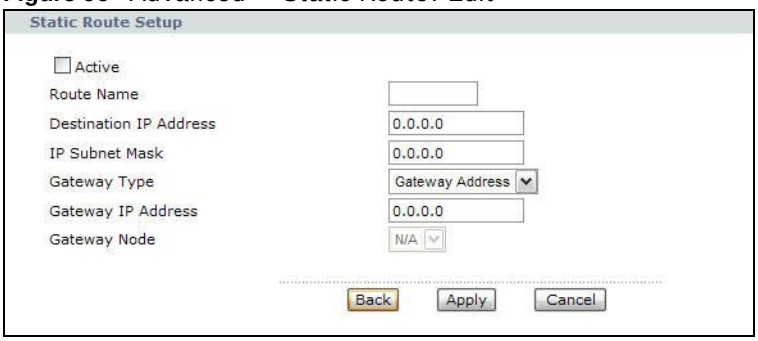
Table 62 Advanced > Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the P-79X. Click the Remove icon to remove a static route from the P-79X. A window displays asking you to confirm that you want to delete the route.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

15.2.1 Static Route Edit

Use this screen to configure the required information for a static route. Select a static route index number and click **Edit**. The screen shown next appears.

Figure 96 Advanced > Static Route: Edit



The following table describes the labels in this screen.

Table 63 Advanced > Static Route: Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. The text may consist of up to 9 letters, numerals and any printable character found on a typical English language keyboard. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway Type	Use either **Gateway Address** or **Gateway Node** to configure a static route.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Gateway Node	This field is available when you select **Gateway Node** from **Gateway Type**. Select a remote node to set the static route. A remote note is a connection point outside of the local area network. One example of a remote node is your connection to your ISP.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

16

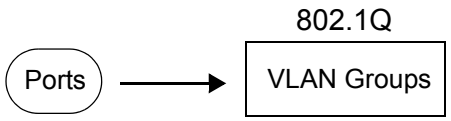
802.1Q

16.1 Overview

This chapter describes how to configure the 802.1Q settings.

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. A VLAN group can be treated as an individual device. Each group can have its own rules about where and how to forward traffic. You can assign any ports on the P-79X to a VLAN group and configure the settings for the group. You may also set the priority level for traffic trasmitted through the ports.

Figure 97 802.1Q



16.1.1 What You Can Do in the 802.1Q Screens

- Use the **Group Setting** screen (Section 16.2 on page 163) to activate 802.1Q, specify the management VLAN group, display the VLAN groups and configure the settings for each VLAN group.
- Use the **Port Setting** screen (Section 16.3 on page 165) to configure the PVID.

16.1.2 What You Need to Know About 802.1Q

IEEE 802.1Q Tagged VLAN

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the device on which they were created. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

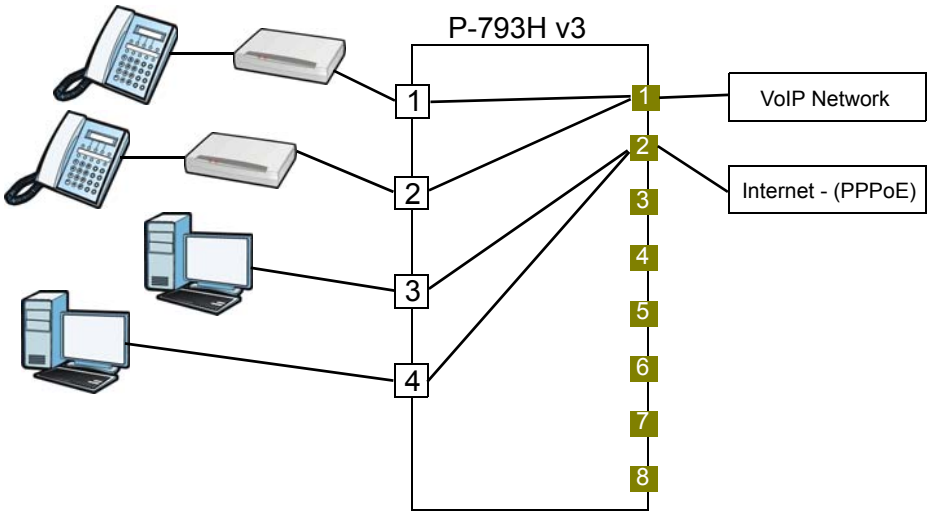
Forwarding Tagged and Untagged Frames

Each port on the device is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware device to an 802.1Q VLAN-unaware device, the P-79X first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware device to an 802.1Q VLAN-aware switch, the P-79X first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

Whether to tag an outgoing frame depends on the setting of the egress port on a per-VLAN, per-port basis (recall that a port can belong to multiple VLANs). If the tagging on the egress port is enabled for the VID of a frame, then the frame is transmitted as a tagged frame; otherwise, it is transmitted as an untagged frame.

16.1.3 802.1Q Example

This example shows how to configure the 802.1Q settings on the P-79X.



LAN1 and LAN2 are connected to ATAs (Analogue Telephone Adapters) and used for VoIP traffic.

You would start with the following steps.

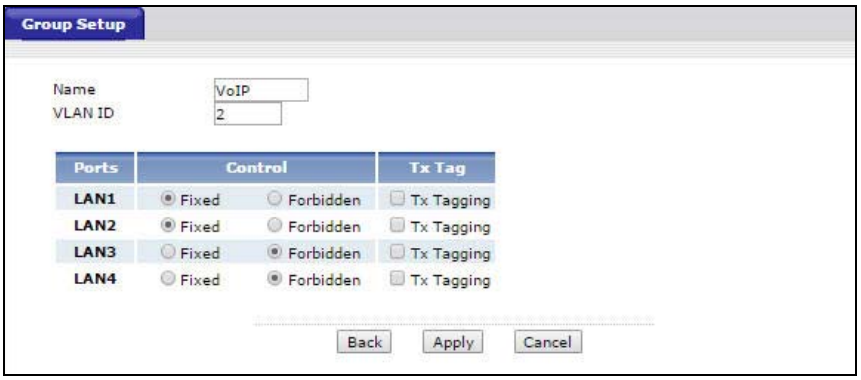
1 Click **Advanced** > **802.1Q** > **Group Setting**, and then click the **Edit** button to display the following screen.

2 In the **Name** field type VoIP to identify the group.

3 In the **VLAN ID** field type in 2 to identify the VLAN group.

4 In the **Control** field, select **Fixed** for LAN1and LAN2 to be permanent members of the VLAN group.

5 Click **Apply**.

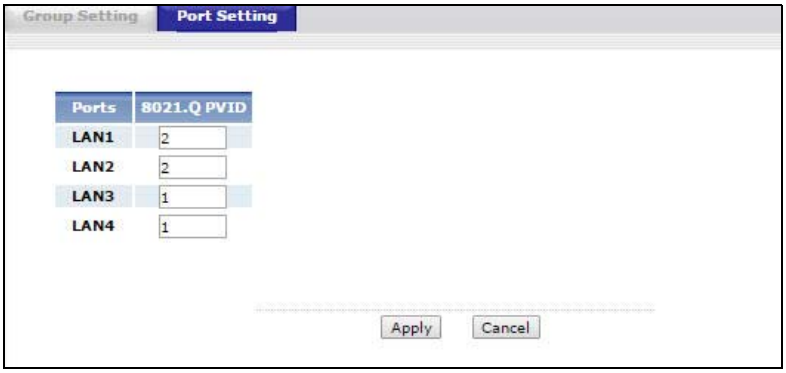


To set a high priority for VoIP traffic, follow these steps.

1 Click **Advanced** > **802.1Q** > **Port Setting** to display the following screen.

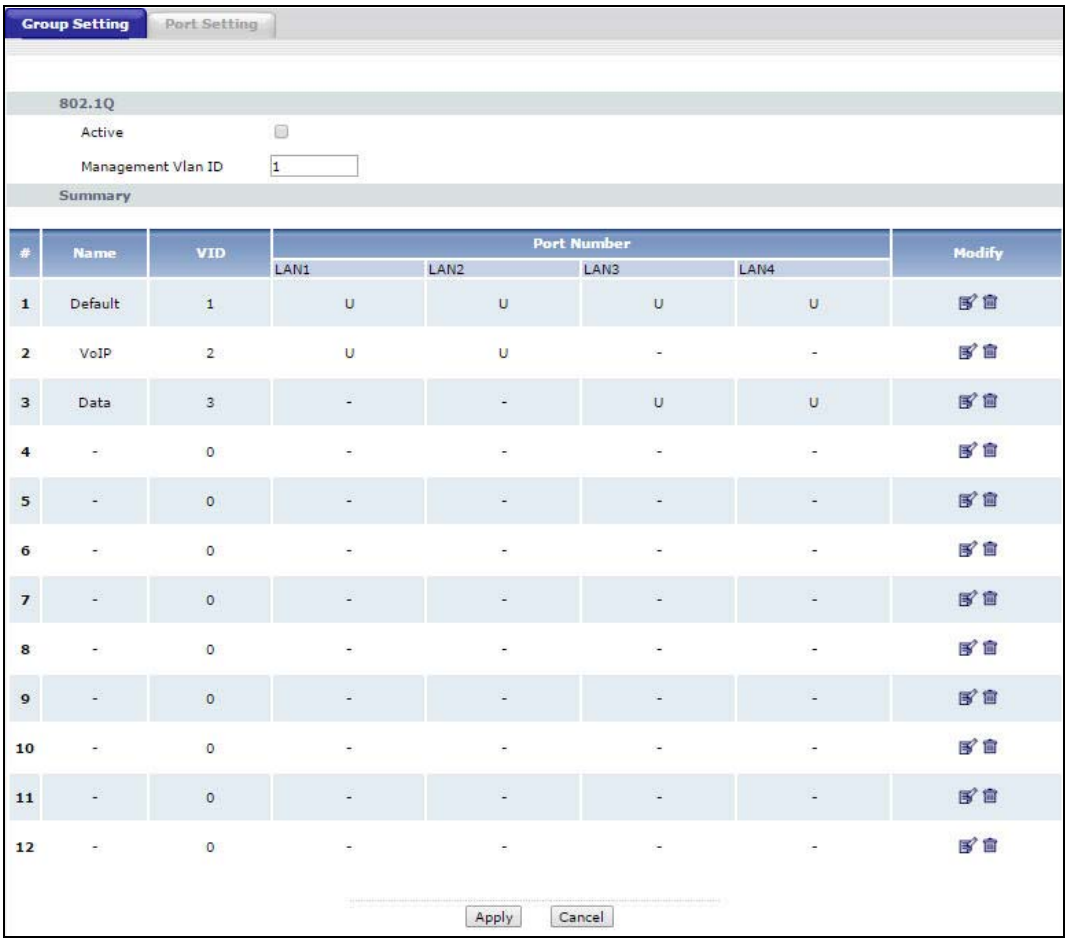
2 Type **2** in the **802.1Q PVID** column for LAN1and LAN2.

3 Click **Apply**.



Ports 3 and 4 are connected to desktop computers and are used for Internet traffic.

Follow the same steps as in VLAN2 to configure the settings for VLAN3. The summary screen should then display as follows.

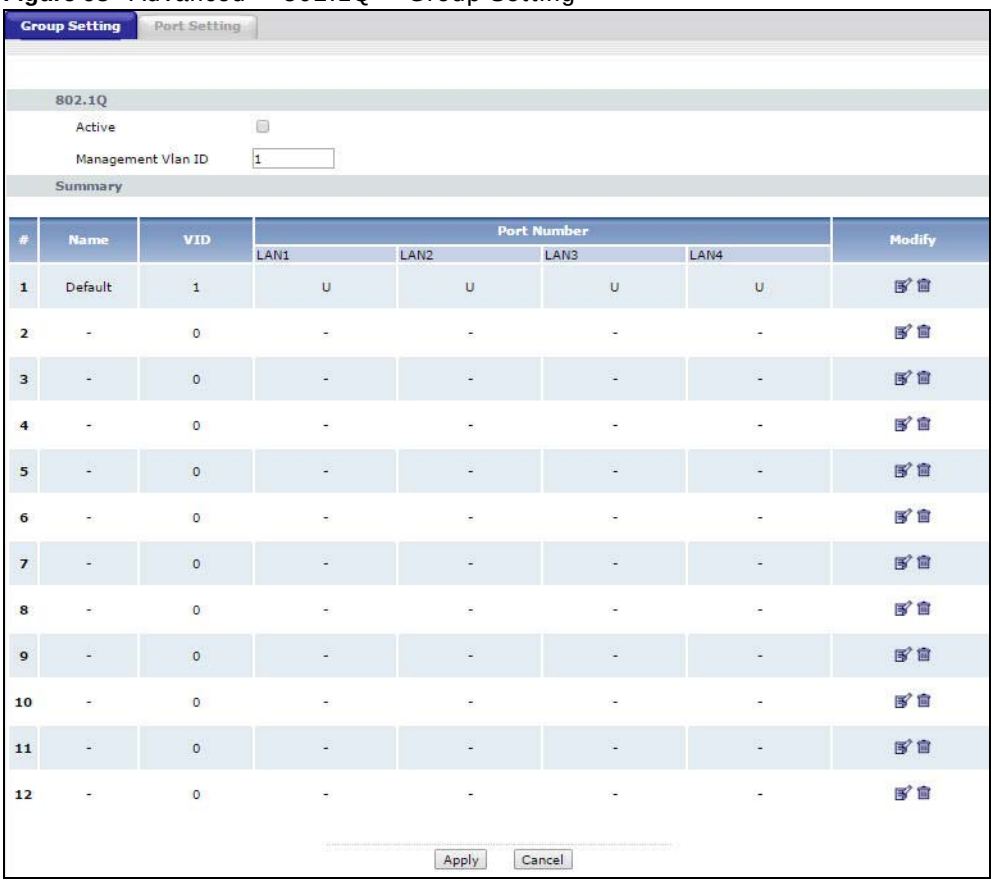


This completes the 802.1Q setup.

16.2 The 802.1Q Group Setting Screen

Use this screen to activate 802.1Q and display the VLAN groups. Click **Advanced > 802.1Q** to display the following screen.

Figure 98 Advanced > 802.1Q > Group Setting



The following table describes the labels in this screen.

Table 64 Advanced > 802.1Q > Group Setting

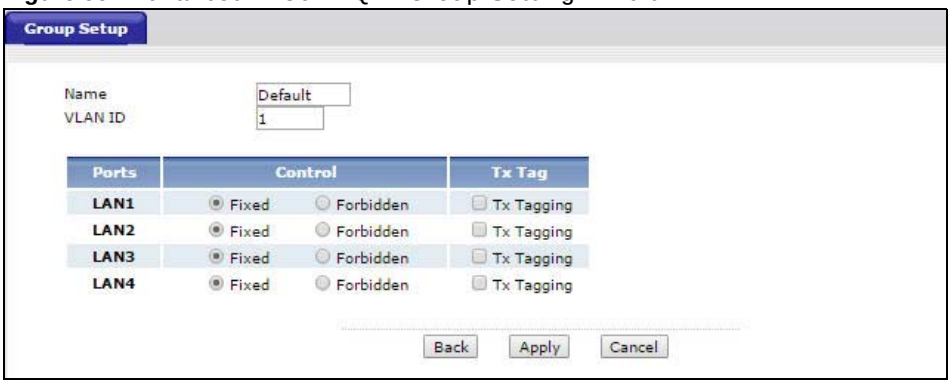
LABEL	DESCRIPTION
802.1Q	
Active	Select this check box to activate the 802.1Q feature.
Management Vlan ID	Enter the ID number of a VLAN group. All interfaces (ports and SSIDs) are in the management VLAN by default. If you disable the management VLAN, you will not be able to access the P-79X.
Summary	
#	This field displays the index number of the VLAN group.
Name	This field displays the name of the VLAN group.
VID	This field displays the ID number of the VLAN group.
Port Number	These columns display the VLAN's settings for each port. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as "**–**".
Modify	Click the **Edit** button to configure the ports in the VLAN group. Click the **Remove** button to delete the VLAN group.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

16.2.1 Editing 802.1Q Group Setting

Use this screen to configure the settings for each VLAN group.

In the **802.1Q** screen, click the **Edit** button from the **Modify** filed to display the following screen.

Figure 99 Advanced > 802.1Q > Group Setting > Edit



The following table describes the labels in this screen.

Table 65 Advanced > 802.1Q > Group Setting > Edit

LABEL	DESCRIPTION
Name	Enter a descriptive name for the VLAN group for identification purposes. The text may consist of up to 8 letters, numerals, “-”, “_” and “@”.
VLAN ID	Assign a VLAN ID for the VLAN group. The valid VID range is between 1 and 4094.
Ports	This field displays the types of ports available to join the VLAN group.
Control	Select **Fixed** for the port to be a permanent member of the VLAN group. Select **Forbidden** if you want to prohibit the port from joining the VLAN group.
Tx Tag	Select **Tx Tagging** if you want the port to tag all outgoing traffic trasmitted through this VLAN. You select this if you want to create VLANs across different devices and not just the P-79X.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

16.3 The 802.1Q Port Setting Screen

Use this screen to configure the PVID. Click **Advanced** > **802.1Q** > **Port Setting** to display the following screen.

Figure 100 Advanced > 802.1Q > Port Setting

The following table describes the labels in this screen.

Table 66 Advanced > 802.1Q > Port Setting

LABEL	DESCRIPTION
Ports	This field displays the types of ports available to join the VLAN group.
802.1Q PVID	Assign a VLAN ID for the port. The valid VID range is between 1 and 4094. The P-79X assigns the PVID to untagged frames or priority-tagged frames received on this port.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

17

Quality of Service (QoS)

17.1 Overview

Use the **QoS** screens to set up your P-79X to use QoS for traffic management.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control bandwidth. QoS allows the P-79X to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data are equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

The P-79X assigns each packet a priority and then queues the packet accordingly. Packets assigned with a high priority are processed more quickly than those with low priorities if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

17.1.1 What You Can Do in the QoS Screens

- Use the **General** screen (Section 17.2 on page 170) to enable QoS on the P-79X, decide allowable bandwidth using QoS and configure priority mapping settings for traffic that does not match a custom class.
- Use the **Class Setup** screen (Section 17.3 on page 171) to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.

17.1.2 What You Need to Know About QoS

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. Class of Service (CoS) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technologies include IEEE 802.1p layer 2 tagging and Differentiated Services (DiffServ or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit Type of Service (ToS) field in the IP header.

Tagging and Marking

In a QoS class, you can configure whether to add or change the DiffServ Code Point (DSCP) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Finding Out More

See Section 17.4 on page 175 for advanced technical information on QoS.

17.1.3 QoS Class Setup Example

In the following figure, your Internet connection has an upstream transmission speed of 50 Mbps. You configure a classifier to assign the highest priority queue (6) to VoIP traffic from the LAN interface, so that voice traffic would not get delayed when there is network congestion. Traffic from the boss's IP address (192.168.1.23 for example) is mapped to queue 5. Traffic that does not match these two classes are assigned priority queue based on the internal QoS mapping table on the P-79X.

Figure 101 QoS Example

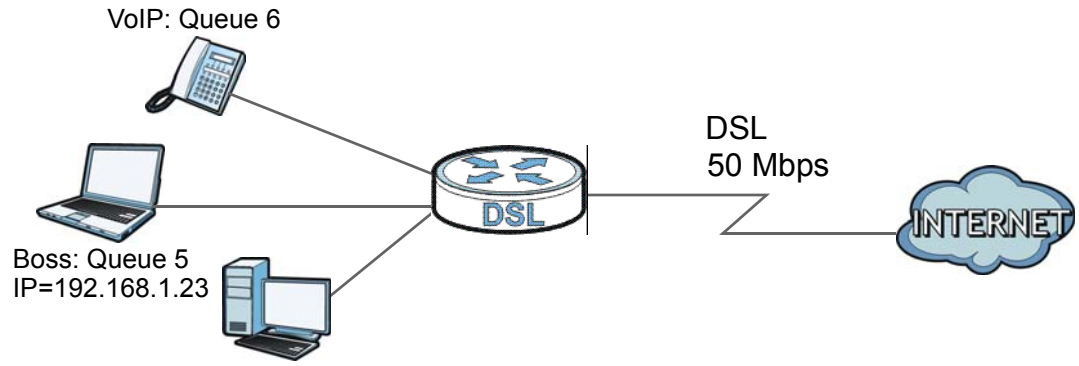


Figure 102 QoS Class Example: VoIP -1

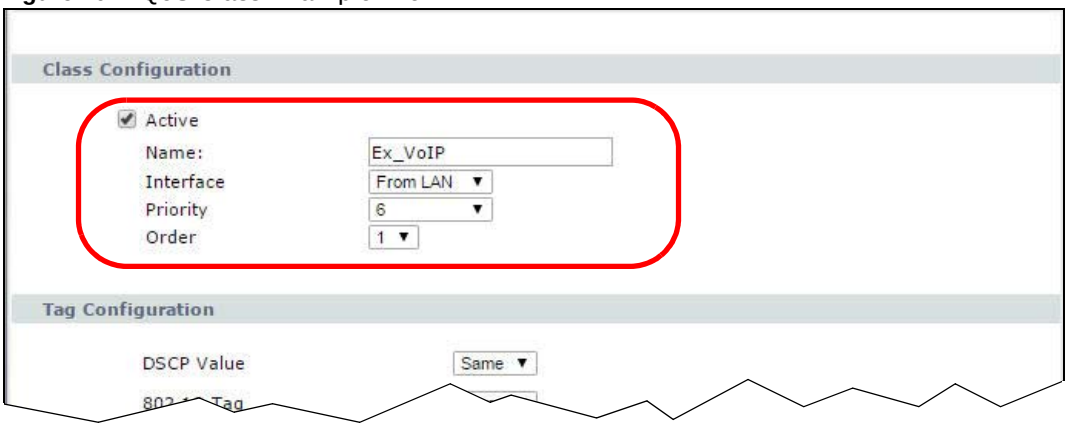


Figure 103 QoS Class Example: VoIP -2

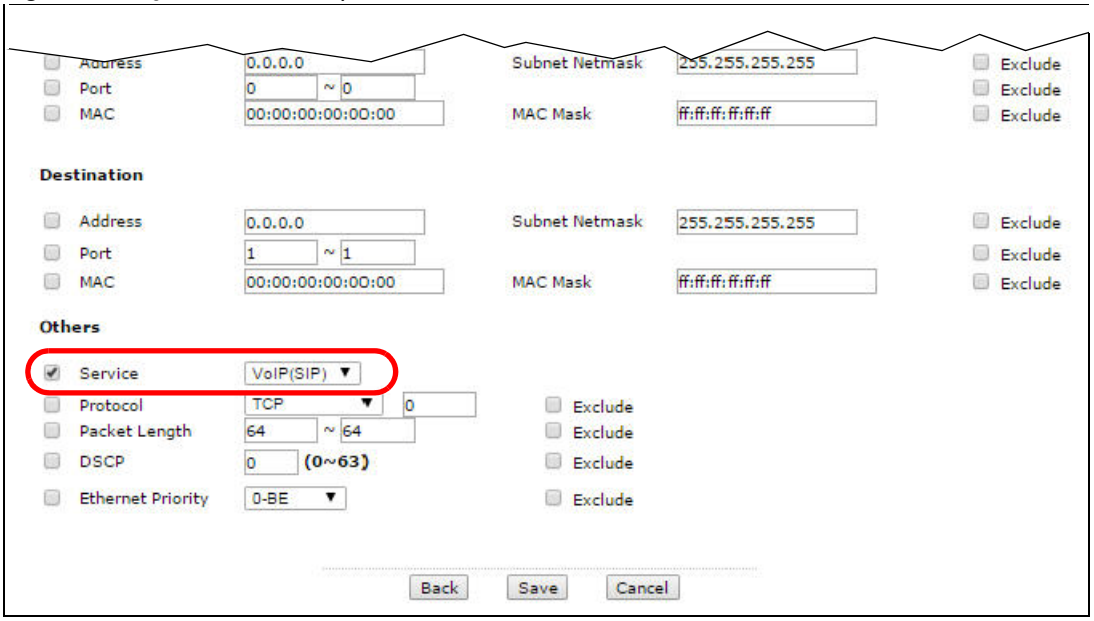


Figure 104 QoS Class Example: Boss -1

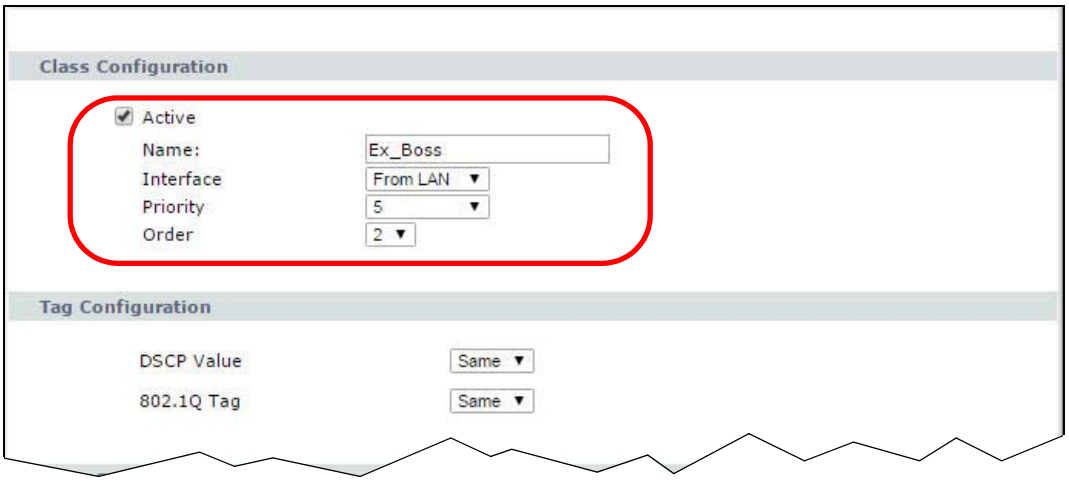
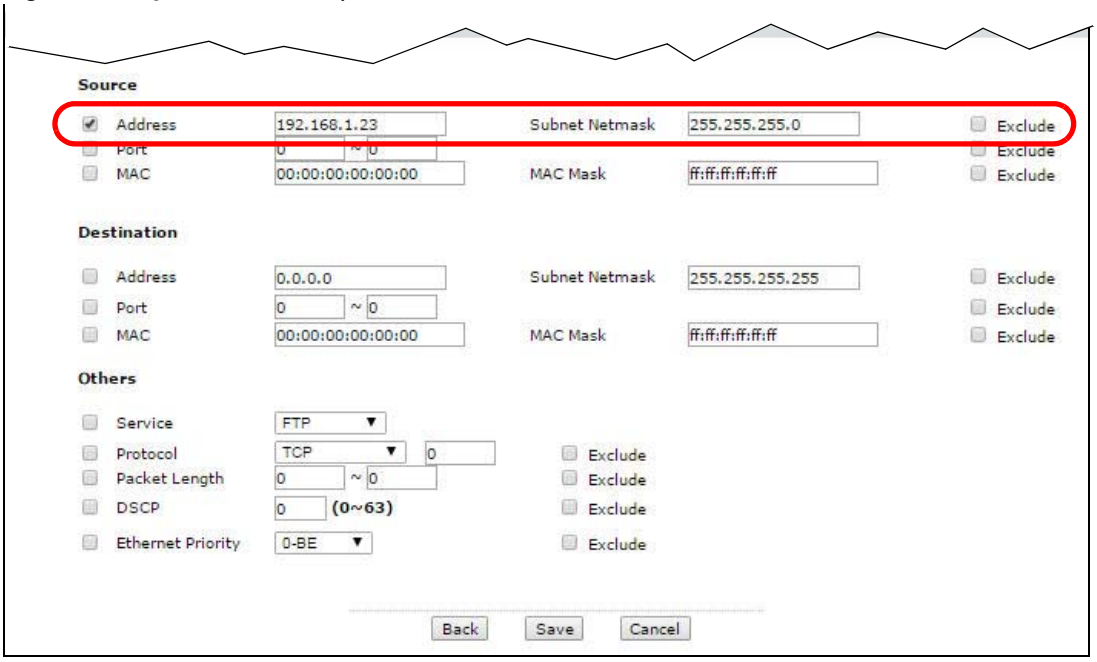


Figure 105 QoS Class Example: Boss -2

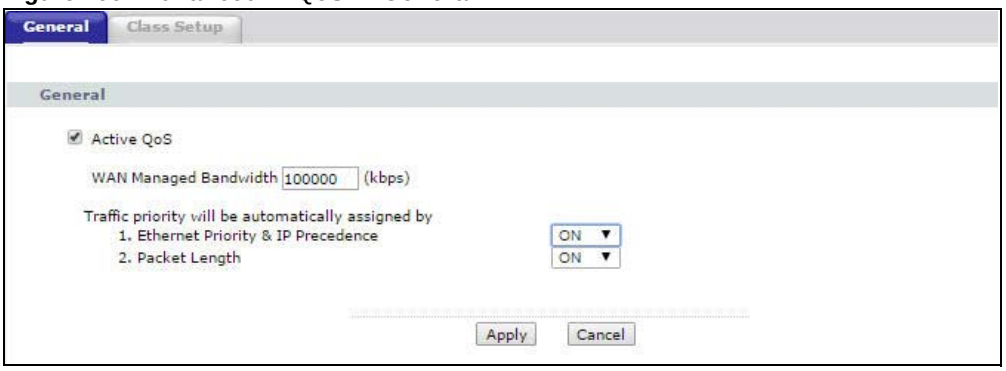


17.2 The QoS General Screen

Use this screen to enable or disable QoS and have the P-79X automatically assign priority to traffic according to the IEEE 802.1p priority level, IP precedence and/or packet length.

Click **Advanced > QoS** to open the screen as shown next.

Figure 106 Advanced > QoS > General



The following table describes the labels in this screen.

Table 67 Advanced > QoS > General

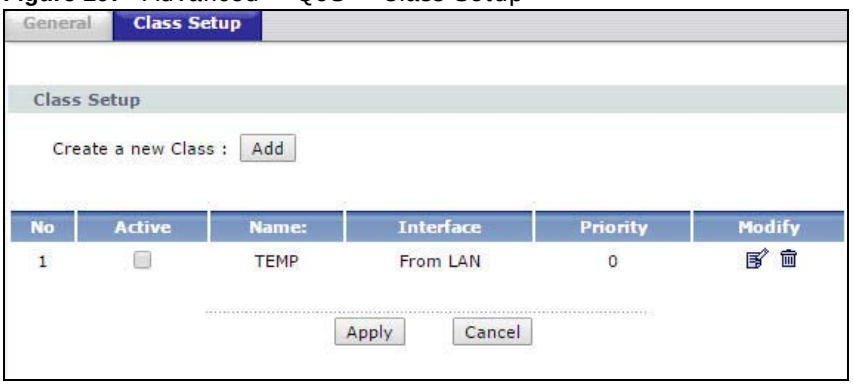
LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the P-79X forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
WAN Managed Bandwidth	Enter the amount of bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can set this number higher than the interface's actual transmission speed. This will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth. You can also set this number lower than the interface's actual transmission speed. This will cause the P-79X to not use some of the interface's available bandwidth.
Traffic priority will be automatically assigned by	These fields are ignored if traffic matches a class you configured in the **Class Setup** screen. If you select **ON** and traffic does not match a class configured in the **Class Setup** screen, the P-79X assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence and/or packet length. See Section 17.4.4 on page 177 for more information. If you select **OFF**, traffic which does not match a class is mapped to queue two.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

17.3 The Class Setup Screen

Use this screen to add, edit or delete classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Click **Advanced > QoS > Class Setup** to open the following screen.

Figure 107 Advanced > QoS > Class Setup



The following table describes the labels in this screen.

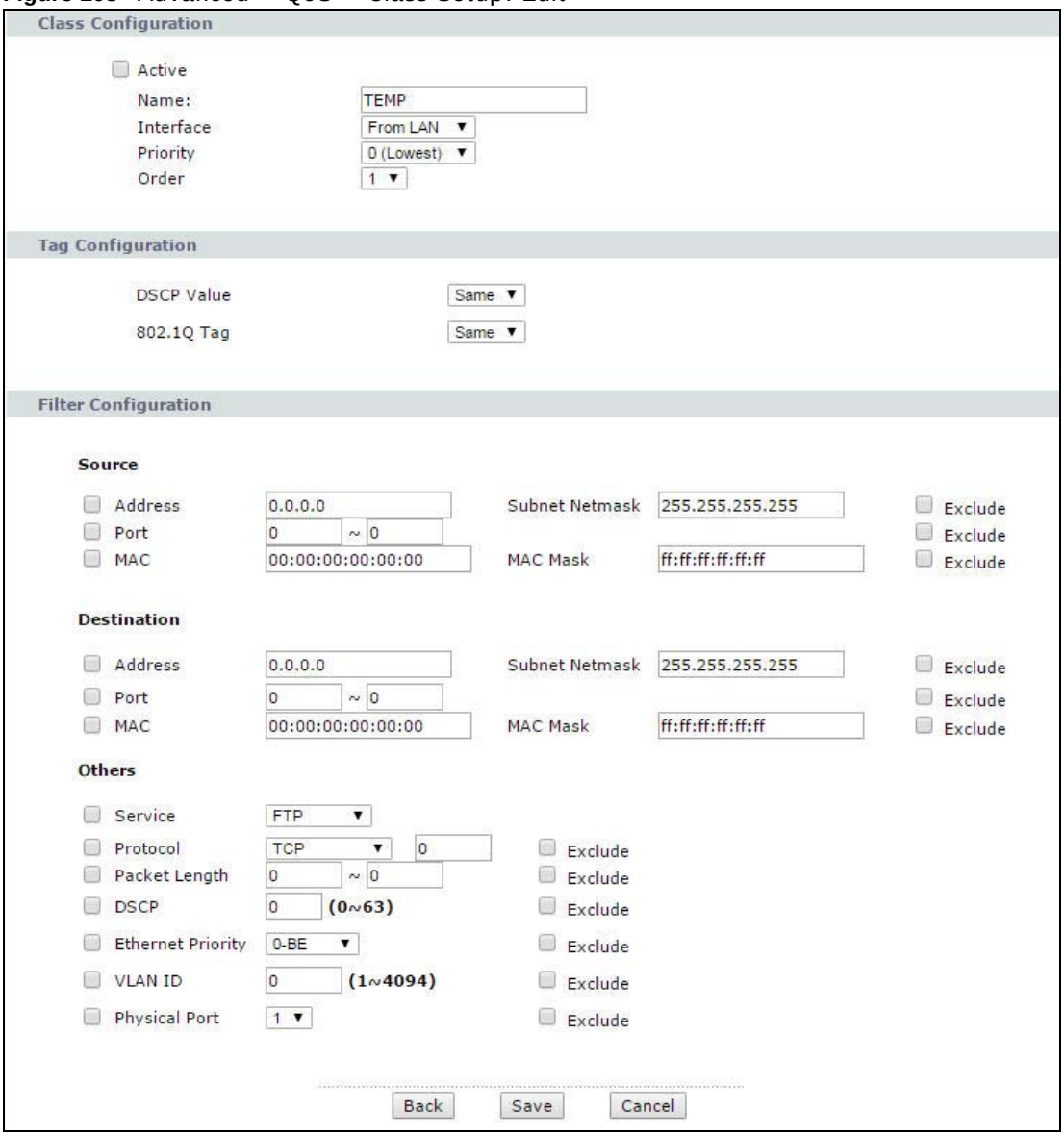
Table 68 Advanced > QoS > Class Setup

LABEL	DESCRIPTION
Create a new Class	Click **Add** to create a new classifier.
No	This is the number of each classifier. The ordering of the classifiers is important as the classifiers are applied in turn.
Active	Select the check box to enable this classifier.
Name	This is the name of the classifier.
Interface	This shows the interface from which traffic of this classifier should come.
Priority	This is the priority assigned to traffic of this classifier.
Modify	Click the Edit icon to go to the screen where you can edit the classifier. Click the Remove icon to delete an existing classifier.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

17.3.1 The Class Configuration Screen

Use this screen to configure a classifier. Click the **Add** button or the **Edit** icon in the **Modify** field to display the following screen.

Figure 108 Advanced > QoS > Class Setup: Edit



See Appendix F on page 279 for a list of commonly-used services. The following table describes the labels in this screen.

Table 69 Advanced > QoS > Class Setup: Edit

LABEL	DESCRIPTION
Class Configuration	
Active	Select the check box to enable this classifier.
Name	The text may consist of up to 20 letters, numerals and any printable character found on a typical English language keyboard.
Interface	Select from which interface traffic of this class should come.
Priority	Select a priority level (between 0 and 7) or select **Auto** to have the P-79X map the matched traffic to a queue according to the internal QoS mapping table. See Section 17.4.4 on page 177 for more information. "0" is the lowest priority level and "7" is the highest.

Table 69 Advanced > QoS > Class Setup: Edit (continued)

LABEL	DESCRIPTION
Order	This shows the ordering number of this classifier. Select an existing number for where you want to put this classifier and click **Apply** to move the classifier to the number you selected. For example, if you select 2, the classifier you are moving becomes number 2 and the previous classifier 2 gets pushed down one.
Tag Configuration	
DSCP Value	Select **Same** to keep the DSCP fields in the packets. Select **Auto** to map the DSCP value to 802.1 priority level automatically.
802.1Q Tag	Select **Same** to keep the priority setting and VLAN ID of the frames. Select **Auto** to map the 802.1 priority level to the DSCP value automatically.
Filter Configuration	Use the following fields to configure the criteria for traffic classification.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the source. 0 means any source port number. See *Appendix F on page 279* for some common services and port numbers.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the destination IP address in dotted decimal notation.
Subnet Netmask	Enter the destination subnet mask. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the destination. 0 means any source port number. See Appendix F on page 279 for some common services and port numbers.
MAC	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified destination MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.

Table 69 Advanced > QoS > Class Setup: Edit (continued)

LABEL	DESCRIPTION
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
Service	This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields. SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select the check box and select **VoIP(SIP)** from the drop-down list box to configure this classifier for traffic that uses SIP. File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select the check box and select **FTP** from the drop-down list box to configure this classifier for FTP traffic.
Protocol	Select this option and select the protocol (**TCP** or **UDP**) or select **User defined** and enter the protocol (service type) number. 0 means any protocol number.
Packet Length	Select this option and enter the minimum and maximum packet length (from 28 to 1500) in the fields provided.
DSCP	Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Ethernet Priority	Select this option and select a priority level (between 0 and 7) from the drop down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	Select this option and specify a VLAN ID number between 2 and 4094.
Physical Port	Select this option and select a LAN port.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

17.4 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

17.4.1 IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 70 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

17.4.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

17.4.3 DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

Differentiated Services (DiffServ) is a Class of Service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

17.4.4 Automatic Priority Queue Assignment

If you enable QoS on the P-79X, the P-79X can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the P-79X. On the P-79X, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 71 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

18

Dynamic DNS Setup

18.1 Overview

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

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

18.1.1 What You Need To Know About DDNS

DYNDNS Wildcard

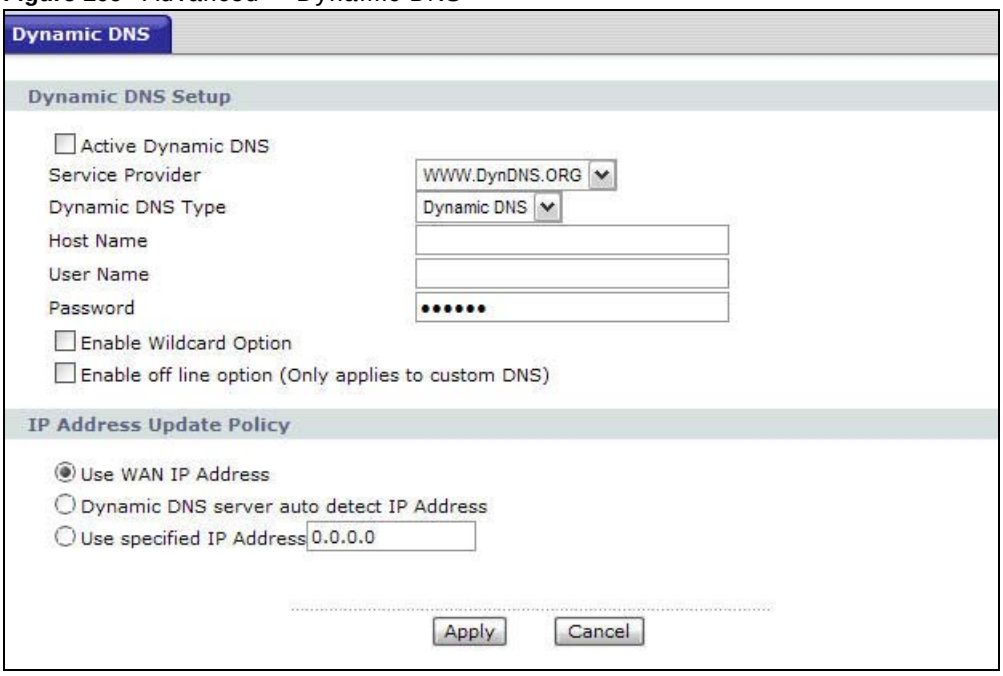
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

18.2 The Dynamic DNS Screen

Use this screen to change your P-79X's DDNS. Click **Advanced > Dynamic DNS**. The screen appears as shown.

Figure 109 Advanced > Dynamic DNS



The following table describes the fields in this screen.

Table 72 Advanced > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your P-79X by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when **CustomDNS** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.
Dynamic DNS server auto detect IP Address	Select this option only when there are one or more NAT routers between the P-79X and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the P-79X and the DDNS server.

Table 72 Advanced > Dynamic DNS (continued)

LABEL	DESCRIPTION
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

19

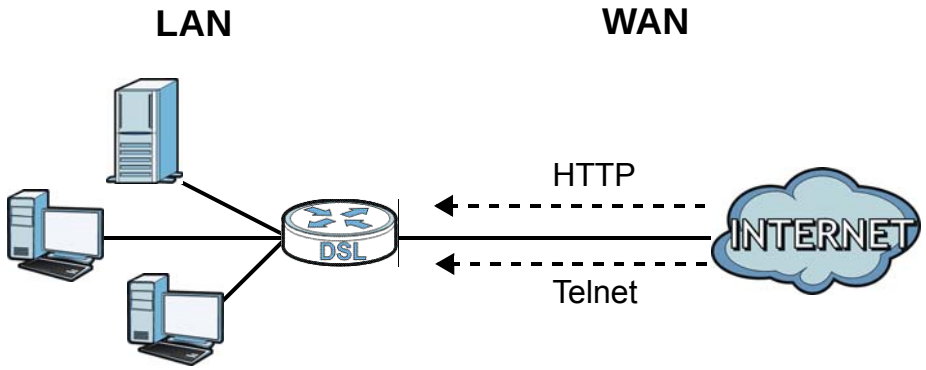
Remote Management

19.1 Overview

Remote management allows you to determine which services/protocols can access which P-79X interface (if any) from which computers.

The following figure shows remote management of the P-79X coming in from the WAN.

Figure 110 Remote Management From the WAN



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

You may manage your P-79X from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (WAN and LAN)
- None (Disable)

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

You may only have one remote management session running at a time. The P-79X automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1 Telnet

2 HTTP

19.1.1 What You Can Do in the Remote Management Screens

- Use the **WWW** screen (Section 19.2 on page 183) to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the P-79X.
- Use the **Telnet** screen (Section 19.3 on page 184) to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the P-79X.
- Use the **SSH** screen (Section 19.4 on page 184) to configure through which interface(s) and from which IP address(es) users can use SSH to manage the P-79X.
- Use the **SNMP** screen (Section 19.5 on page 185) to configure your P-79X's settings for Simple Network Management Protocol management.
- Use the **DNS** screen (Section 19.6 on page 188) to configure through which interface(s) and from which IP address(es) users can send DNS queries to the P-79X.
- Use the **ICMP** screen (Section 19.7 on page 189) to set whether or not your P-79X will respond to pings and probes for services that you have not made available.
- Use the **CWMP** screen (Section 19.8 on page 190) to configure your P-79X to be managed by an ACS.

19.1.2 What You Need to Know About Remote Management

Remote Management Limitations

Remote management does not work when:

- You have not enabled that service on the interface in the corresponding remote management screen.
- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the P-79X will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- There is a firewall rule that blocks it.

Remote Management and NAT

When NAT is enabled:

- Use the P-79X's WAN IP address when configuring from the WAN.

- Use the P-79X's LAN IP address when configuring from the LAN.

System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The P-79X automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

19.2 The WWW Screen

Use this screen to specify how to connect to the P-79X from a web browser, such as Internet Explorer. You can also specify which IP addresses the access can come from.

Note: If you disable the **WWW** service in this screen, then the P-79X blocks all HTTP connection attempts.

19.2.1 Configuring the WWW Screen

Click **Advanced > Remote MGMT** to display the **WWW** screen.

Figure 111 Advanced > Remote MGMT > WWW

The following table describes the labels in this screen.

Table 73 Advanced > Remote MGMT > WWW

LABEL	DESCRIPTION
Port	You may change the server port number for a service, if needed. However, you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the P-79X using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the P-79X using this service. Select **All** to allow any computer to access the P-79X using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the P-79X using this service.

Table 73 Advanced > Remote MGMT > WWW

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

19.3 The Telnet Screen

You can use Telnet to access the P-79X's command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

Click **Advanced > Remote MGMT** > **Telnet** tab to display the screen as shown.

Figure 112 Advanced > Remote MGMT > Telnet

The following table describes the labels in this screen.

Table 74 Advanced > Remote MGMT > Telnet

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the P-79X using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the P-79X using this service. Select **All** to allow any computer to access the P-79X using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the P-79X using this service.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

19.4 The SSH Screen

You can use SSH (Secure Shell) to access the P-79X's command line interface. Specify from which IP address the access can come.

Click **Advanced > Remote MGMT** > **SSH**. The screen appears as shown.

Figure 113 Advanced > Remote MGMT> SSH

The following table describes the labels in this screen.

Table 75 Advanced > Remote MGMT > SSH

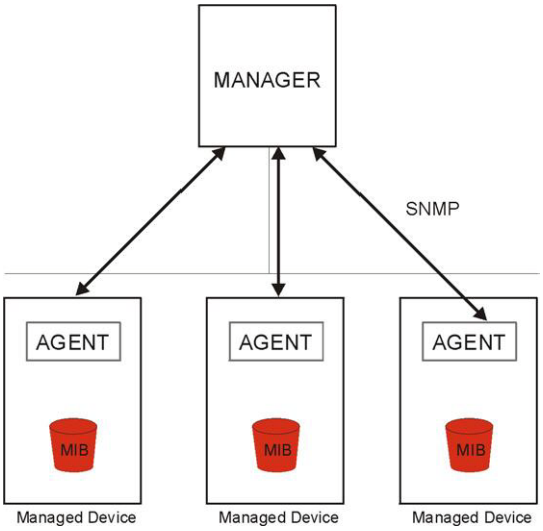
LABEL	DESCRIPTION
Port	This field displays the port number of the SSH service. You must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the P-79X using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the P-79X using this service. Select **All** to allow any computer to access the P-79X using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the P-79X using this service.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

19.5 The SNMP Screen

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your P-79X supports SNMP agent functionality, which allows a manager station to manage and monitor the P-79X through the network. The P-79X supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

Note: SNMP is only available if TCP/IP is configured.

Figure 114 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the P-79X). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

19.5.1 Supported MIBs

The P-79X supports MIB II, which is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

19.5.2 SNMP Traps

The P-79X will send traps to the SNMP manager when any one of the following events occurs:

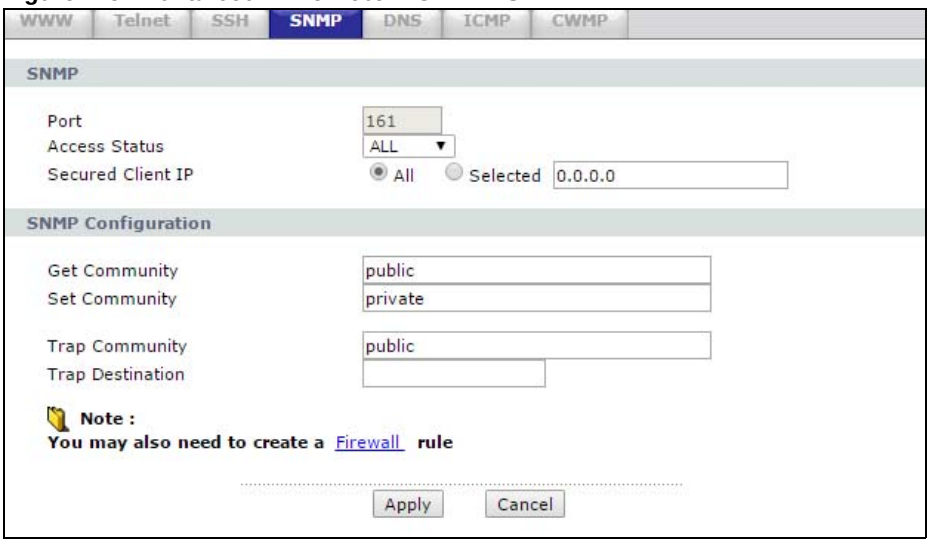
Table 76 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

19.5.3 Configuring SNMP

To change your P-79X's SNMP settings, click **Advanced > Remote MGMT** > **SNMP**. The screen appears as shown.

Figure 115 Advanced > Remote MGMT > SNMP



The following table describes the labels in this screen.

Table 77 Advanced > Remote MGMT > SNMP

LABEL	DESCRIPTION
SNMP	
Port	This field displays the port number of the SNMP service. You must use the same port number in order to use that service for remote management.

Table 77 Advanced > Remote MGMT > SNMP

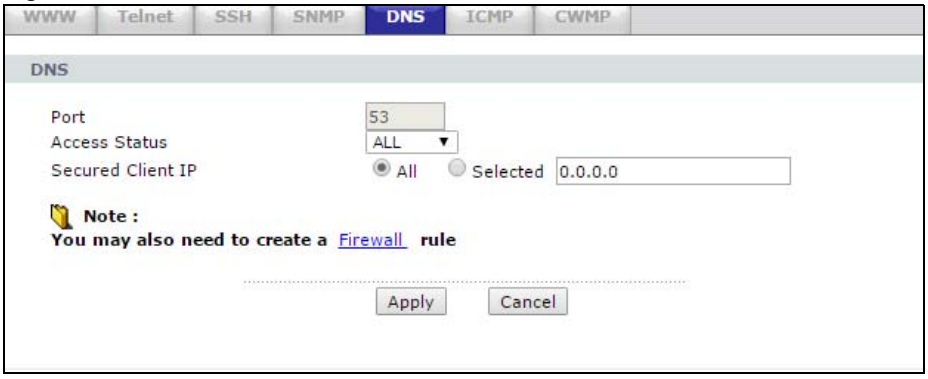
LABEL	DESCRIPTION
Access Status	Select the interface(s) through which a computer may access the P-79X using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the P-79X using this service. Select **All** to allow any computer to access the P-79X using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the P-79X using this service.
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
TrapCommunity	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
TrapDestination	Type the IP address of the station to send your SNMP traps to.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

19.6 The DNS Screen

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to Chapter 8 on page 74 for background information.

Use this screen to set from which IP address the P-79X will accept DNS queries and on which interface it can send them your P-79X’s DNS settings. This feature is not available when the P-79X is set to bridge mode. Click **Advanced > Remote MGMT** > **DNS** to change your P-79X’s DNS settings.

Figure 116 Advanced > Remote MGMT > DNS



The following table describes the labels in this screen.

Table 78 Advanced > Remote MGMT > DNS

LABEL	DESCRIPTION
Port	The DNS service port number is 53 and cannot be changed here.
Access Status	Select the interface(s) through which a computer may send DNS queries to the P-79X.
Secured Client IP	A secured client is a “trusted” computer that is allowed to send DNS queries to the P-79X. Select **All** to allow any computer to send DNS queries to the P-79X. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the P-79X.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

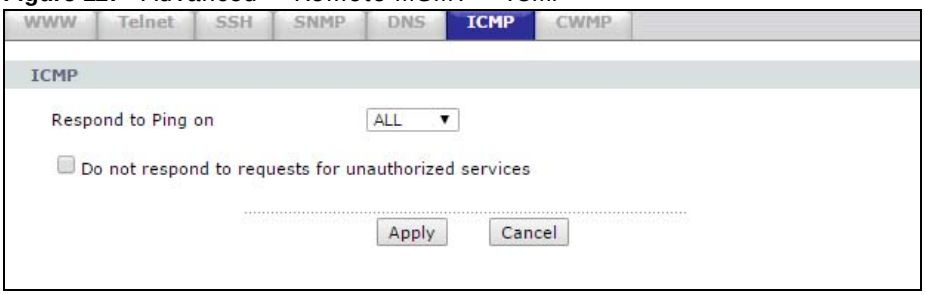
19.7 The ICMP Screen

To change your P-79X’s security settings, click **Advanced > Remote MGMT** > **ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your P-79X, an ICMP response packet is automatically returned. This allows the outside user to know the P-79X exists. Your P-79X supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your P-79X when unsupported ports are probed.

Note: If you want your device to respond to pings and requests for unauthorized services, you may also need to configure the firewall anti probing settings to match.

Figure 117 Advanced > Remote MGMT > ICMP



The following table describes the labels in this screen.

Table 79 Advanced > Remote MGMT > ICMP

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The P-79X will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the P-79X by probing for unused ports. If you select this option, the P-79X will not respond to port request(s) for unused ports, thus leaving the unused ports and the P-79X unseen. If this option is not selected, the P-79X will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the P-79X's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the P-79X reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

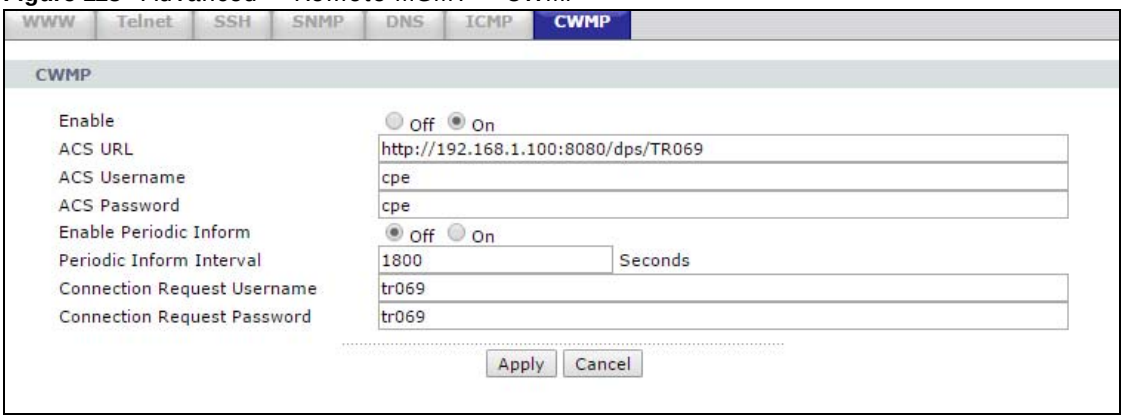
19.8 The CWMP Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your P-79X, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the P-79X, modify settings, perform firmware upgrades as well as monitor and diagnose the P-79X. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Advanced > Remote MGMT** > **CWMP** to open the following screen. Use this screen to configure your P-79X to be managed by an ACS.

Figure 118 Advanced > Remote MGMT > CWMP



The following table describes the labels in this screen.

Table 80 Advanced > Remote MGMT> CWMP

LABEL	DESCRIPTION
Enable	Select **On** for the P-79X to send periodic inform via TR-069 on the WAN. Otherwise, select **Off**.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS Username	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
Enable Periodic Inform	Select **On** for the P-79X to send periodic inform via TR-069 on the WAN. Otherwise, select **Off**.
Periodic Inform Interval	Enter the time interval (in seconds) at which the P-79X sends information to the auto-configuration server.
Connection Request Username	Enter the connection request user name. When the ACS makes a connection request to the P-79X, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the P-79X, this password is used to authenticate the ACS.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

20

Universal Plug-and-Play (UPnP)

20.1 Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

20.1.1 What You Can Do in the UPnP Screen

Use the **UPnP** screen (Section 20.2 on page 193) to enable UPnP on the P-79X and allow UPnP-enabled applications to automatically configure the P-79X.

20.1.2 What You Need to Know About UPnP

Identifying UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the P-79X allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

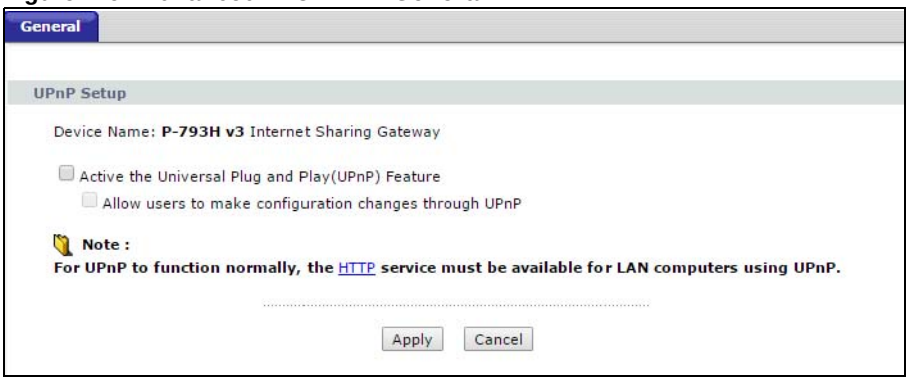
See the following sections for examples of installing and using UPnP.

20.2 The UPnP Screen

Use the following screen to configure the UPnP settings on your P-79X. Click **Advanced > UPnP** to display the screen shown next.

See Section 20.1 on page 192 for more information.

Figure 119 Advanced > UPnP > General



The following table describes the fields in this screen.

Table 81 Advanced > UPnP > General

LABEL	DESCRIPTION
Active the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the P-79X's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the P-79X so that they can communicate through the P-79X, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

20.3 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows XP.

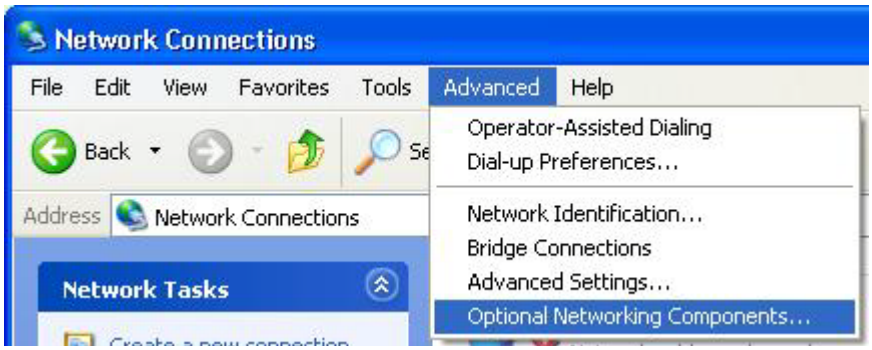
Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

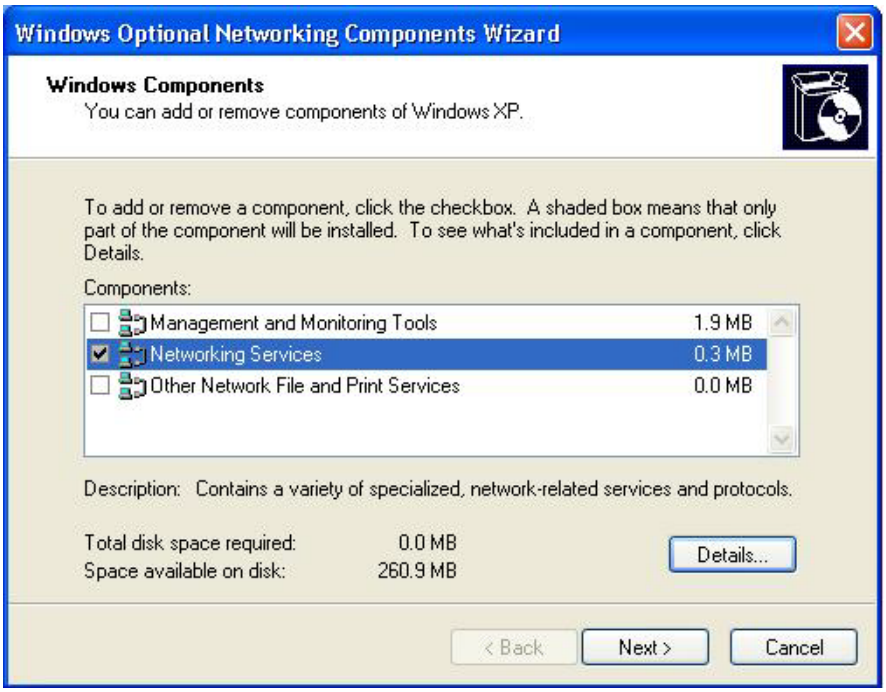
1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

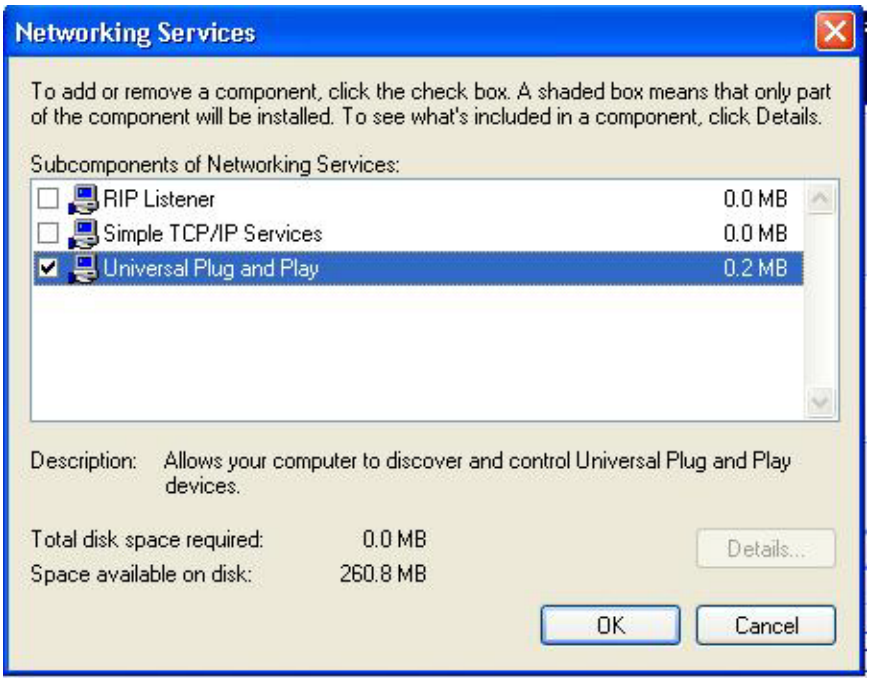
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.



4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.



5 In the **Networking Services** window, select the **Universal Plug and Play** check box.



6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

20.4 Using UPnP in Windows XP Example

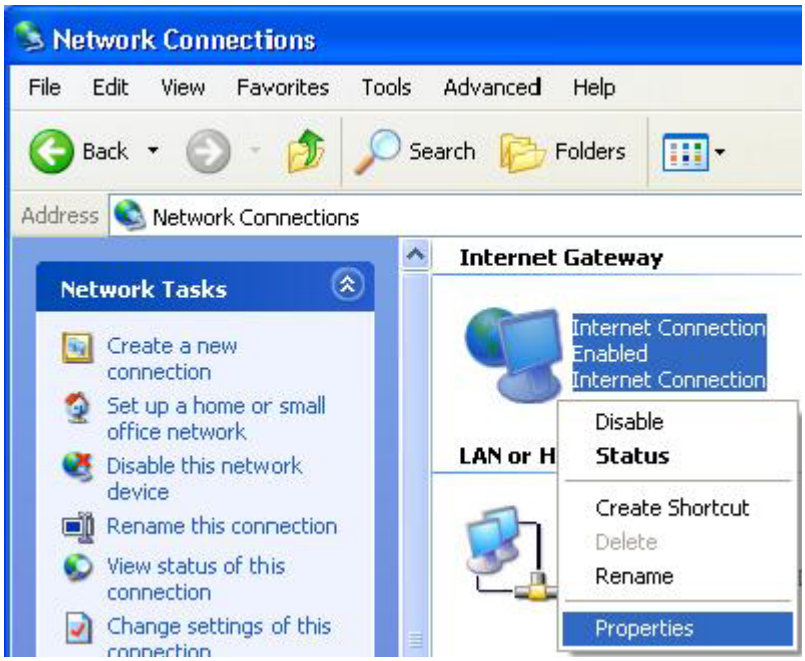
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the P-79X.

Make sure the computer is connected to a LAN port of the P-79X. Turn on your computer and the P-79X.

Auto-discover Your UPnP-enabled Network Device

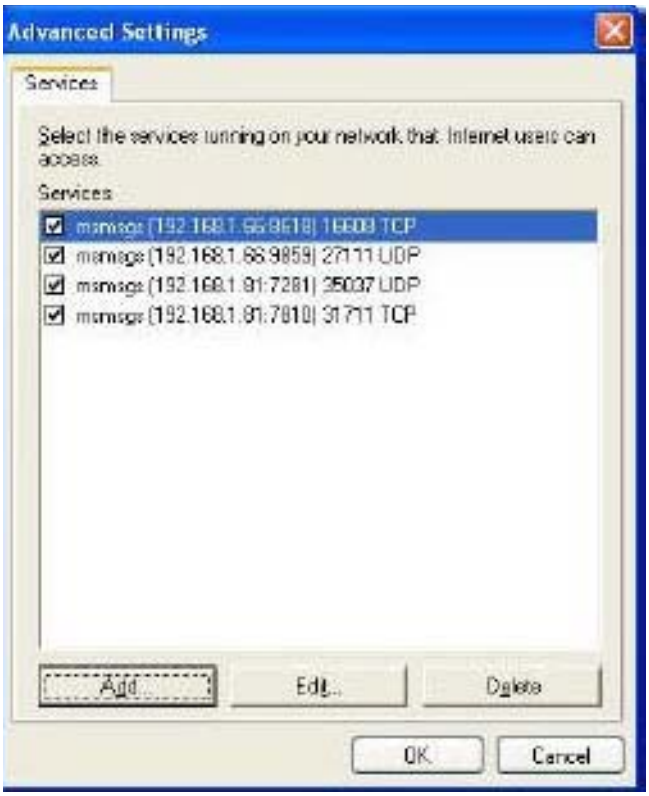
1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

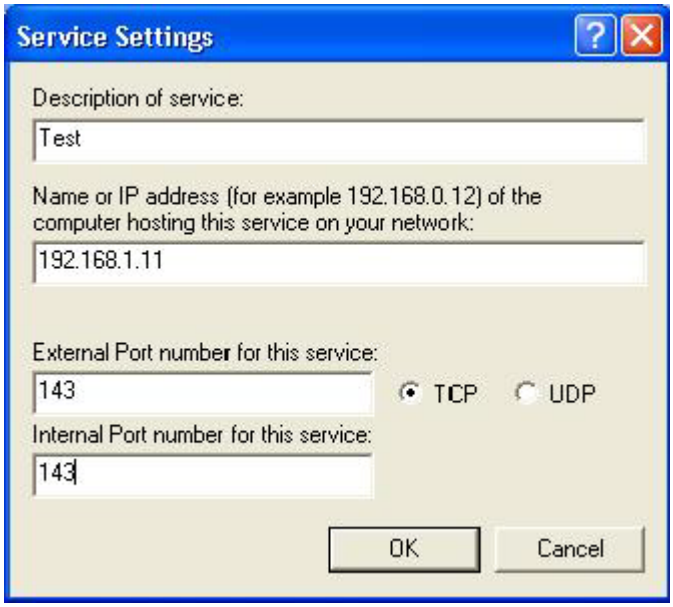
2 Right-click the icon and select **Properties**.



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.





5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

7 Double-click on the icon to display your current Internet connection status.

Web Configurator Easy Access

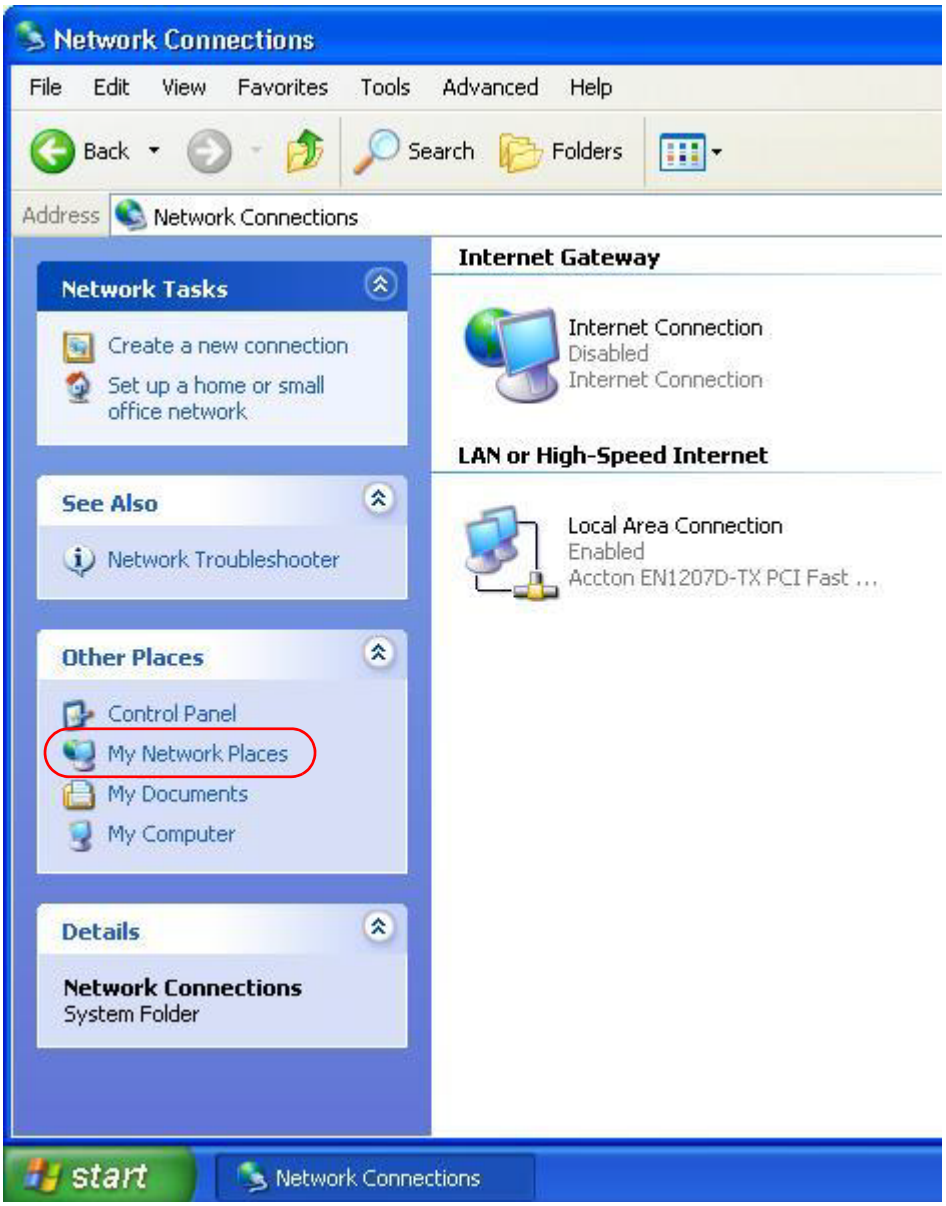
With UPnP, you can access the web-based configurator on the P-79X without finding out the IP address of the P-79X first. This comes helpful if you do not know the IP address of the P-79X.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your P-79X and select **Invoke**. The web configurator login screen displays.

6 Right-click on the icon for your P-79X and select **Properties**. A properties window displays with basic information about the P-79X.

21

System Settings

21.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

21.1.1 What You Can Do in the System Settings Screens

- Use the **General** screen (Section 21.2 on page 201) to configure system settings.
- Use the **Time Setting** screen (Section 21.3 on page 203) to set the system time.

21.1.2 What You Need to Know About System Settings

DHCP

DHCP (Dynamic Host Configuration Protocol) is a method of allocating IP addresses to devices on a network from a DHCP Server. Often your ISP or a router on your network performs this function.

LAN

A LAN (local area network) is typically a network which covers a small area, made up of computers and other devices which share resources such as Internet access, printers etc.

21.2 The General Screen

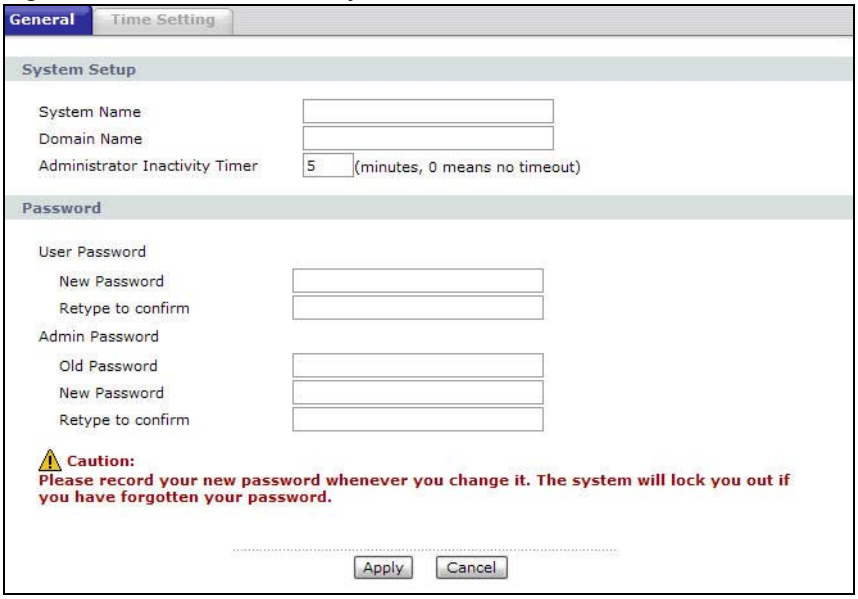
Use this screen to configure system settings such as the system and domain name, inactivity timeout interval and system password.

The **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". Find the system name of your Windows computer by following one of the steps below.

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the P-79X **System Name**.

Click **Maintenance > System** to open the **General** screen.

Figure 120 Maintenance > System > General



The following table describes the labels in this screen.

Table 82 Maintenance > System > General

LABEL	DESCRIPTION
System Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name. The **Domain Name** entry is propagated to the DHCP clients on the LAN.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or telnet) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password	
User Password	
New Password	Type your new user password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the P-79X.
Retype to confirm	Type the new password again for confirmation.
Admin Password	
Old Password	Type the default password or the existing password you use to access the system in this field.

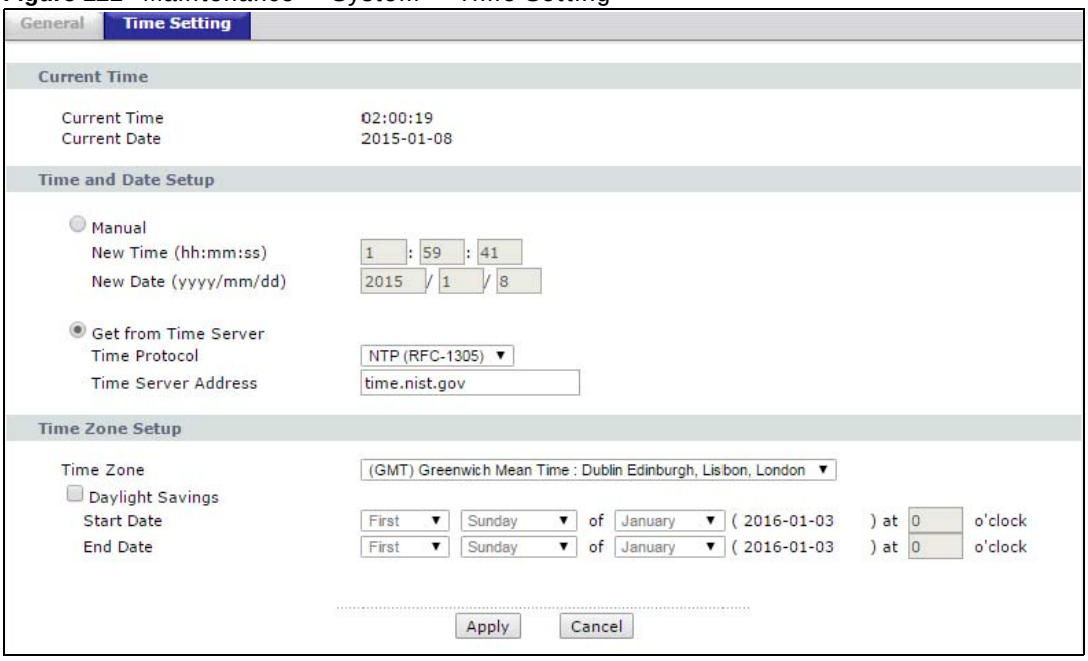
Table 82 Maintenance > System > General

LABEL	DESCRIPTION
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the P-79X.
Retype to confirm	Type the new password again for confirmation.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

21.3 The Time Setting Screen

Use this screen to configure the P-79X's time based on your local time zone. To change your P-79X's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown.

Figure 121 Maintenance > System > Time Setting



The following table describes the fields in this screen.

Table 83 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time	
Current Time	This field displays the time of your P-79X. Each time you reload this page, the P-79X synchronizes the time with the time server.
Current Date	This field displays the date of your P-79X. Each time you reload this page, the P-79X synchronizes the date with the time server.

Table 83 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the P-79X get the time and date from the time server you specified below.
Time Protocol	Select the time service protocol that your time server sends when you turn on the P-79X. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305)**, is similar to Time (RFC 868).
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 83 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

22

Logs

22.1 Overview

This chapter contains information about configuring general log settings and viewing the P-79X's logs.

The web configurator allows you to choose which categories of events and/or alerts to have the P-79X log and then display the logs or have the P-79X send them to an administrator (as e-mail) or to a syslog server.

22.1.1 What You Can Do in the Log Screens

- Use the **View Log** screen (Section 22.2 on page 206) to see the logs for the categories that you selected in the **Log Settings** screen.
- Use The **Log Settings** screen (Section 22.3 on page 207) to configure the mail server, the syslog server, when to send logs and what logs to send.

22.1.2 What You Need To Know About Logs

Alerts

An alert is a message that is enabled as soon as the event occurs. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Logs

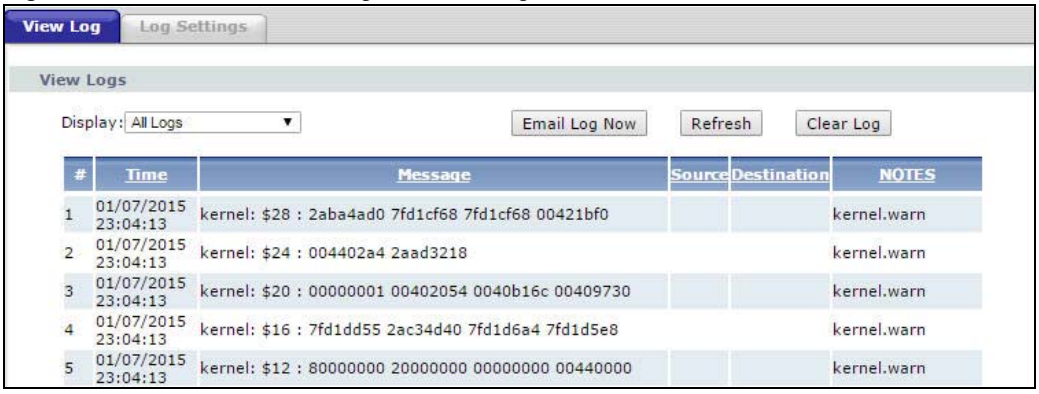
A log is a message about an event that occurred on your P-79X. For example, when someone logs in to the P-79X, you can set a schedule for how often logs should be enabled, or sent to a syslog server.

22.2 The View Log Screen

Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 22.3 on page 207). Click **Maintenance > Logs** to open the **View Log** screen.

Entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries by that column's criteria. Click the heading cell again to reverse the sort order. A triangle indicates ascending or descending sort order.

Figure 122 Maintenance > Logs > View Log



The following table describes the fields in this screen.

Table 84 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** screen display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Email Log Now	Click this to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**).
Refresh	Click this to renew the log screen.
Clear Log	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.

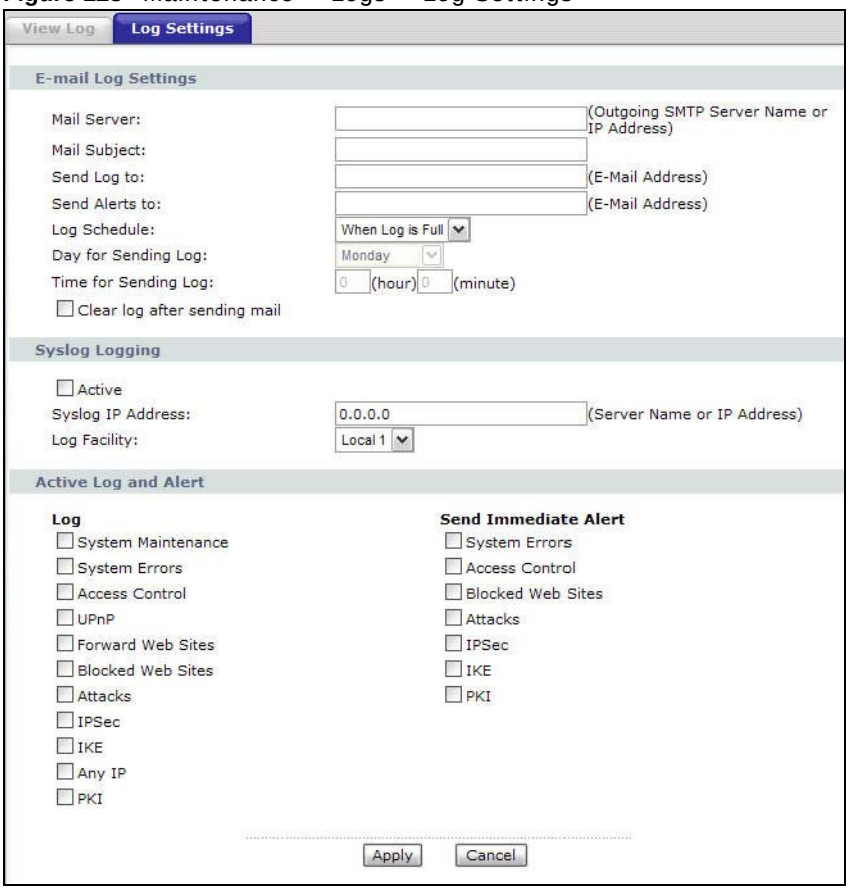
22.3 The Log Settings Screen

Use the **Log Settings** screen to configure the mail server, the syslog server, when to send logs and what logs to send.

To change your P-79X's log settings, click **Maintenance > Logs** > **Log Settings**. The screen appears as shown.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full. Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 123 Maintenance > Logs > Log Settings



The following table describes the fields in this screen.

Table 85 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the P-79X sends. Not all P-79X models have this field.
Send Log to	The P-79X sends logs to the e-mail address specified in this field. If this field is left blank, the P-79X does not send logs via e-mail.
Send Alerts to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.

Table 85 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the P-79X sends an E-mail of the logs.
Syslog Logging	The P-79X sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the P-79X to send E-mail alerts immediately.
Apply	Click this to save your customized settings and exit this screen.
Cancel	Click this to restore your previously saved settings.

22.4 SMTP Error Messages

If there are difficulties in sending e-mail the following error message appears.

“SMTP action request failed. ret= ??". The “??"are described in the following table.

Table 86 SMTP Error Messages

-1 means P-79X out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail

Table 86 SMTP Error Messages

-7 means DATA fail
-8 means mail data send fail

22.4.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- "End of Log" message shows that a complete log has been sent.

Figure 124 E-mail Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
.....{snip}.....
.....{snip}.....
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log
```

22.5 Log Descriptions

This section provides descriptions of example log messages.

Table 87 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
WAN interface gets IP: %s	A WAN interface got a new IP address from the DHCP, PPPoE, or dial-up server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.

Table 87 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Successful WEB login	Someone has logged on to the router's web configurator interface.
WEB login failed	Someone has failed to log on to the router's web configurator interface.
Successful TELNET login	Someone has logged on to the router via telnet.
TELNET login failed	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the router via ftp.
FTP login failed	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Starting Connectivity Monitor	Starting Connectivity Monitor.
Time initialized by Daytime Server	The router got the time and date from the Daytime server.
Time initialized by Time server	The router got the time and date from the time server.
Time initialized by NTP server	The router got the time and date from the NTP server.
Connect to Daytime server fail	The router was not able to connect to the Daytime server.
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router’s SSH server.
SSH login failed	Someone has failed to log on to the router’s SSH server.
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

Table 88 System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.

Table 89 Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

Table 90 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out.Default timeout values:ICMP idle timeout (s): 60UDP idle timeout (s): 60TCP connection (three way handshaking) timeout (s): 30TCP FIN-wait timeout (s): 60TCP idle (established) timeout (s): 3600
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst").

Table 91 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set: %d, rule: %d)	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see Table 100 on page 216.

Table 92 ICMP Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

Table 93 CDR Logs

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID.For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s	The PPPoE, PPTP or dial-up call is connected.
board %d line %d channel %d, call %d, %s C02 Call Terminated	The PPPoE, PPTP or dial-up call was disconnected.

Table 94 PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection's Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection's Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection's Internet Protocol Control Protocol stage is starting.

Table 94 PPP Logs (continued)

LOG MESSAGE	DESCRIPTION
ppp:IPCP Opening	The PPP connection's Internet Protocol Control Protocol stage is opening.
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 95 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 96 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: block keyword	The content of a requested web page matched a user defined keyword.
%s	The system forwarded web content.

For type and code details, see Table 100 on page 216.

Table 97 Attack Logs

LOG MESSAGE	DESCRIPTION
attack [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack.
land [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.
ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.

Table 97 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.

Table 98 802.1X Logs

LOG MESSAGE	DESCRIPTION
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.
No Server to authenticate user.	There is no authentication server to authenticate a user.

Table 99 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(L to L/P-79X)	LAN to LAN/P-79X	ACL set for packets traveling from the LAN to the LAN or the P-79X.
(W to W/P-79X)	WAN to WAN/P-79X	ACL set for packets traveling from the WAN to the WAN or the P-79X.

Table 100 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 101 Syslog Logs

LOG MESSAGE	DESCRIPTION
<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>	"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to RFC 2408 for detailed information on each type.

Table 102 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

23

Tools

23.1 Overview

This chapter explains how to upload new firmware, manage configuration files and restart your P-79X.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your P-79X.

23.1.1 What You Can Do in the Tool Screens

- Use the **Firmware Upgrade** screen (Section 23.2 on page 224) to upload firmware to your device.
- Use the **Configuration** screen (Section 23.3 on page 225) to backup and restore device configurations. You can also reset your device settings back to the factory default.
- Use the **Restart** screen (Section 23.4 on page 228) to restart your ZyXEL device.

23.1.2 What You Need To Know About Tools

Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the P-79X's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. Find this firmware at www.zyxel.com.With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the P-79X.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file "config.cfg".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the P-79X only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the P-79X and the external filename refers to the filename not on the P-79X, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **Status** screen to confirm that you have uploaded the correct firmware version.

Table 103 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the P-79X. Uploading the rom-0 file replaces the entire ROM file system, including your P-79X configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the P-79X.	*.bin

FTP Restrictions

FTP will not work when:

1. The firewall is active (turn the firewall off or create a firewall rule to allow access from the WAN).
2. You have disabled the FTP service in the **Remote Management** screen.
3. The IP you entered in the Secured Client IP field does not match the client IP. If it does not match, the device will disallow the FTP session.

23.1.3 Before You Begin

- Ensure you have either created a firewall rule to allow access from the WAN or turned the firewall off, otherwise the FTP will not function.
- Make sure the FTP service has not been disabled in the Remote Management screen.

23.1.4 Tool Examples

Using FTP or TFTP to Restore Configuration

This example shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device. When the Restore Configuration process is complete, the device automatically restarts.

Restore Using FTP Session Example

Figure 125 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to Section 23.1.2 on page 218 to read about configurations that disallow TFTP and FTP over WAN.

FTP and TFTP Firmware and Configuration File Uploads

These examples show you how to upload firmware and configuration files.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device.

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your device.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Use “put” to transfer files from the computer to the device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

FTP Session Example of Firmware File Upload

Figure 126 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed in this chapter.

Refer to Section 23.1.2 on page 218 to read about configurations that disallow TFTP and FTP over WAN.

TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the device and log in. Because TFTP does not have any security checks, the device records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Enter the command “sys stdio 0” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute management idle timeout (default) when the file transfer is complete.
3. Launch the TFTP client on your computer and connect to the device. Set the transfer mode to binary before starting data transfer.
4. Use the TFTP client (see the example below) to transfer files between the device and the computer. The file name for the firmware is “ras”.

   Note that the telnet connection must be active and the device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the device’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

Using the FTP Commands to Back Up Configuration

1 Launch the FTP client on your computer.

2 Enter “open”, followed by a space and the IP address of your P-79X.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is “1234”).

5 Enter “bin” to set transfer mode to binary.

6 Use “get” to transfer files from the P-79X to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the P-79X to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

7 Enter “quit” to exit the ftp prompt.

FTP Command Configuration Backup Example

This figure gives an example of using FTP commands from the DOS command prompt to save your device’s configuration onto your computer.

Figure 127 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 104 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

Backup Configuration Using TFTP

The P-79X supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the P-79X and log in. Because TFTP does not have any security checks, the P-79X records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Enter command "`sys stdio 0`" to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter command "`sys stdio 5`" to restore the five-minute management idle timeout (default) when the file transfer is complete.
3. Launch the TFTP client on your computer and connect to the P-79X. Set the transfer mode to binary before starting data transfer.
4. Use the TFTP client (see the example below) to transfer files between the P-79X and the computer. The file name for the configuration file is "`rom-0`" (rom-zero, not capital o).

   Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "`get`" to transfer from the P-79X to the computer and "binary" to set binary transfer mode.

TFTP Command Configuration Backup Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the P-79X IP address, "get" transfers the file source on the P-79X (rom-0, name of the configuration file on the P-79X) to the file destination on the computer and renames it config.rom.

Configuration Backup Using GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 105 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the P-79X. 192.168.1.1 is the P-79X's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the P-79X and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the P-79X. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

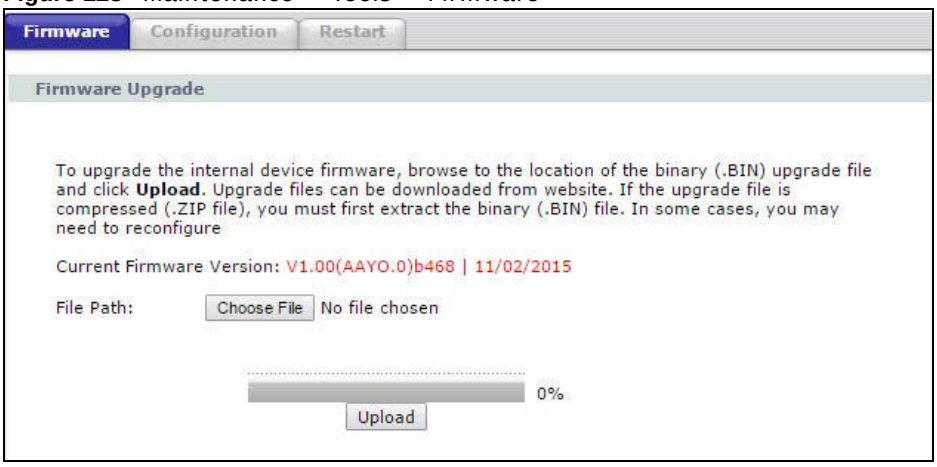
Refer to Section 23.1.2 on page 218 to read about configurations that disallow TFTP and FTP over WAN.

23.2 The Firmware Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your P-79X. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Section 23.1.4 on page 219 for upgrading firmware using FTP/TFTP commands.

Do NOT turn off the P-79X while firmware upload is in progress!

Figure 128 Maintenance > Tools > Firmware



The following table describes the labels in this screen.

Table 106 Maintenance > Tools > Firmware

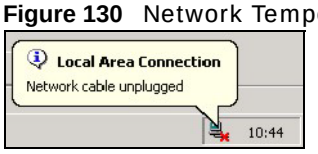
LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Choose File** to find it.
Choose File	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the P-79X again.

Figure 129 Firmware Upload In Progress

The P-79X automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 130 Network Temporarily Disconnected



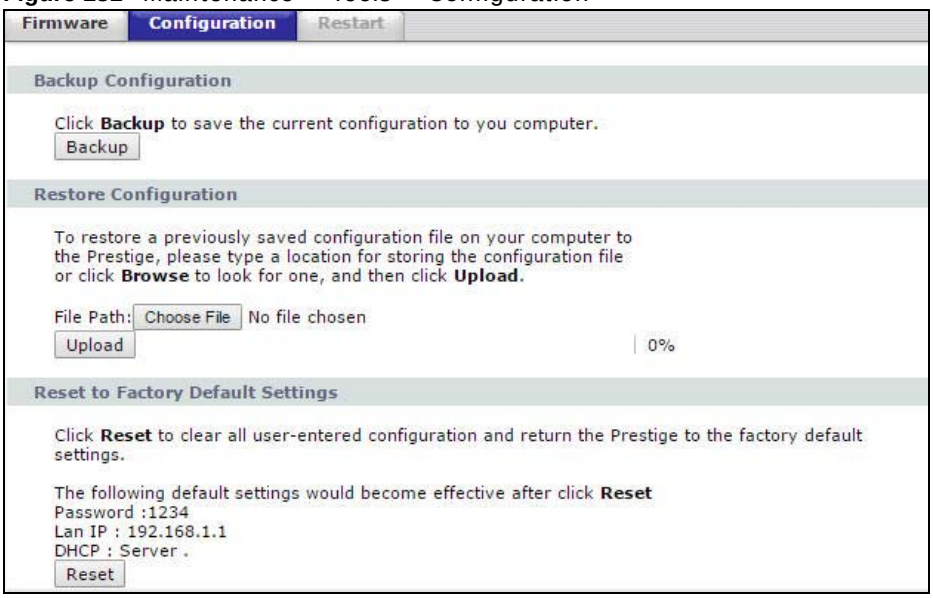
After two minutes, log in again and check your new firmware version in the **Status** screen.

23.3 The Configuration Screen

See Section 23.1.4 on page 219 for transferring configuration files using FTP/TFTP commands.

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 131 Maintenance > Tools > Configuration



Backup Configuration

Backup Configuration allows you to back up (save) the P-79X's current configuration to a file on your computer. Once your P-79X is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the P-79X's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your P-79X.

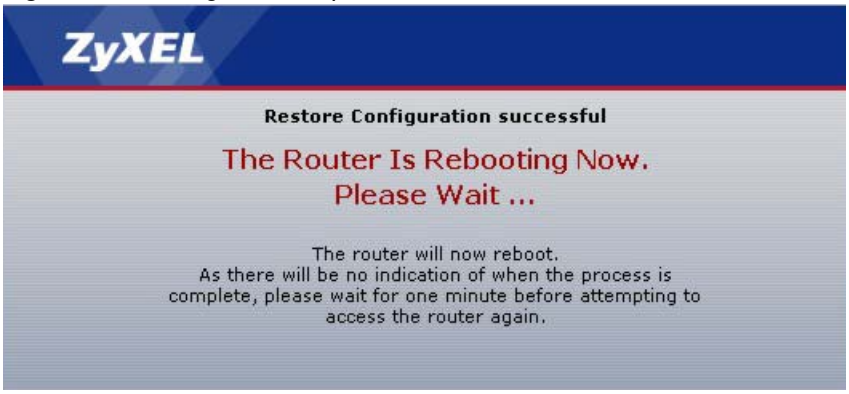
Table 107 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Choose File** to find it.
Choose File	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.

Do not turn off the P-79X while configuration file upload is in progress.

After you see a "restore configuration successful" screen, you must then wait one minute before logging into the P-79X again.

Figure 132 Configuration Upload Successful



The P-79X automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 133 Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix C on page 244 for details on how to set up your computer's IP address.

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the P-79X to its factory defaults. The following warning screen appears.

Figure 134 Reset Warning Message

Figure 135 Reset In Process Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your P-79X. Refer to Section 1.5 on page 18 for more information on the **RESET** button.

23.4 The Restart Screen

System restart allows you to reboot the P-79X remotely without turning the power off. You may need to do this if the P-79X hangs, for example.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the P-79X reboot. This does not affect the P-79X's configuration.

Figure 136 Maintenance > Tools >Restart

24

Diagnostic

24.1 Overview

These read-only screens display information to help you identify problems with the P-79X.

24.1.1 What You Can Do in the Diagnostic Screens

- Use the **General** screen (Section 24.2 on page 229) to ping an IP address.
- Use the **DSL Line** screen (Section 24.3 on page 230) to view the DSL line statistics and reset the ADSL line.

24.2 The General Diagnostic Screen

Use this screen to ping an IP address. Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 137 Maintenance > Diagnostic > General

The following table describes the fields in this screen.

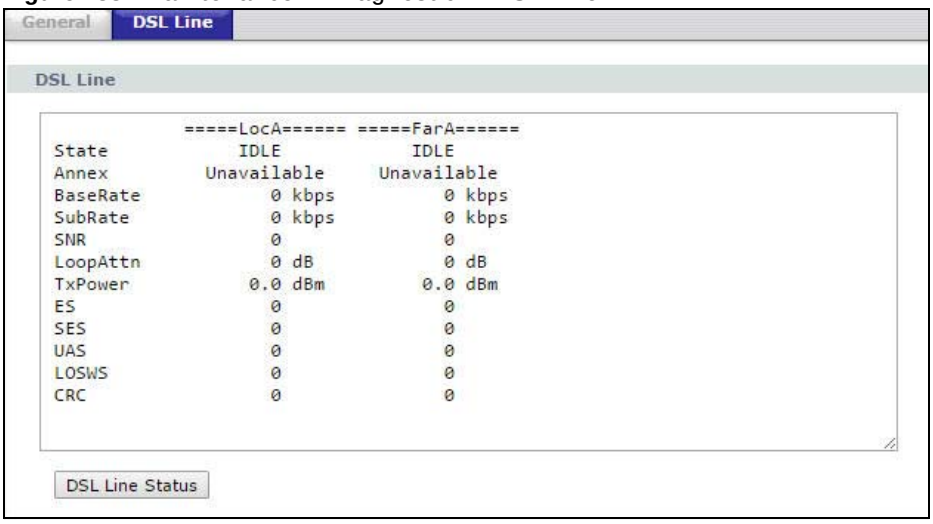
Table 108 Maintenance > Diagnostic > General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer or the URL that you want to ping in order to test a connection.
Ping	Click this to ping the IP address that you entered.

24.3 The DSL Line Diagnostic Screen

Use this screen to view the DSL line statistics and reset the ADSL line. Click **Maintenance > Diagnostic** > **DSL Line** to open the screen shown next.

Figure 138 Maintenance > Diagnostic > DSL Line



The following table describes the fields in this screen.

Table 109 Maintenance > Diagnostic > DSL Line

LABEL	DESCRIPTION
DSL Line Status	Click this to view statistics about the DSL connections. **noise margin downstream** is the signal to noise ratio for the downstream part of the connection (coming into the P-79X from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is. **output power upstream** is the amount of power (in decibels) that the P-79X is using to transmit to the ISP. **attenuation downstream** is the reduction in amplitude (in decibels) of the DSL signal coming into the P-79X from the ISP. Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each called tones. The rest of the display is the line's bit allocation. This is displayed as the number (in hexadecimal format) of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support certain ADSL transmission rates, and possibly to determine whether particular specific types of interference or line attenuation exist. Refer to the ITU-T G.992.1 recommendation for more information on DMT. The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. There will be some tones without any bits as there has to be space between the upstream and downstream channels.

25

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- P-79X Access and Login
- Internet Access
- Network Connections

25.1 Power, Hardware Connections, and LEDs

The P-79X does not turn on. None of the LEDs turn on.

1. Make sure the P-79X is turned on.
2. Make sure you are using the power adaptor or cord included with the P-79X.
3. Make sure the power adaptor or cord is connected to the P-79X and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the P-79X off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.4 on page 16.
2. Check the hardware connections.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the P-79X off and on.
5. If the problem continues, contact the vendor.

25.2 P-79X Access and Login

I forgot the IP address for the P-79X.

1 The default IP address is **192.168.1.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the P-79X by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the P-79X (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 18.

I forgot the password.

1 The default admin password is **1234**, and the default user password is **user**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 18.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section 8.2 on page 75), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the P-79X.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix D on page 264.

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix C on page 244. Your P-79X is a DHCP server by default.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the P-79X. See Appendix C on page 244.

4 Reset the device to its factory defaults, and try to access the P-79X with the default IP address. See Section 1.5 on page 18.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the P-79X using another service, such as Telnet. If you can access the P-79X, check the remote management settings and firewall rules to find out why the P-79X does not respond to HTTP.
- If your computer is connected to the **WAN** port, use a computer that is connected to a **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the P-79X.

1 Make sure you have entered the password correctly. The default admin password is **1234**, and the default user password is **user**. The field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the P-79X. Log out of the P-79X in the other session, or ask the person who is logged in to log out.

3 Turn the P-79X off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 18.

I cannot Telnet to the P-79X.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

25.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.4 on page 16.

2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

4 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the P-79X), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.4 on page 16.

2 Turn the P-79X off and on.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.4 on page 16. If the P-79X is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Turn the P-79X off and on.

3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

25.4 Network Connections

My network cannot be connected. How can I check the Internet connection status?

1 Check the LEDs on the P-79X for the following situations:

- If the **DSL** LEDs are off, there is no DSL connection. Check if your cables are connected properly to the P-79X.
- If the **DSL** LEDs are blinking fast, the P-79X is initializing the DSL line. If they keeps blinking for a long time, please reboot the device.

Note: For Internet access setup or point-to-point connections, the DSL1 and DSL2 LEDs indicate the status of a single connection (act as one LED). For point-to-2point connections, the DSL1 and DSL2 LEDs indicate the status of connection 1 and connection 2 respectively.

- If the **INTERNET** LED lights red, the P-79X attempted to become IP connected but failed. The reason might be no DHCP response, no PPPoE response, PPPoE authentication failed, or no IP address from IPCP. Please check if you have entered the correct ISP account and password when setting up the Internet connection. If the status is the same, reboot the device. If the problem remains, please contact your vendor or customer support.

2 Excess errors may occur if the quality of your line is poor. If you hear noise on the line while making a telephone call, you should ask your local telecommunications office to check the lines in your house or apartment building and the line from your residence to your DSL service provider.

A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See *http://www.zyxel.com/homepage.shtml* and also

http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

Asia

China

- ZyXEL Communications (Shanghai) Corp.
  ZyXEL Communications (Beijing) Corp.
  ZyXEL Communications (Tianjin) Corp.
- http://www.zyxel.cn

India

- ZyXEL Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- ZyXEL Kazakhstan

- http://www.zyxel.kz

Korea

- ZyXEL Korea Corp.
- http://www.zyxel.kr

Malaysia

- ZyXEL Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- ZyXEL Philippines
- http://www.zyxel.com.ph

Singapore

- ZyXEL Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com/tw/zh/

Thailand

- ZyXEL Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

Europe

Austria

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Belarus

- ZyXEL BY
- http://www.zyxel.by

Belgium

- ZyXEL Communications B.V.
- http://www.zyxel.com/be/nl/
- http://www.zyxel.com/be/fr/

Bulgaria

- ZyXEL България
- http://www.zyxel.com/bg/bg/

Czech Republic

- ZyXEL Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- ZyXEL Communications A/S
- http://www.zyxel.dk

Estonia

- ZyXEL Estonia
- http://www.zyxel.com/ee/et/

Finland

- ZyXEL Communications
- http://www.zyxel.fi

France

- ZyXEL France
- http://www.zyxel.fr

Germany

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Hungary

- ZyXEL Hungary & SEE
- http://www.zyxel.hu

Italy

- ZyXEL Communications Italy
- http://www.zyxel.it/

Latvia

- ZyXEL Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- ZyXEL Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- ZyXEL Benelux
- http://www.zyxel.nl

Norway

- ZyXEL Communications
- http://www.zyxel.no

Poland

- ZyXEL Communications Poland
- http://www.zyxel.pl

Romania

- ZyXEL Romania
- http://www.zyxel.com/ro/ro

Russia

- ZyXEL Russia
- http://www.zyxel.ru

Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Spain

- ZyXEL Communications ES Ltd
- http://www.zyxel.es

Sweden

- ZyXEL Communications

- http://www.zyxel.se

Switzerland

- Studerus AG
- http://www.zyxel.ch/

Turkey

- ZyXEL Turkey A.S.
- http://www.zyxel.com.tr

UK

- ZyXEL Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

- ZyXEL Ukraine
- http://www.ua.zyxel.com

Latin America

Argentina

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Brazil

- ZyXEL Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Ecuador

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Israel

- ZyXEL Communication Corporation
- http://il.zyxel.com/homepage.shtml

Middle East

- ZyXEL Communication Corporation

- http://www.zyxel.com/me/en/

North America

USA

- ZyXEL Communications, Inc. - North America Headquarters
- http://www.zyxel.com/us/en/

Oceania

Australia

- ZyXEL Communications Corporation
- http://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

B

Wall-mounting Instructions

Do the following to hang your P-79X on a wall.

Note: See the product specifications appendix for the size of screws to use and how far apart to place them.

1 Locate a high position on a wall that is free of obstructions. Use a sturdy wall.

2 Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.

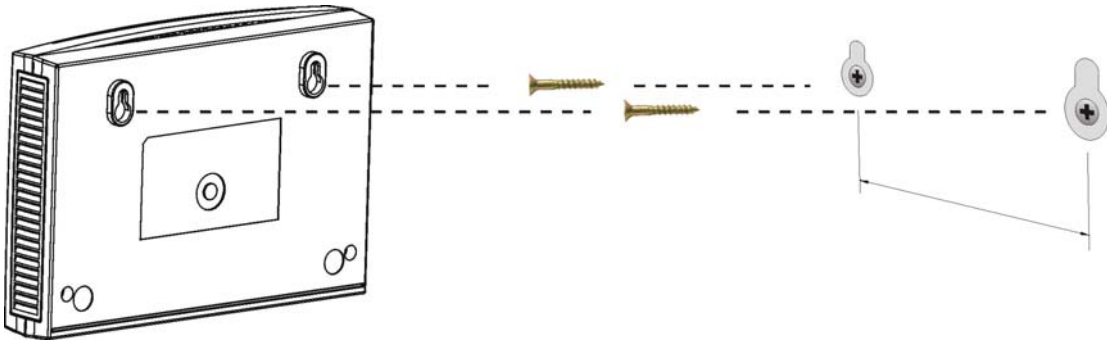
Note: Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

3 Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.

4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the P-79X with the connection cables.

5 Align the holes on the back of the P-79X with the screws on the wall. Hang the P-79X on the screws.

Figure 139 Wall-mounting Example



C

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

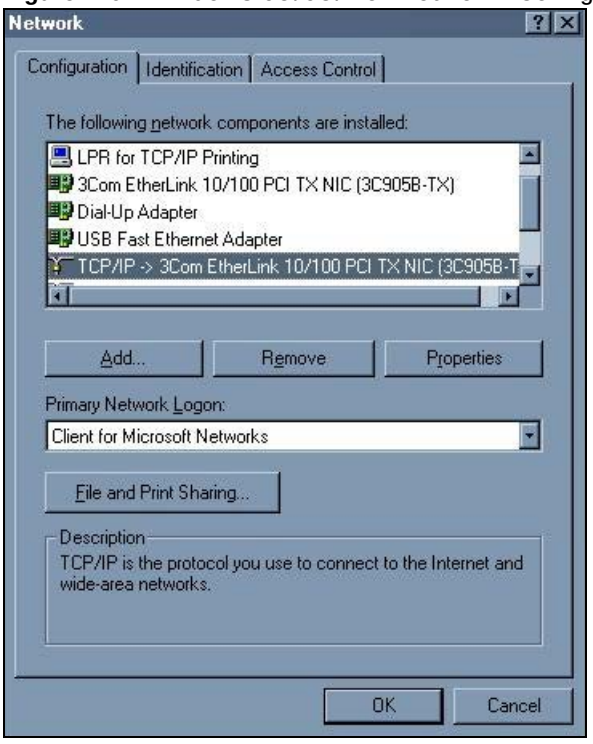
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the P-79X's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 140 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

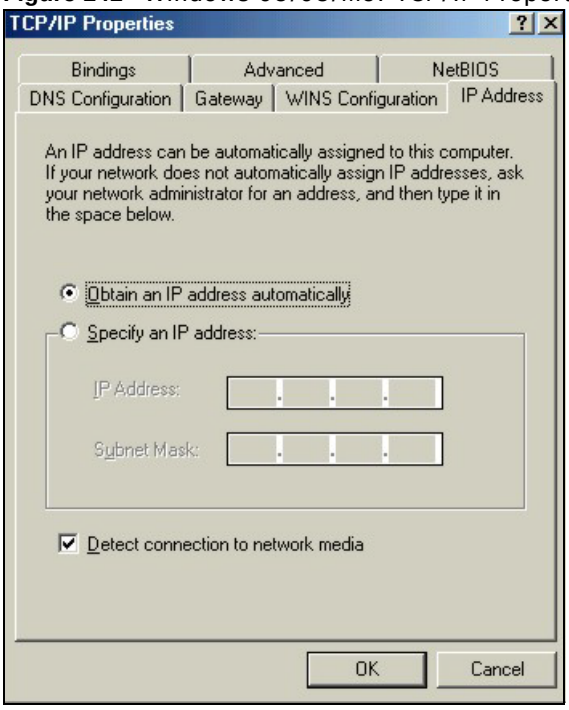
If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.
3. Select **Microsoft** from the list of manufacturers.
4. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5. Restart your computer so the changes you made take effect.

Configuring

1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
2. Click the **IP Address** tab.
   - If your IP address is dynamic, select **Obtain an IP address automatically**.
   - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

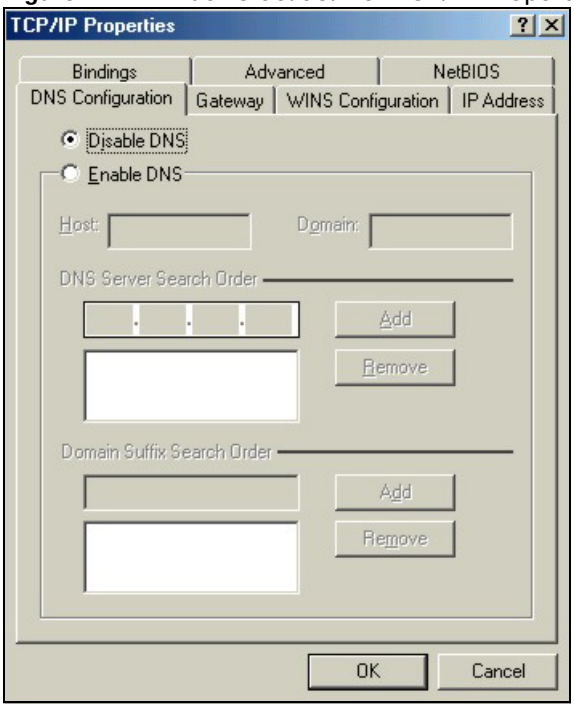
Figure 141 Windows 95/98/Me: TCP/IP Properties: IP Address



3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 142 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your P-79X and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

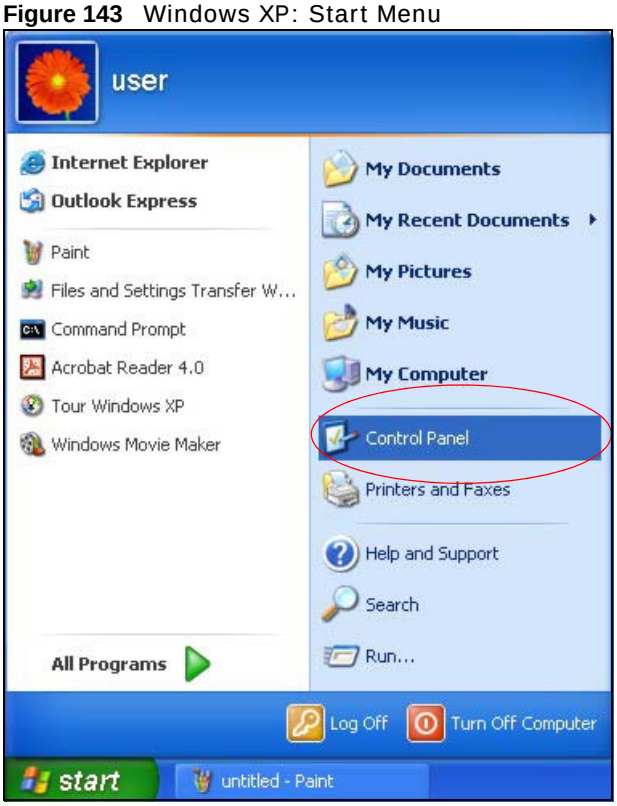
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 143 Windows XP: Start Menu

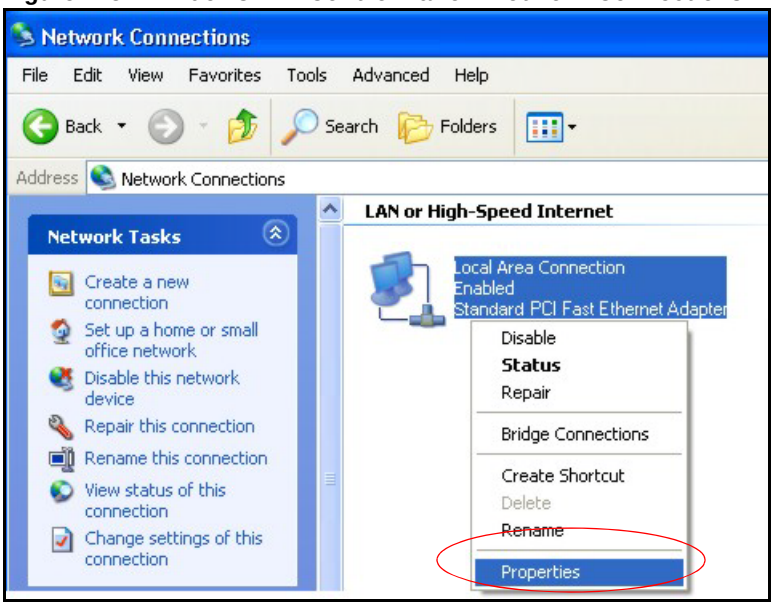


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 144 Windows XP: Control Panel

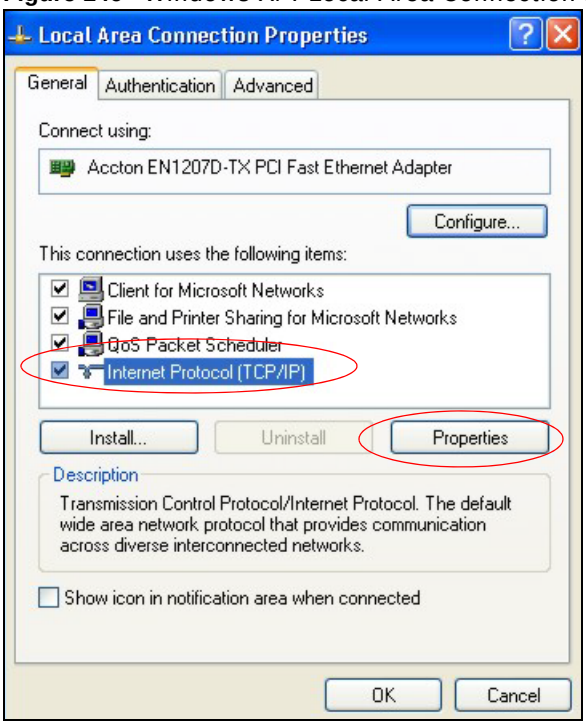
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 145 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

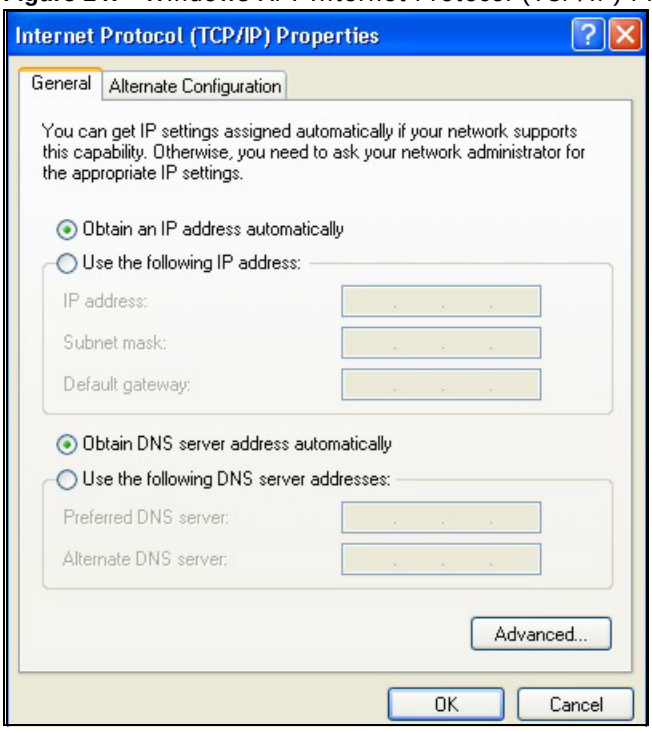
Figure 146 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 147 Windows XP: Internet Protocol (TCP/IP) Properties

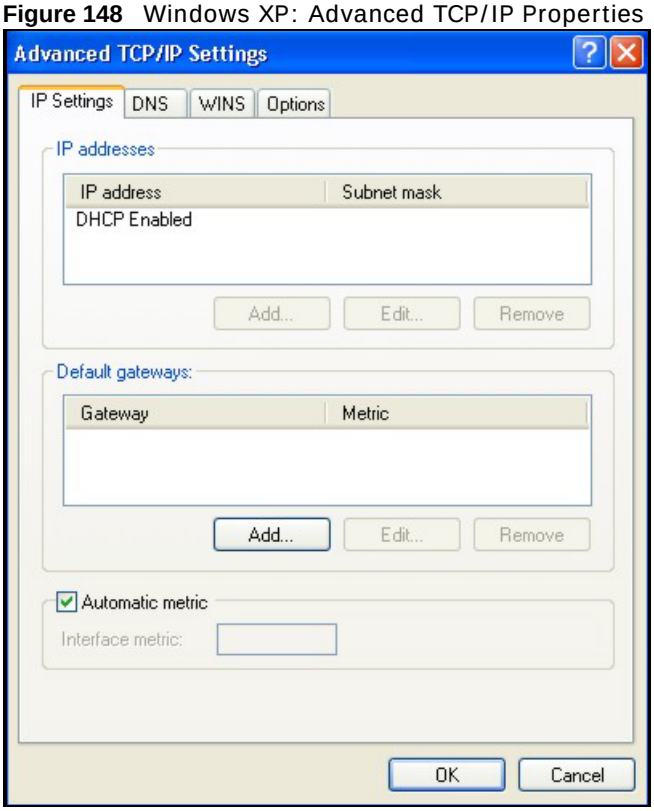


6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 148 Windows XP: Advanced TCP/IP Properties

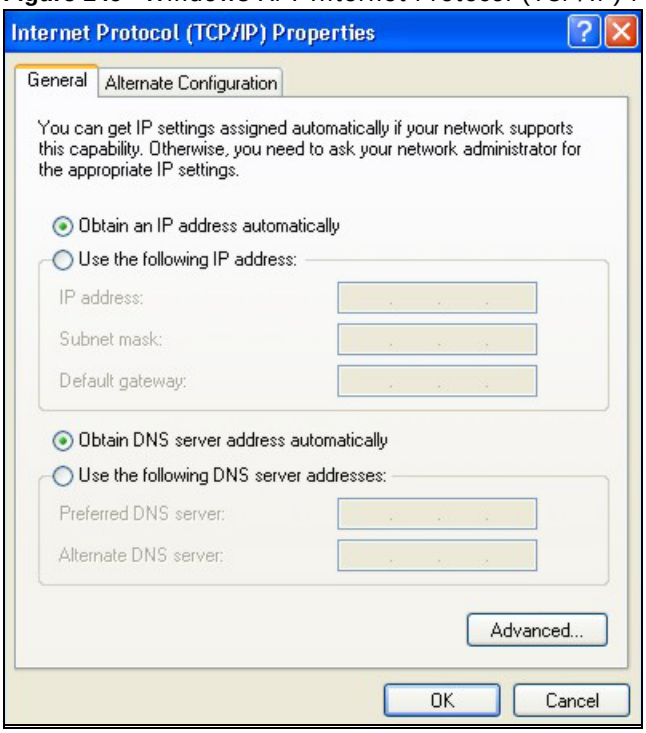


7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 149 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your P-79X and restart your computer (if prompted).

Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

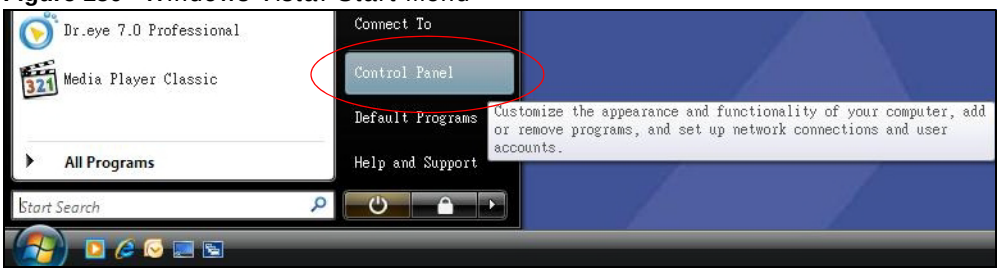
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Windows Vista

This section shows screens from Windows Vista Enterprise Version 6.0.

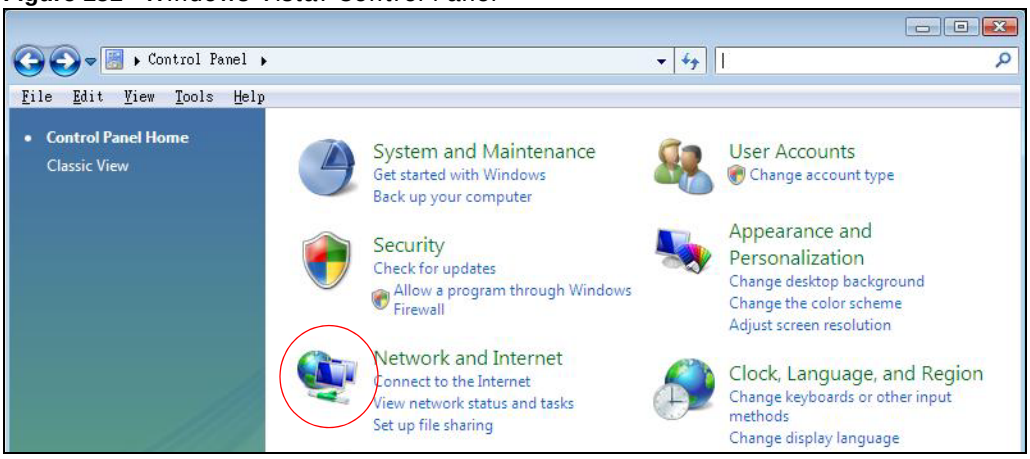
1 Click the **Start** icon, **Control Panel**.

Figure 150 Windows Vista: Start Menu



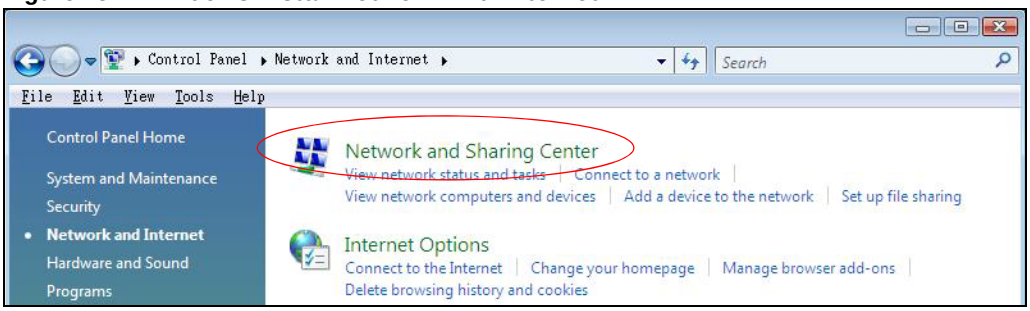
2 In the **Control Panel**, double-click **Network and Internet**.

Figure 151 Windows Vista: Control Panel



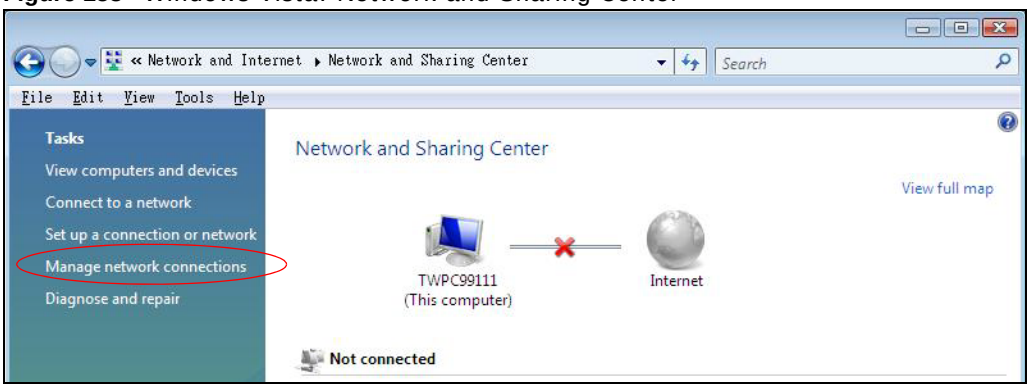
3 Click **Network and Sharing Center**.

Figure 152 Windows Vista: Network And Internet



4 Click **Manage network connections**.

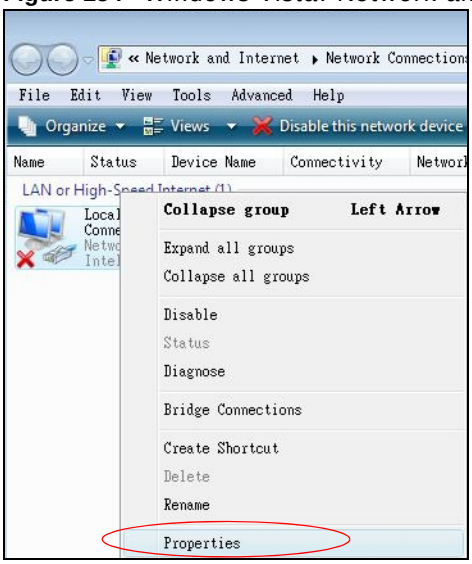
Figure 153 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then click **Properties**.

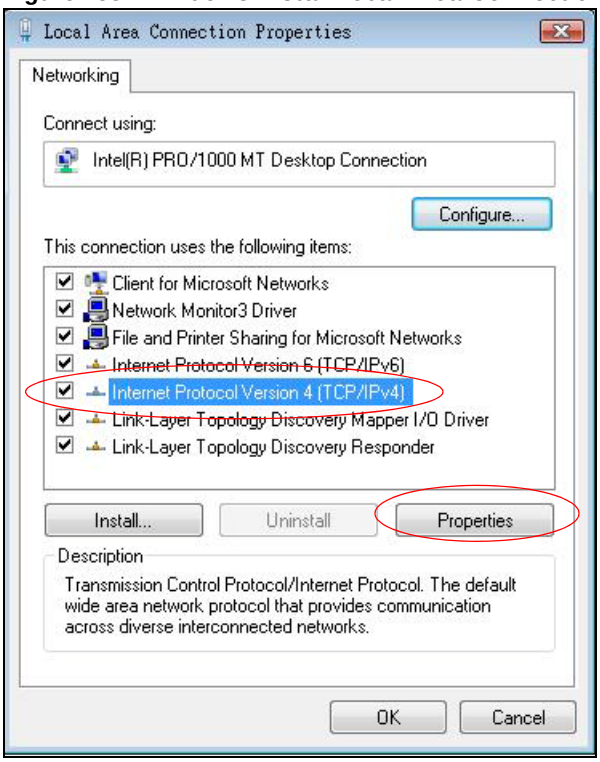
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

Figure 154 Windows Vista: Network and Sharing Center



6 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

Figure 155 Windows Vista: Local Area Connection Properties

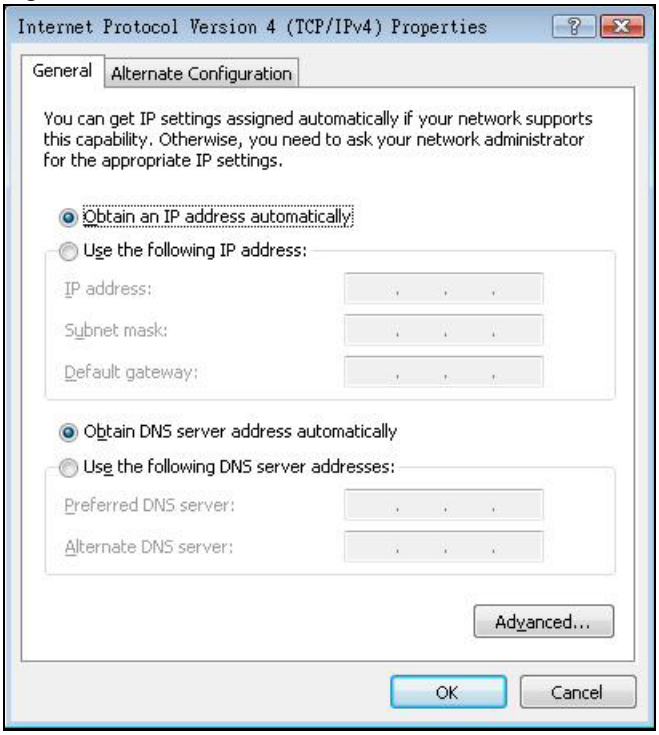


7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General tab**).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 156 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties

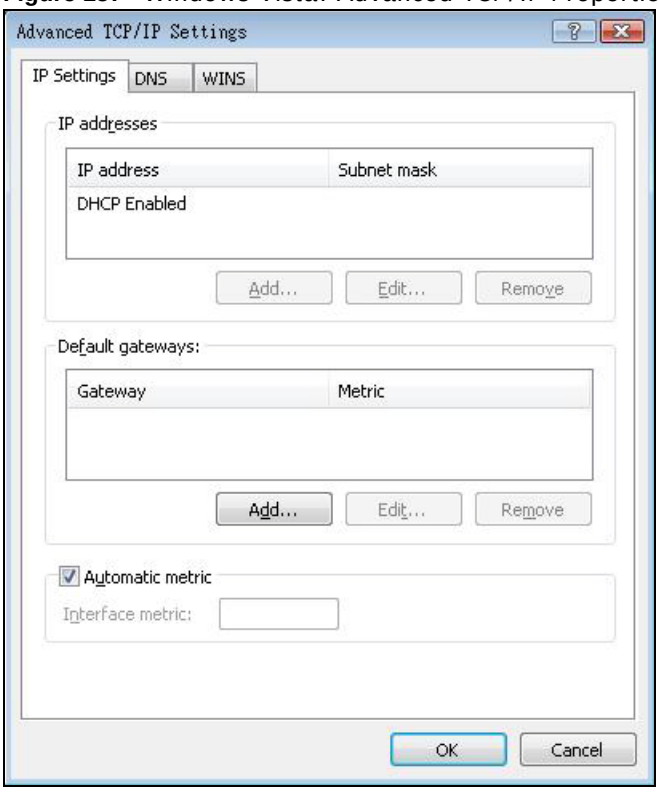


8 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 157 Windows Vista: Advanced TCP/IP Properties

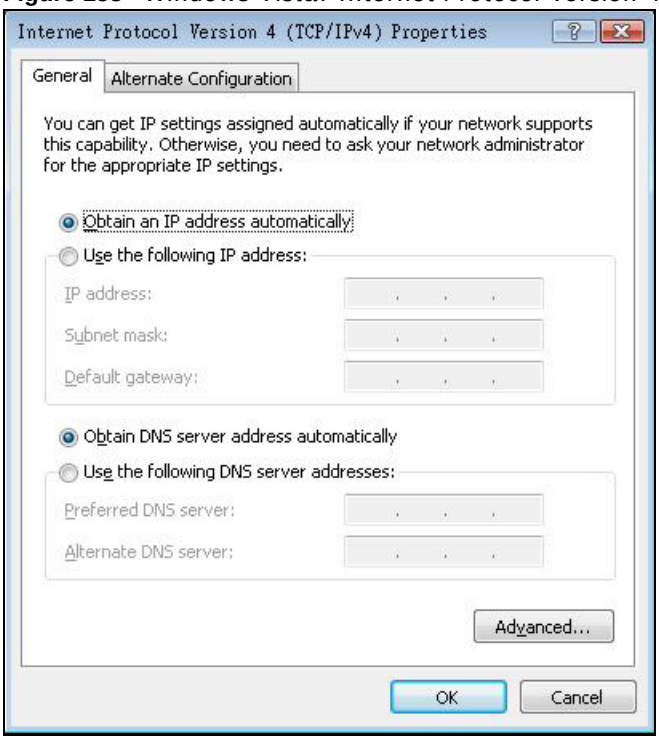


9 In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General tab**):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 158 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



10 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

11 Click **Close** to close the **Local Area Connection Properties** window.

12 Close the **Network Connections** window.

13 Turn on your P-79X and restart your computer (if prompted).

Verifying Settings

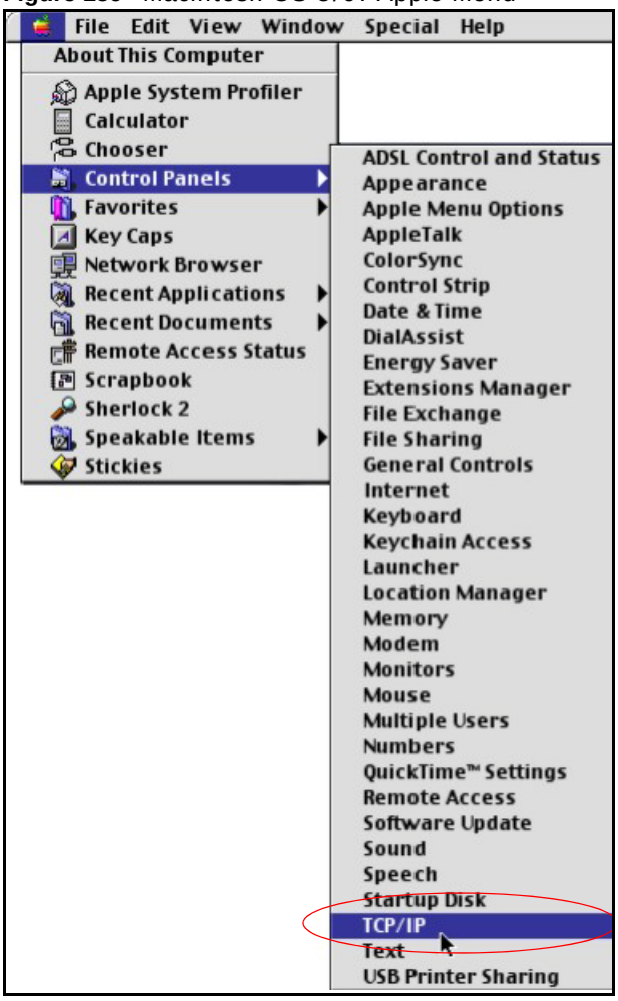
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

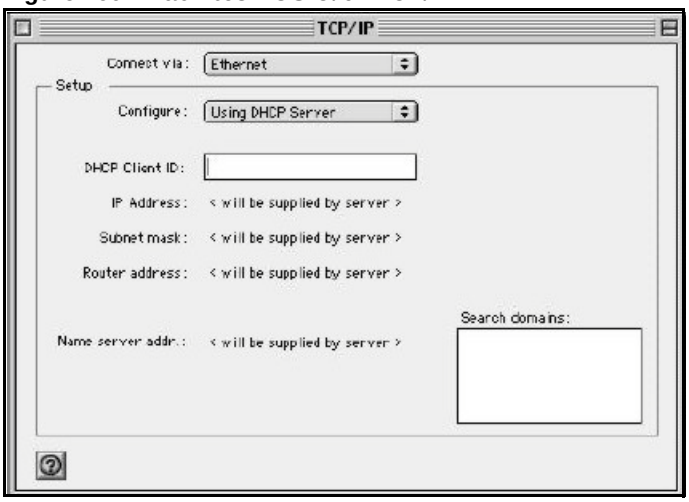
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 159 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 160 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your P-79X in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your P-79X and restart your computer (if prompted).

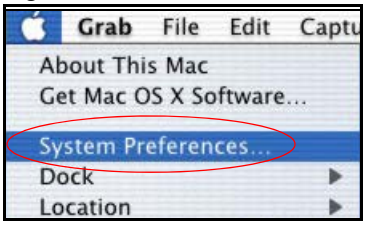
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 161 Macintosh OS X: Apple Menu

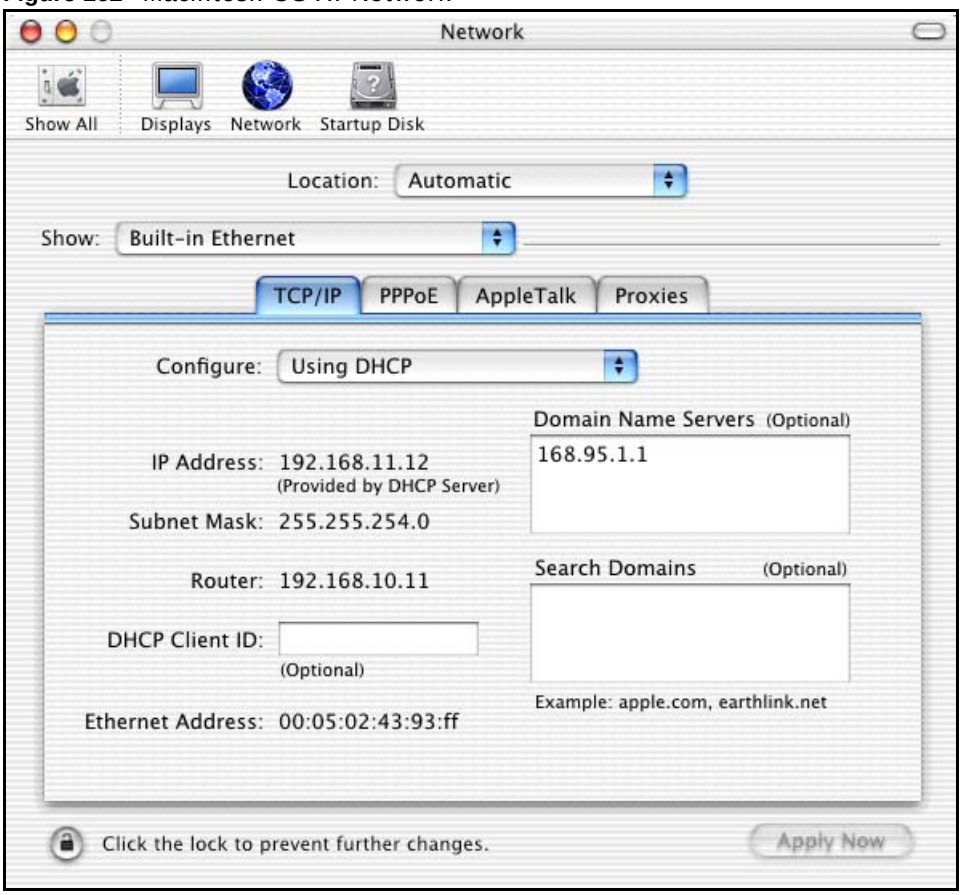


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 162 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your P-79X in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your P-79X and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

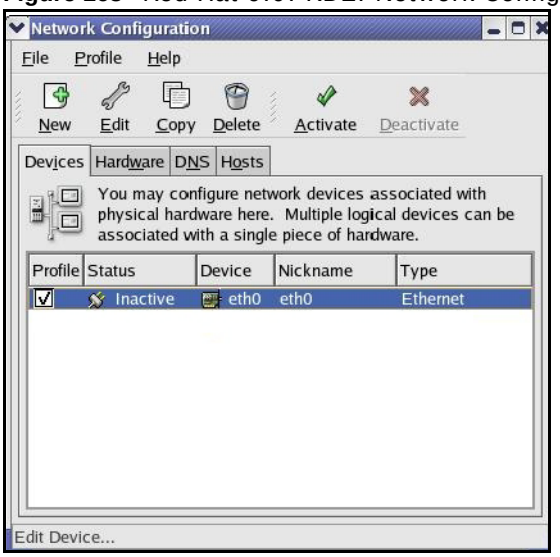
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 163 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

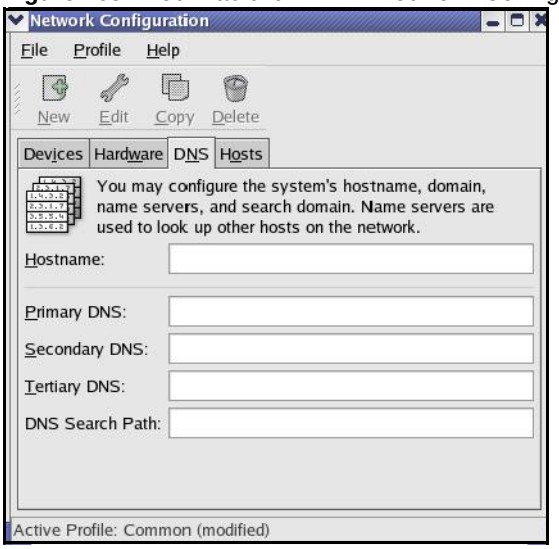
Figure 164 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

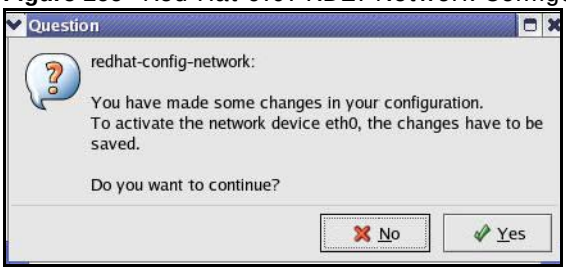
Figure 165 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 166 Red Hat 9.0: KDE: Network Configuration: Activate



7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 167 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 168 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the resolv.conf file in the /etc directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 169 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter ./network restart in the /etc/rc.d/init.d directory. The following figure shows an example.

Figure 170 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                  [OK]
Shutting down loopback interface:              [OK]
Setting network parameters:                    [OK]
Bringing up loopback interface:                [OK]
Bringing up interface eth0:                    [OK]
```

Verifying Settings

Enter ifconfig in a terminal screen to check your TCP/IP properties.

Figure 171 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

D

Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

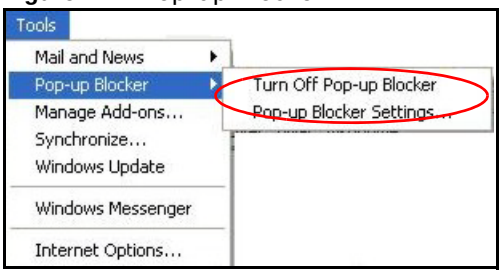
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 172 Pop-up Blocker

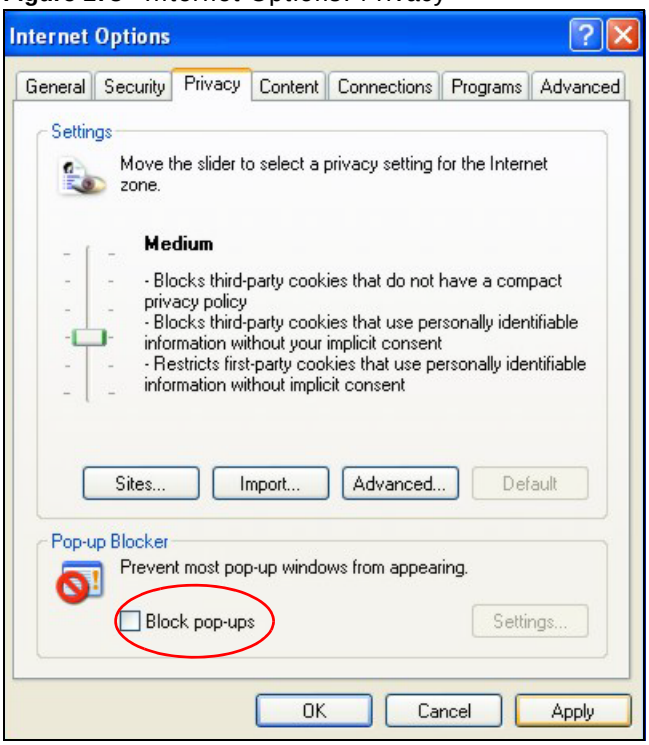


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 173 Internet Options: Privacy



3 Click **Apply** to save this setting.

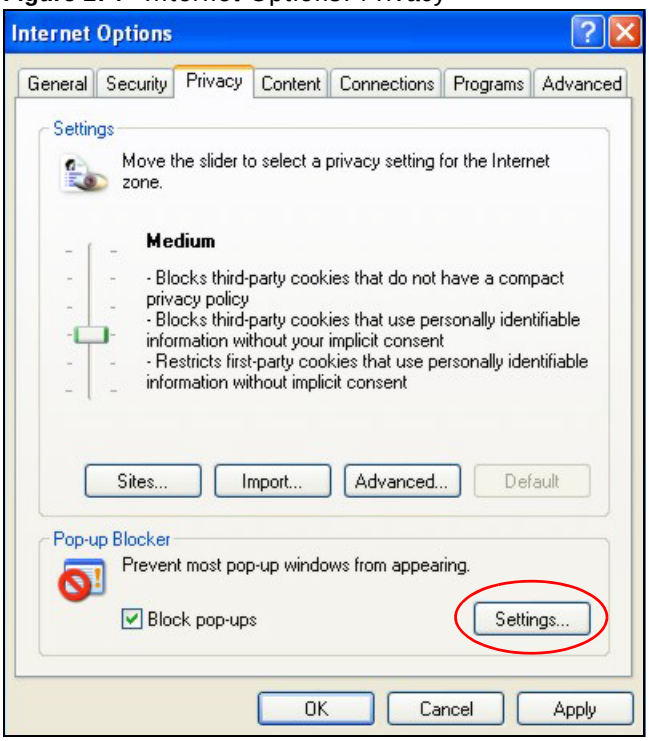
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 174 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 175 Pop-up Blocker Settings

5 Click **Close** to return to the **Privacy** screen.

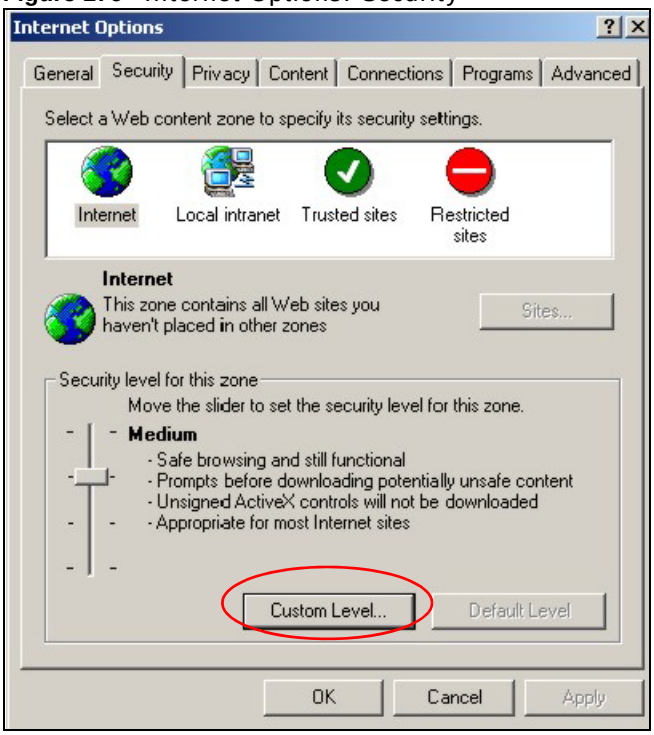
6 Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 176 Internet Options: Security



2 Click the **Custom Level...** button.

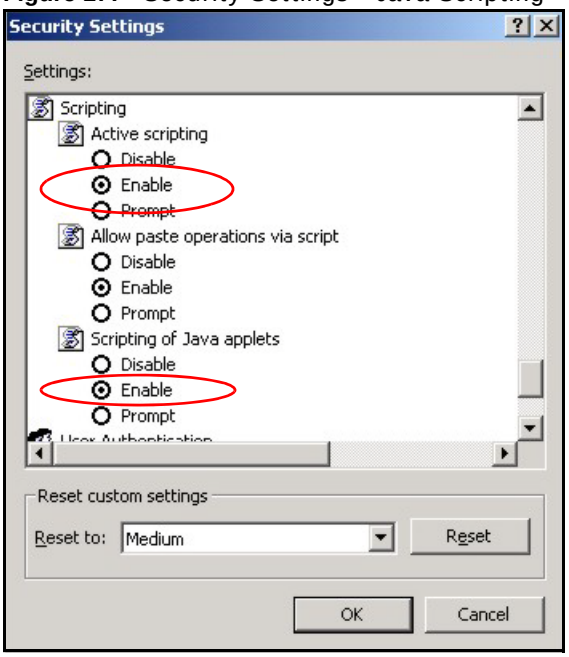
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 177 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

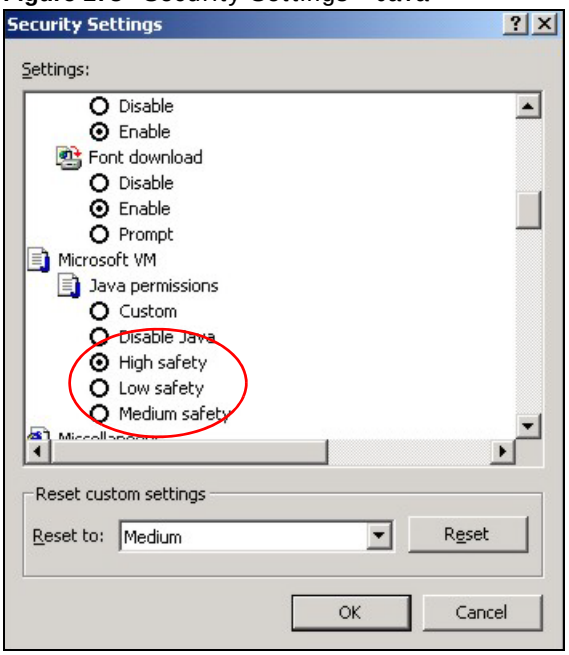
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 178 Security Settings - Java



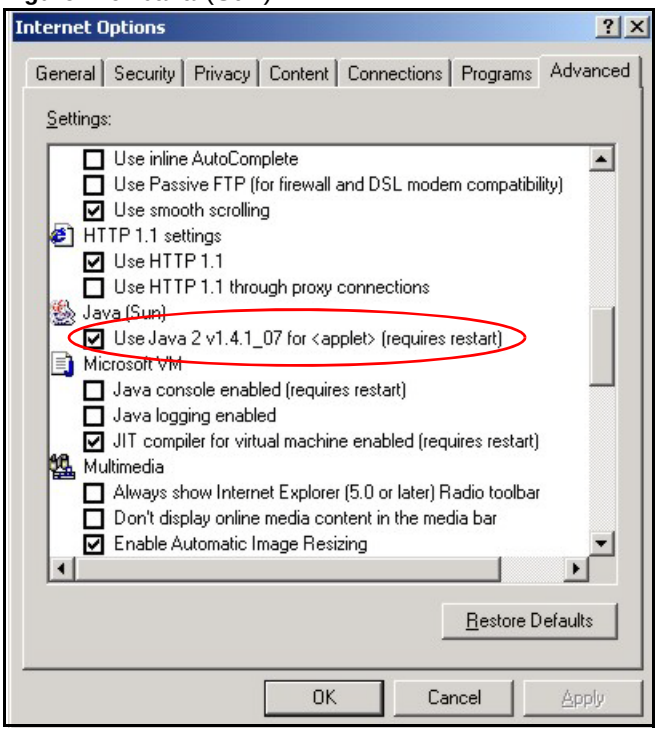
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 179 Java (Sun)

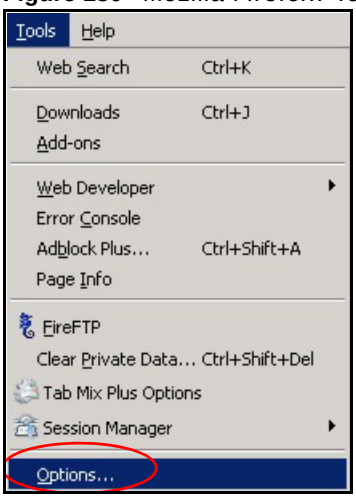


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

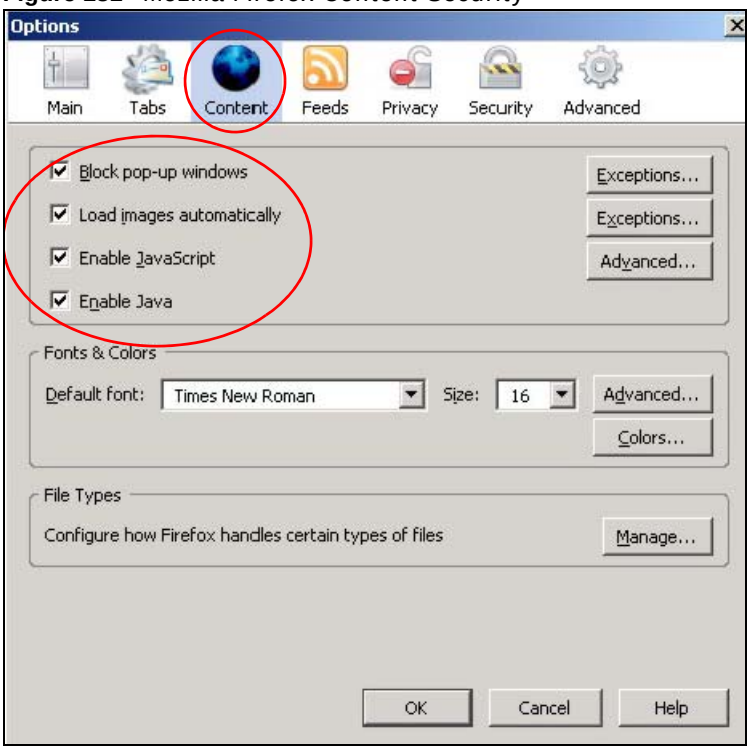
You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 180 Mozilla Firefox: Tools > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 181 Mozilla Firefox Content Security



E

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

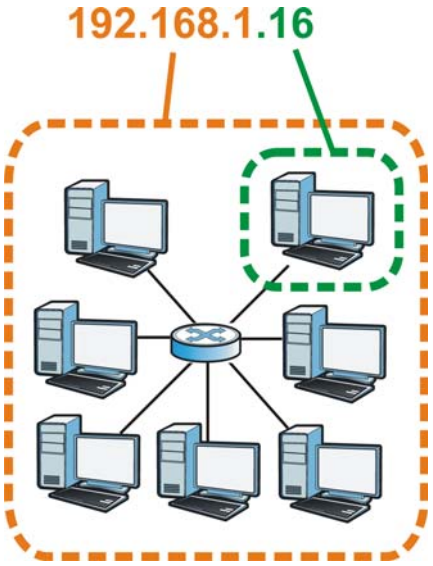
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 182 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 110 Subnet Masks

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 111 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 112 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 113 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192

Table 113 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

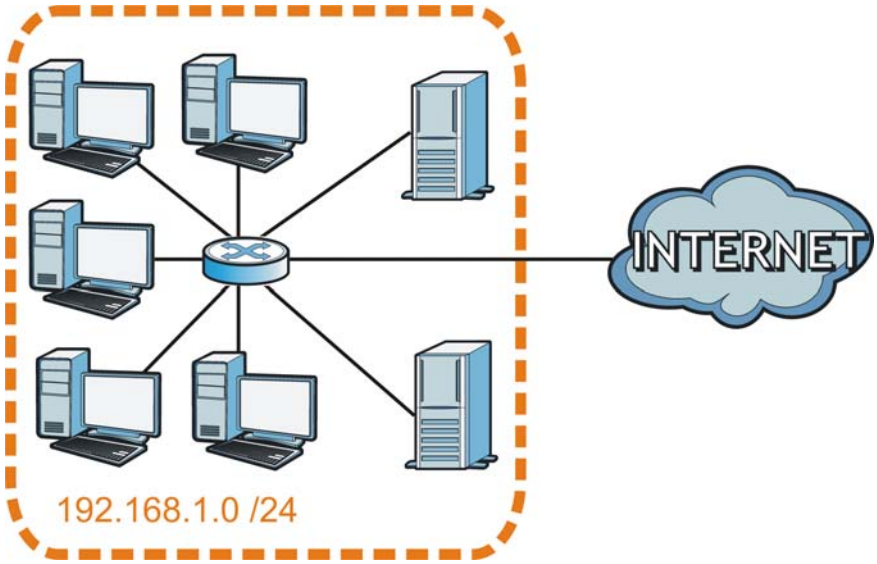
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 183 Subnetting Example: Before Subnetting

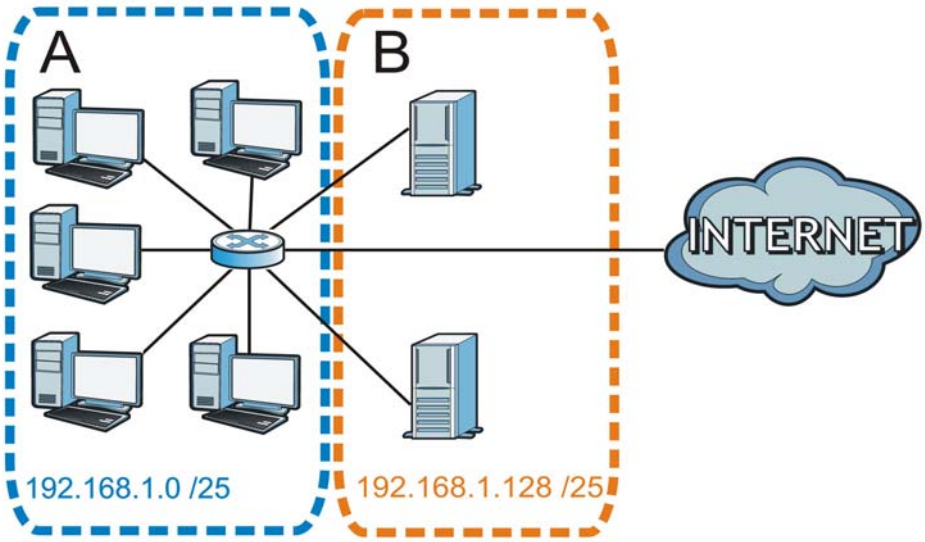


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 184 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of 2^7 – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 114 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 115 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 116 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 117 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 118 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191

Table 118 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 119 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 120 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the P-79X.

Once you have decided on the network number, pick an IP address for your P-79X that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your P-79X will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the P-79X unless you are instructed to do otherwise.

Private IP Addresses

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

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

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

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

F

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 121 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.

Table 121 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).

Table 121 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

G

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

UNITED STATES of AMERICA

The following information applies if you use the product within USA area.

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - •Reorient or relocate the receiving antenna
  - •Increase the separation between the equipment or devices
  - •Connect the equipment to an outlet other than the receiver's
  - •Consult a dealer or an experienced radio/TV technician for assistance

CANADA

The following information applies if you use the product within Canada area

Industry Canada ICES statement

CAN ICES-3 (B)/NMB-3(B)

EUROPEAN UNION

The following information applies if you use the product within the European Union.

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- DO not use this product near water, for example, in a wet basement or near a swimming pool.
- DO not expose your device to dampness, dust or corrosive liquids.
- DO not store things on the device.
- DO not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- DO not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- DO not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- DO not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- DO not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- DO not obstruct the device ventilation slots, as insufficient airflow may harm your device.

The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

- For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
- For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

ErP (Energy-related Products)

ZyXEL products put on the EU market in compliance with the requirement of the European Parliament and the Council published

Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called

as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

Network standby power consumption < 12W, and/or

Off mode power consumption < 0.5W, and/or

Standby mode power consumption < 0.5W.

Wireless setting, please refer to "Wireless" chapter for more detail.

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

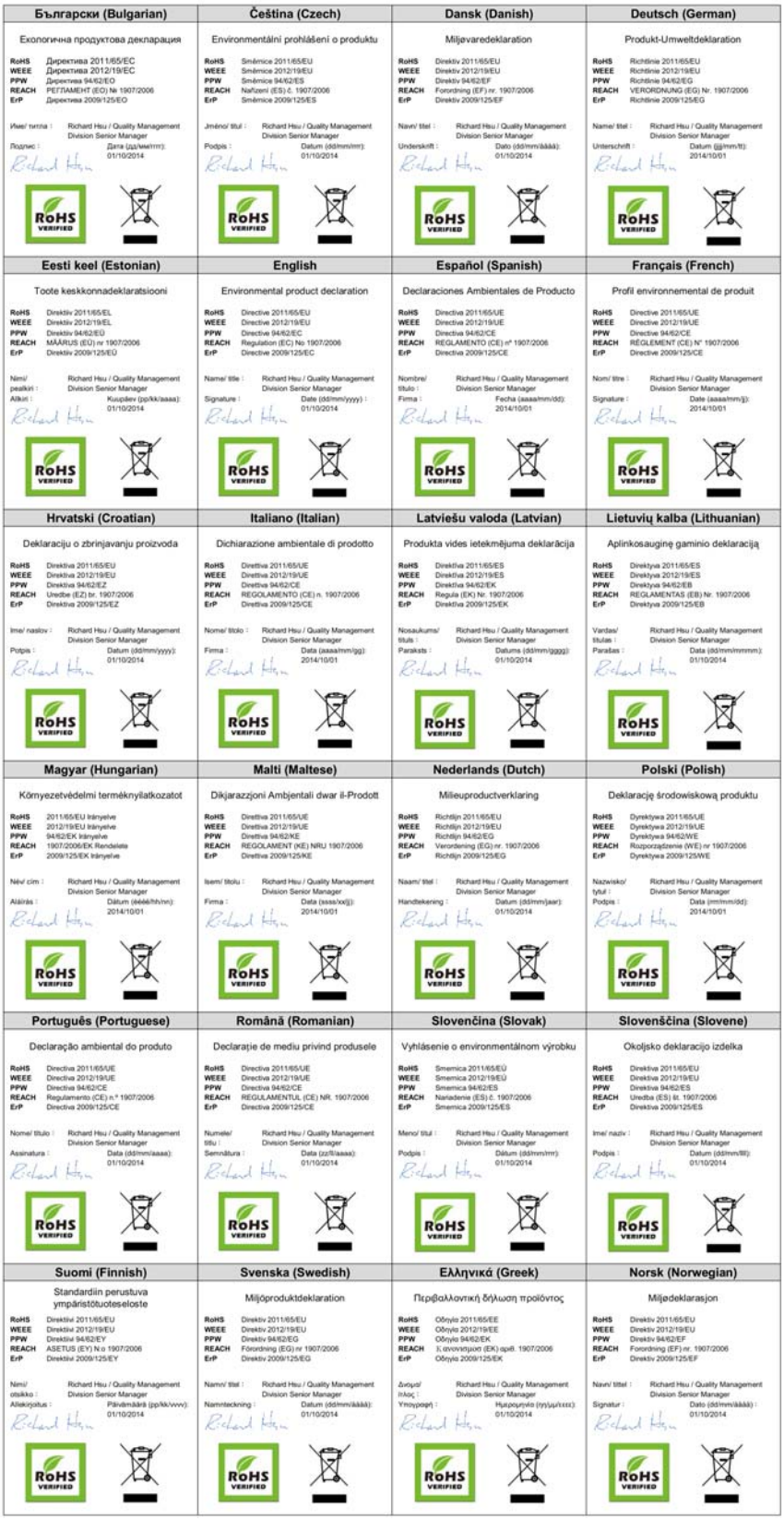
El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

Environmental Product Declaration



Български (Bulgarian)

Екологична продуктова декларация

RoHS Директива 2011/65/EC
WEEE Директива 2012/19/EC
PPW Директива 94/62/EO
REACH РЕГЛАМЕНТ (ЕО) № 1907/2006
ErP Директива 2009/125/EO

Име/ титла : Richard Hsu / Quality Management Division Senior Manager
Подпис : Дата (дд/мм/гггг): 01/10/2014

Čeština (Czech)

Environmentální prohlášení o produktu

RoHS Směrnice 2011/65/EU
WEEE Směrnice 2012/19/EU
PPW Směrnice 94/62/ES
REACH Nařízení (ES) č. 1907/2006
ErP Směrnice 2009/125/ES

Jméno/ titul : Richard Hsu / Quality Management Division Senior Manager
Podpis : Datum (dd/mm/rrrr): 01/10/2014

Dansk (Danish)

Miljøvaredeklaration

RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EF
REACH Forordning (EF) nr. 1907/2006
ErP Direktiv 2009/125/EF

Navn/ titel : Richard Hsu / Quality Management Division Senior Manager
Underskrift : Dato (dd/mm/åååå): 01/10/2014

Deutsch (German)

Produkt-Umweltdeklaration

RoHS Richtlinie 2011/65/EU
WEEE Richtlinie 2012/19/EU
PPW Richtlinie 94/62/EG
REACH VERORDNUNG (EG) Nr. 1907/2006
ErP Richtlinie 2009/125/EG

Name/ titel : Richard Hsu / Quality Management Division Senior Manager
Unterschrift : Datum (tt/mm/jj): 2014/10/01

Eesti keel (Estonian)

Toote keskkonnadeklaratsiooni

RoHS Direktiiv 2011/65/EL
WEEE Direktiiv 2012/19/EL
PPW Direktiiv 94/62/EÜ
REACH MÄÄRUS (EÜ) nr 1907/2006
ErP Direktiiv 2009/125/EÜ

Nimi/ positsioon : Richard Hsu / Quality Management Division Senior Manager
Allkiri : Kuupäev (pp/kk/aaaa): 01/10/2014

English

Environmental product declaration

RoHS Directive 2011/65/EU
WEEE Directive 2012/19/EU
PPW Directive 94/62/EC
REACH Regulation (EC) No 1907/2006
ErP Directive 2009/125/EC

Name/ title : Richard Hsu / Quality Management Division Senior Manager
Signature : Date (dd/mm/yyyy) : 01/10/2014

Español (Spanish)

Declaraciones Ambientales de Producto

RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH REGLAMENTO (CE) nº 1907/2006
ErP Directiva 2009/125/CE

Nombre/ título : Richard Hsu / Quality Management Division Senior Manager
Firma : Fecha (aaaa/mm/dd): 2014/10/01

Français (French)

Profil environnemental de produit

RoHS Directive 2011/65/UE
WEEE Directive 2012/19/UE
PPW Directive 94/62/CE
REACH RÈGLEMENT (CE) N° 1907/2006
ErP Directive 2009/125/CE

Nom/ titre : Richard Hsu / Quality Management Division Senior Manager
Signature : Date (aaaa/mm/jj): 2014/10/01

Hrvatski (Croatian)

Deklaraciju o zbrinjavanju proizvoda

RoHS Direktiva 2011/65/EU
WEEE Direktiva 2012/19/EU
PPW Direktiva 94/62/EZ
REACH Uredbe (EZ) br. 1907/2006
ErP Direktiva 2009/125/EZ

Ime/ naslov : Richard Hsu / Quality Management Division Senior Manager
Potpis : Datum (dd/mm/yyyy): 01/10/2014

Italiano (Italian)

Dichiarazione ambientale di prodotto

RoHS Direttiva 2011/65/UE
WEEE Direttiva 2012/19/UE
PPW Direttiva 94/62/CE
REACH REGOLAMENTO (CE) n. 1907/2006
ErP Direttiva 2009/125/CE

Nome/ titolo : Richard Hsu / Quality Management Division Senior Manager
Firma : Data (aaaa/mm/gg): 2014/10/01

Latviešu valoda (Latvian)

Produkta vides ietekmējuma deklarācija

RoHS Direktīva 2011/65/ES
WEEE Direktīva 2012/19/ES
PPW Direktīva 94/62/EK
REACH Regula (EK) Nr. 1907/2006
ErP Direktīva 2009/125/EK

Nosaukums/ tituls : Richard Hsu / Quality Management Division Senior Manager
Paraksts : Datums (dd/mm/gggg): 01/10/2014

Lietuvių kalba (Lithuanian)

Aplinkosauginę gaminio deklaraciją

RoHS Direktyva 2011/65/ES
WEEE Direktyva 2012/19/ES
PPW Direktyva 94/62/EB
REACH REGLAMENTAS (EB) Nr. 1907/2006
ErP Direktyva 2009/125/EB

Vardas/ titulas : Richard Hsu / Quality Management Division Senior Manager
Parašas : Data (dd/mm/mmmm): 01/10/2014

Magyar (Hungarian)

Környezetvédelmi terméknyilatkozatot

RoHS 2011/65/EU irányelve
WEEE 2012/19/EU irányelve
PPW 94/62/EK irányelve
REACH 1907/2006/EK Rendelete
ErP 2009/125/EK irányelve

Név/ cím : Richard Hsu / Quality Management Division Senior Manager
Aláírás : Dátum (éééé/hh/nn): 2014/10/01

Malti (Maltese)

Dikjarazzjoni Ambjentali dwar il-Prodott

RoHS Direttiva 2011/65/UE
WEEE Direttiva 2012/19/UE
PPW Direttiva 94/62/KE
REACH REGOLAMENT (KE) NRU 1907/2006
ErP Direttiva 2009/125/KE

Isem/ titolu : Richard Hsu / Quality Management Division Senior Manager
Firma : Data (sssa/xx/jj): 2014/10/01

Nederlands (Dutch)

Milieuproductverklaring

RoHS Richtlijn 2011/65/EU
WEEE Richtlijn 2012/19/EU
PPW Richtlijn 94/62/EG
REACH Verordening (EG) nr. 1907/2006
ErP Richtlijn 2009/125/EG

Naam/ titel : Richard Hsu / Quality Management Division Senior Manager
Handtekening : Datum (dd/mm/jaar): 01/10/2014

Polski (Polish)

Deklarację środowiskową produktu

RoHS Dyrektywa 2011/65/UE
WEEE Dyrektywa 2012/19/UE
PPW Dyrektywa 94/62/WE
REACH Rozporządzenie (WE) nr 1907/2006
ErP Dyrektywa 2009/125/WE

Nazwisko/ tytuł : Richard Hsu / Quality Management Division Senior Manager
Podpis : Data (rr/mm/dd): 2014/10/01

Português (Portuguese)

Declaração ambiental do produto

RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH Regulamento (CE) n.º 1907/2006
ErP Directiva 2009/125/CE

Nome/ título : Richard Hsu / Quality Management Division Senior Manager
Assinatura : Data (dd/mm/aaaa): 01/10/2014

Română (Romanian)

Declarație de mediu privind produsele

RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH REGLAMENTUL (CE) NR. 1907/2006
ErP Directiva 2009/125/CE

Numele/ titlu : Richard Hsu / Quality Management Division Senior Manager
Semnătura : Data (zz/ll/aaaa): 01/10/2014

Slovenčina (Slovak)

Vyhlásenie o environmentálnom výrobku

RoHS Smernica 2011/65/EÚ
WEEE Smernica 2012/19/EÚ
PPW Smernica 94/62/ES
REACH Nariadenie (ES) č. 1907/2006
ErP Smernica 2009/125/ES

Meno/ titul : Richard Hsu / Quality Management Division Senior Manager
Podpis : Dátum (dd/mm/rrrr): 01/10/2014

Slovenščina (Slovene)

Okoljsko deklaracijo izdelka

RoHS Direktiva 2011/65/EU
WEEE Direktiva 2012/19/EU
PPW Direktiva 94/62/ES
REACH Uredba (ES) št. 1907/2006
ErP Direktiva 2009/125/ES

Ime/ naziv : Richard Hsu / Quality Management Division Senior Manager
Podpis : Datum (dd/mm/ll): 01/10/2014

Suomi (Finnish)

Standardiin perustuva ympäristötuoteseloste

RoHS Direktiivi 2011/65/EU
WEEE Direktiivi 2012/19/EU
PPW Direktiivi 94/62/EY
REACH ASETUS (EY) N:o 1907/2006
ErP Direktiivi 2009/125/EY

Nimi/ otsikko : Richard Hsu / Quality Management Division Senior Manager
Allekirjoitus : Päivämäärä (pp/kk/vvvv): 01/10/2014

Svenska (Swedish)

Miljöproduktdeklaration

RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EG
REACH Förordning (EG) nr 1907/2006
ErP Direktiv 2009/125/EG

Namn/ titel : Richard Hsu / Quality Management Division Senior Manager
Namnteckning : Datum (dd/mm/åååå): 01/10/2014

Ελληνικά (Greek)

Περιβαλλοντική δήλωση προϊόντος

RoHS Οδηγία 2011/65/ΕΕ
WEEE Οδηγία 2012/19/ΕΕ
PPW Οδηγία 94/62/ΕΚ
REACH Κ ανανησμοσ (ΕΚ) αρθ. 1907/2006
ErP Οδηγία 2009/125/ΕΚ

Δνομα/ Τιτλος : Richard Hsu / Quality Management Division Senior Manager
Υπογραφη : Ημερομηνια (ηη/μμ/εεεε): 01/10/2014

Norsk (Norwegian)

Miljødeklarasjon

RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EF
REACH Forordning (EF) nr. 1907/2006
ErP Direktiv 2009/125/EF

Navn/ tittel : Richard Hsu / Quality Management Division Senior Manager
Signatur : Dato (dd/mm/åååå) : 01/10/2014

台灣

安全警告

為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
- 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W