eir D1000 modem

Wireless N ADSL2+ 4-port Gateway

Version 2.00
Edition 1, 6/2013

User's Guide

Default Login Details	
LAN IP Address	http://192.168.1.254
User Name	admin
Password	see wireless key on the back label

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.

Table of Contents

PART I
User's Guide

1

Introduction

1.1 Overview

The eir D1000 modem is an ADSL2+ router that integrates DSL and NAT, and provides ease of installation and high-speed, shared Internet access. The Device is also a complete security solution with a robust firewall and content filtering.

Only use firmware for your Device's specific model. Refer to the label on the bottom of your Device.

1.2 Ways to Manage the Device

Use any of the following methods to manage the Device.

- Web Configurator. This is recommended for everyday management of the Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- TR-069. This is an auto-configuration server used to remotely configure your device.

1.3 Good Habits for Managing the Device

Do the following things regularly to make the Device more secure and to manage the Device 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 Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Device. You could simply restore your last configuration.

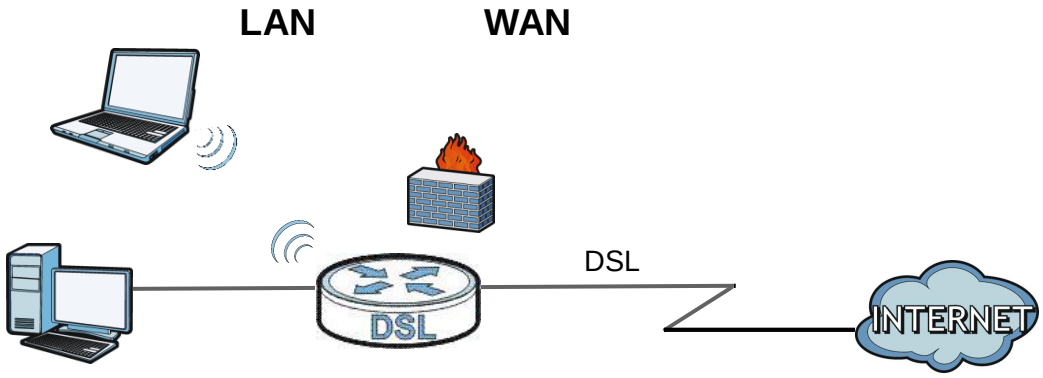
1.4 Applications for the Device

Here are some example uses for which the Device is well suited.

1.4.1 Internet Access

Your Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. Computers can connect to the Device's Ethernet ports (or wirelessly).

Figure 1 Device's Router Features



You can also configure firewall and filtering feature on the Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

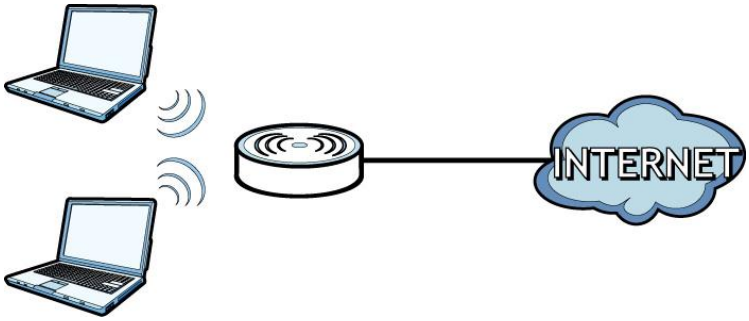
Use the filtering feature to block access to specific web sites or Internet applications such as MSN or Yahoo Messenger. You can also configure IP/MAC filtering rules for incoming or outgoing traffic.

Use QoS to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that the Device gives voice over Internet calls high priority, and/or limit bandwidth devoted to the boss's excessive file downloading.

1.4.2 Wireless Access

The Device is a wireless Access Point (AP) for IEEE 802.11b/g/n compliant clients, such as notebook computers or PDAs and iPads. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables. You can set up a wireless network with WPS (WiFi Protected Setup) or manually add a client to your wireless network.

Figure 2 Wireless Access Example



1.4.3 Using the WPS/WLAN Button

By default, the wireless network on the Device is turned on. To turn it off, simply press the **WPS/ WLAN** button on top of the device for over 5 seconds. When the **WPS/WLAN** LED is green, the wireless network is active.

You can also use the **WPS/WLAN** button to quickly set up a secure wireless connection between the Device and a WPS-compatible client by adding one device at a time.

To activate WPS:

1. Make sure the **POWER** LED is on and not blinking.
2. Press the **WPS/WLAN** button for 1-5 seconds and release it.
3. Press the WPS button on another WPS-enabled device within range of the Device. The **WPS/WLAN** LED should flash while the Device sets up a WPS connection with the other wireless device.
4. Once the connection is successfully made, the **WPS/WLAN** LED shines green.

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 side panel of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the user name and password will be reset to the default.

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 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

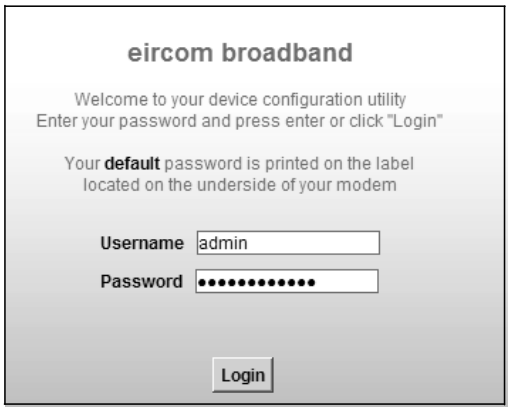
In order to use the web configurator, you need to allow:

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

2.1.1 Accessing the Web Configurator

1. Make sure your Device hardware is properly connected.
2. Launch your web browser.
3. Type "192.168.1.254" as the URL.
4. A password screen displays. Type “admin” (default) as the username and enter the default password (which is the same as the wireless key on the Device’s back label), then click **Login**. If you have changed the password, enter your new password and click **Login**.

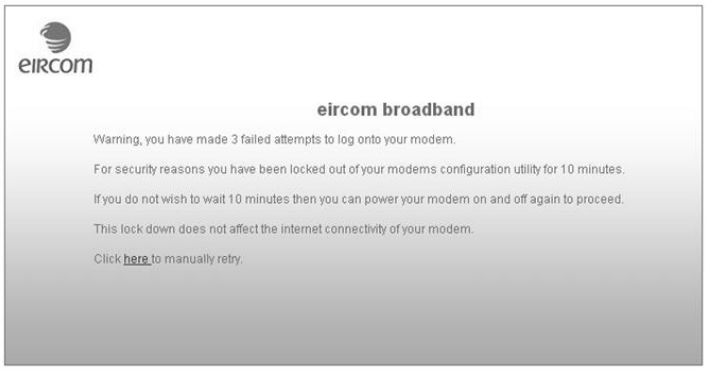
Figure 3 Password Screen



Note: For security reasons, the Device automatically logs you out if you do not use the web configurator for 900 seconds (default). If this happens, log in again.

5 If you enter the wrong username and/or password three times, the Device lockes you out of the login screen for ten minutes and the following screen displays.

Figure 4 Lockout Screen



6 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 **Skip** to proceed to the next screen if you do not want to change the password now.

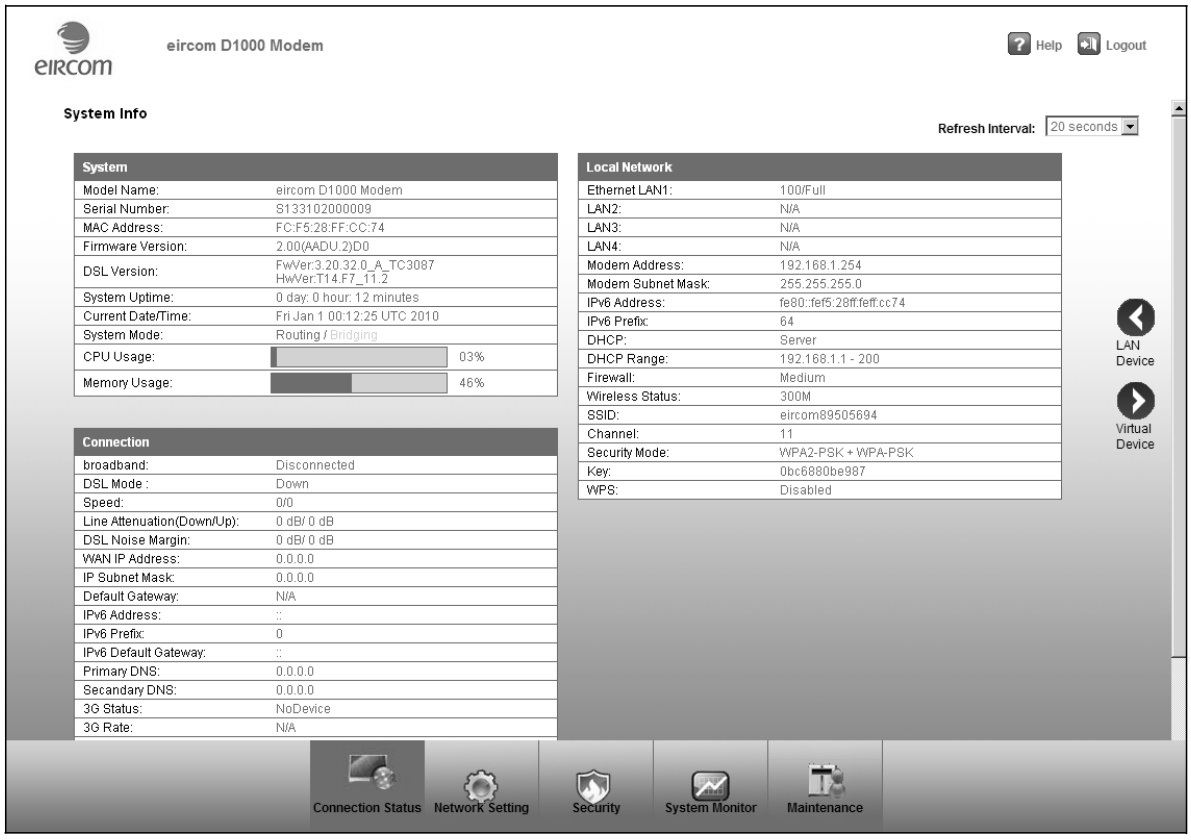
Figure 5 Change Password Screen

The following screen displays and asks if you want to change your wireless settings, including SSID and wireless security key. If you have changed the settings, click **Apply**. If not, click **Skip** to proceed to the **Connection Status** screen if you do not want to change them now.

Figure 6 Change Wireless Settings Screen

7 The **Connection Status** screen appears.

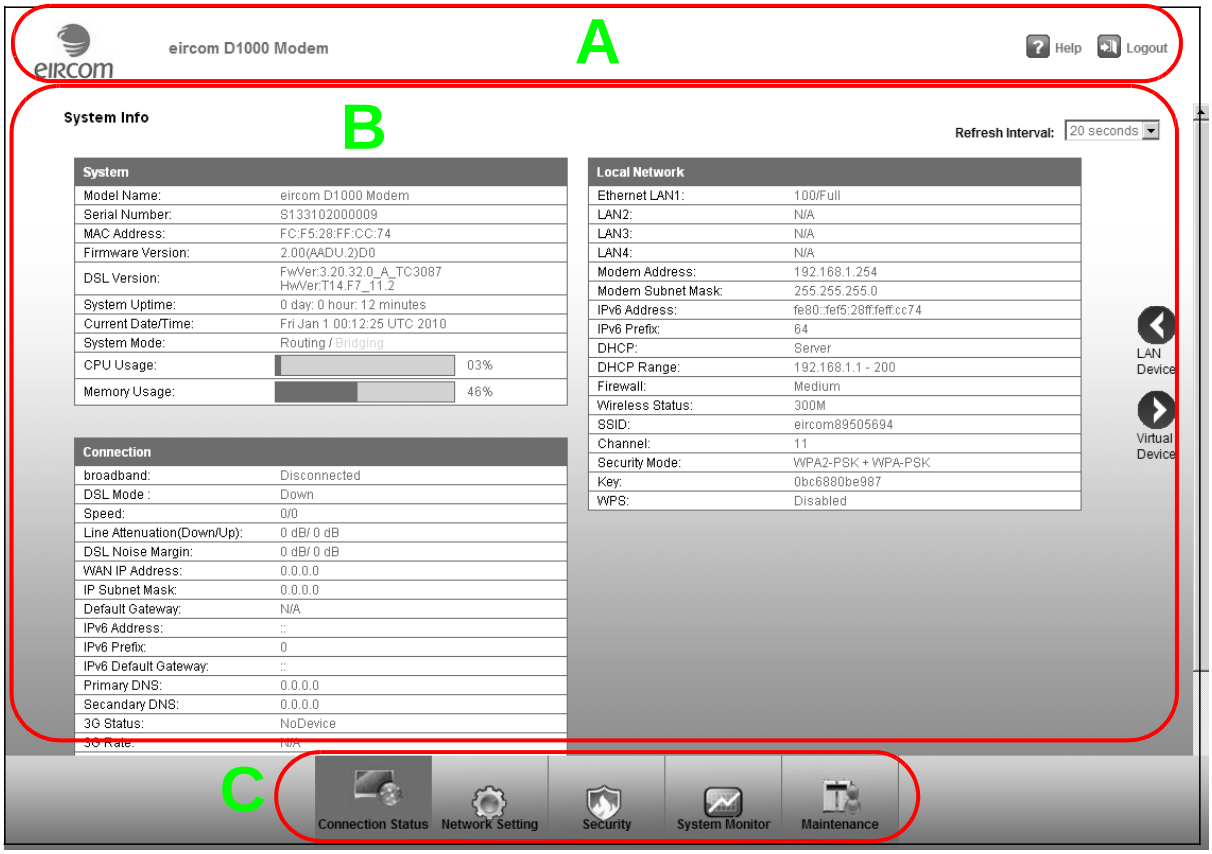
Figure 7 Connection Status



8 The **System Info** screen shows. You can view the Device's interface and system information.

2.2 The Web Configurator Layout

Figure 8 Web Configurator Layout Screen



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

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

2.2.1 Title Bar

The title bar shows the following icon in the upper right corner.

Click this icon to log out of the web configurator.

Click the **Help** icon to go to eir's support website. Click the **Logout** icon to log out of the web configurator.

2.2.2 Main Window

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

If you click **LAN Device** on the **System Info** screen, the **Connection Status** screen appears. See Chapter 3 on page 27 for more information about the **Connection Status** screen.

If you click **Virtual Device** on the **System Info** screen, a visual graphic appears, showing the connection status of the Device's ports.

Figure 9 Virtual Device

2.2.3 Navigation Panel

Use the menu items on the navigation panel to open screens to configure Device features. The following table describes each menu item.

Table 1 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the Device's interface and system information.
Network Setting		
Broadband	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	More Connections	Use this screen to configure additional WAN connections.
	3G Backup	Use this screen to configure your 3G backup Internet connection settings.

Table 1 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Wireless	General	Use this screen to turn the wireless connection on or off, specify the SSID(s) and configure the wireless LAN settings and WLAN authentication/security settings.
	More AP	Use this screen to configure multiple BSSs on the Device.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the Device.
	WPS	Use this screen to use WPS (Wi-Fi Protected Setup) to establish a wireless connection.
	WDS	Use this screen to set up Wireless Distribution System (WDS) links to other access points.
	WMM	Use this screen to enable or disable Wi-Fi MultiMedia (WMM).
	Scheduling	Use this screen to configure when the Device enables or disables the wireless LAN.
	Advanced	Use this screen to configure advanced wireless settings such as output power.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	IP Alias	Use this screen to partition your LAN interface into dfferent logical networks.
	UPnP	Use this screen to enable the UPnP function.
	IPv6 LAN Setup	Use this screen to configure the IPv6 settings on the Device's LAN interface.
	File Sharing	Use this screen to set up file sharing.
	Print Server	The print server screen is used to enable the print server function.
Static Route	Static Route	Use this screen to view and set up static routes on the Device.
	IPv6 Static Route	Use this screen to configure IPv6 static routes.
QoS	General	Use this screen to enable QoS and decide allowable bandwidth using QoS.
	Queue	Use this screen to configure QoS queue assignment.
	Class Setup	Use this screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.
	Game List	Use this screen to give priority to traffic for specific games.
NAT	General	Use this screen to activate/deactivate NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to activate/deactivate the SIP ALG feature.
Port Isolation	General	Use this screen to activate/deactivate port isolation.
	Port Isolation	Use this screen to configure and view port binding groups.
Dynamic DNS	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
Security		

Table 1 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Filter	IP/MAC Filter	Use this screen to configure IPv4/MAC filtering rules for incoming or outgoing traffic.
	IPv6/MAC Filter	Use this screen to configure IPv6/MAC filtering rules for incoming or outgoing traffic.
Firewall	General	Use this screen to activate/deactivate the firewall.
	Default Action	Use this screen to set the default action that the firewall takes on packets that do not match any of the firewall rules.
	Rules	Use this screen to view the configured firewall rules and add, edit or remove a firewall rule.
	DoS	Use this screen to set the thresholds that the Device uses to determine when to start dropping sessions that are not fully established (half-open sessions).
Parental Control	Parental Control	Use this screen to define time periods and days during which the Device performs parental control and/or block web sites with the specific URL.
Certificates	Local Certificates	Use this screen to export self-signed certificates or certification requests and import the Device's CA-signed certificates.
	Trusted CA	Use this screen to save CA certificates to the Device.
System Monitor		
Log	Log	Use this screen to view the logs for the level that you selected. You can export or e-mail the logs.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Device.
	NAT	Use this screen to view the status of NAT sessions on the Device.
Maintenance		
Users Account	Users Account	Use this screen to configure the passwords your user accounts.
System	System	Use this screen to configure management inactivity time-out setting.
Time Setting	Time Setting	Use this screen to change your Device's time and date.
Log Setting	Log Setting	Use this screen to configure the Device's log settings and which logs and/or immediate alerts the Device is to record.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the Device without turning the power off.
Remote MGMT	WWW, Telnet, FTP, SNMP, DNS, ICMP, SSH	Use this screen to enable specific traffic directions for specific network service.
Diagnostic	Ping	Use this screen to test the connections to other devices.
	DSL Line	Use this screen to identify problems with the DSL connection.

PART II
Technical Reference

3

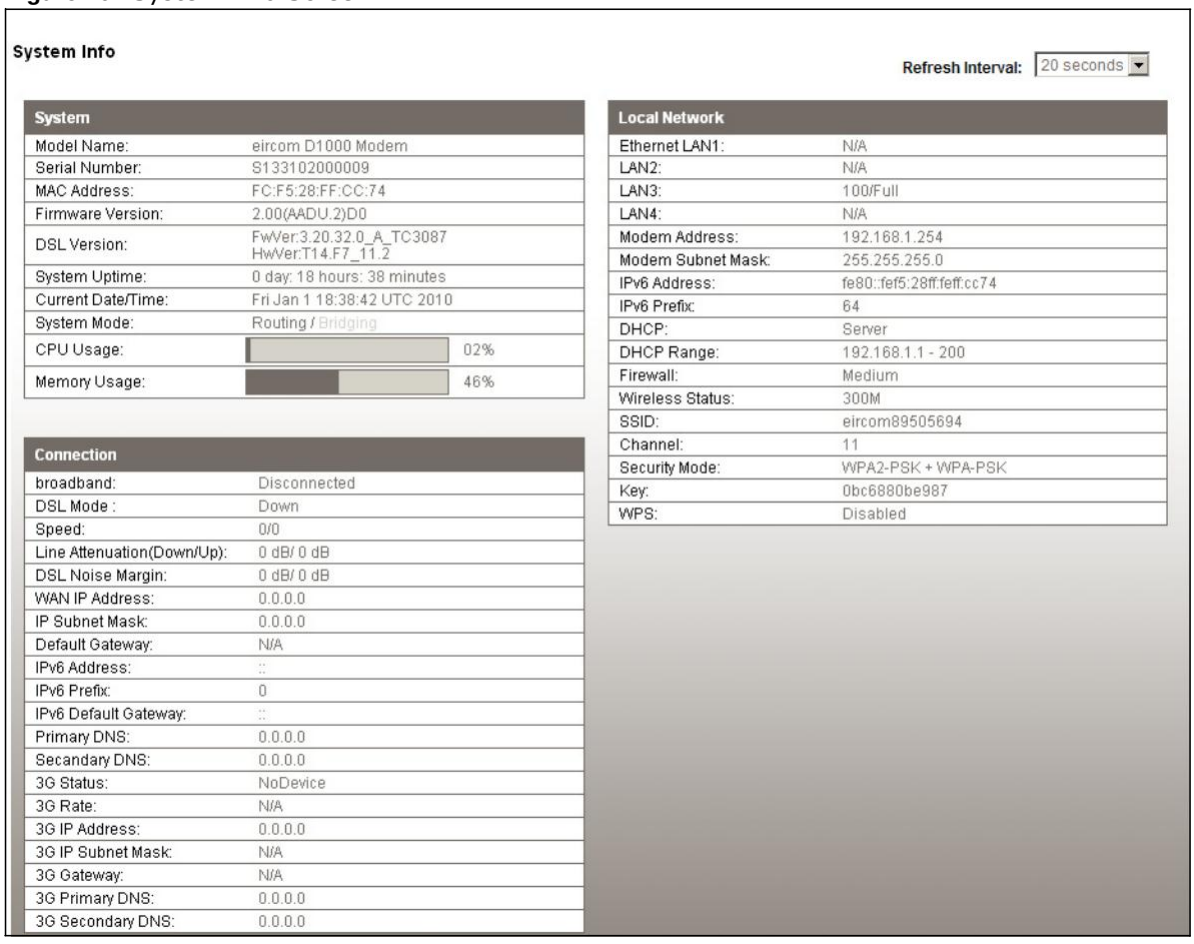
The System Info Screen

3.1 Overview

After you log into the web configurator, the System Info screen shows. Use this screen to view the status of the Device.

3.2 The System Info Screen

Figure 10 System Info Screen



Each field is described in the following table.

Table 2 System Info Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
System	
Model Name	This is the model name of your device.
Serial Number	This field displays the certificate's identification number given by the certification authority.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your Device.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created.
DSL Version	This is the current version of the Device's DSL modem code.
System UpTime	This field displays how long the Device has been running since it last started up. The Device starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it (see Chapter 1 on page 15).
Current Date/ Time	This field displays the current date and time in the Device. You can change this in **Maintenance > Time Setting**.
System Mode	This displays whether the Device is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the Device's processing ability is currently used. When this percentage is close to 100%, the Device 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.
Memory Usage	This field displays what percentage of the Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100% and remains like that for a high period of time, the Device may become unstable and you should restart it. See Section 23.3 on page 193, or turn off the device (unplug the power) for a few seconds.
Connection	
Broadband	This is the current status of your broadband.
DSL Mode	This is the DSL standard that your Device is using.
Speed	This shows the speed of your DSL connection.
Line Attenuation (Down/Up)	This indicates the line attenuation status for each upstream and downstream band.
DSL Noise Margin	This is the signal to noise ratio for the downstream part of the connection (coming into the Device from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is.
WAN IP Address	This field displays the current IP address of the Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
Default Gateway	This is the IP address of the default gateway, if applicable.
IPv6 Address	This is the current IPv6 address of the Device in the WAN. Click this to go to the screen where you can change it.
IPv6 Prefix	This is the current IPv6 prefix length in the WAN.
IPv6 Default Gateway	This is the IPv6 address of the default gateway, if applicable.
Primary/ Secondary DNS	This is the primary/secondary DNS server IP address assigned to the Device.
3G Status	This shows the current status of your 3G connection. **NoDevice** is shown when no 3G card is inserted.

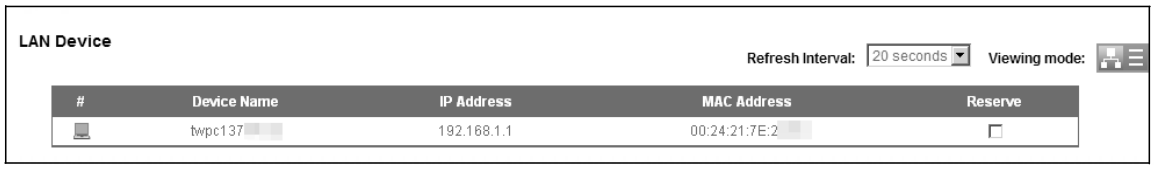
Table 2 System Info Screen (continued)

LABEL	DESCRIPTION
3G Rate	This shows the rate of the 3G connection if it is available.
3G IP Address	This shows the IP address for the 3G connection.
3G IP Subnet Mask	This shows the current subnet mask for the 3G connection.
3G Gateway	This shows the IP address of the 3G connection's default gateway.
3G Primary/ Secondary DNS	This shows the first and second DNS server address assigned by the ISP.
Local Network	
LAN1 LAN2 LAN3 LAN4	This displays the link speed and duplex mode of the LAN port(s) in use. (LAN1 is reserved for Ethernet WAN.)
Modem Address	This field displays the current IP address of the Device in the LAN.
Modem Subnet Mask	This field displays the current subnet mask in the LAN.
IPv6 Address	This is the current IPv6 address of the Device in the LAN. Click this to go to the screen where you can change it.
IPv6 Prefix	This is the current IPv6 prefix length in the LAN.
IPv6 Prefix	This is the current IPv6 prefix in the LAN.
DHCP	This field displays what DHCP services the Device is providing to the LAN. Choices are: **Server** - The Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The Device is not providing any DHCP services to the LAN.
DHCP Range	This is the IP address range that the Device is assigning to other computers in the LAN when it acts as a DHCP server.
Firewall	This shows the security level setting of the Device's firewall.
Wireless Status	This displays whether wireless LAN is turned on or off.
SSID	This is the descriptive name used to identify the Device in the wireless LAN.
Channel	This is the channel number used by the Device now.
Security Mode	This displays the type of security the Device is using in the wireless LAN.
Key	This displays the wireless key of the Device.
WPS	**Configured** displays when the WPS security settings have been configured and wireless clients can connect with the device through WPS. **Unconfigured** displays when the device has not been configured and wireless clients can't establish a link with the device through WPS.

3.3 The LAN Device Screen

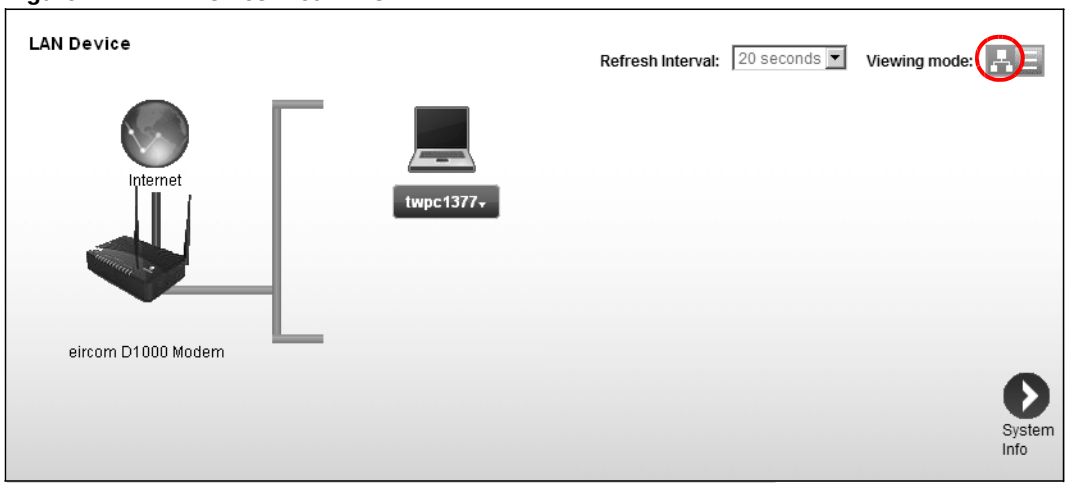
Click **LAN Device** in the **System Info** screen to view the information of the client(s) connected to the Device. In this screen, you can configure how often you want the Device to update this screen in **Refresh Interval**.

Figure 11 LAN Device: List View



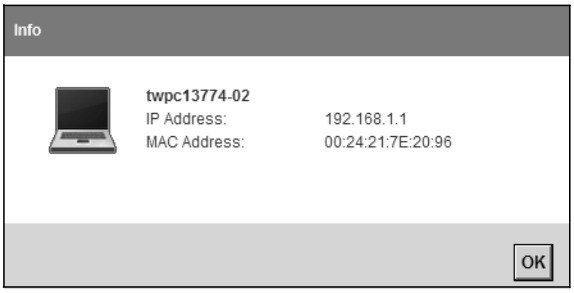
If you want to view the connection status of the Device and its client(s), click **Icon View** in the **Viewing mode** selection box.

Figure 12 LAN Device: Icon View



Click on a client's name to show an **Info** button.

- Click it to view information about the client. Click **OK** to close the screen.



4

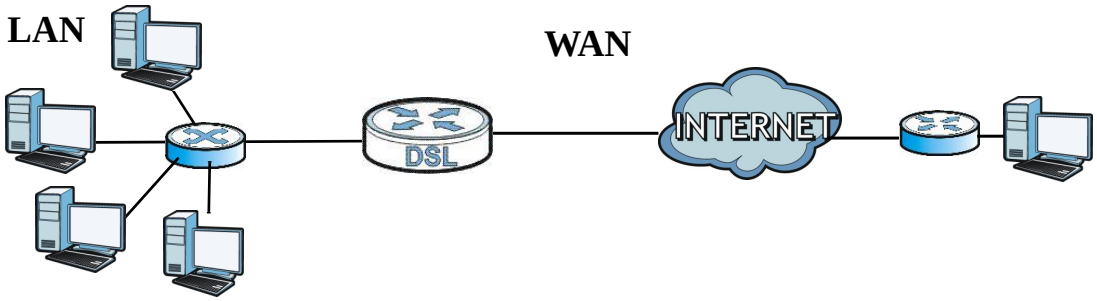
Broadband

4.1 Overview

This chapter describes the Device's **Broadband** screens. Use these screens to configure your Device 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 13 LAN and WAN



4.1.1 What You Can Do in the WAN Screens

- Use the **Internet Connection** screen (Section 4.2 on page 32) to configure the WAN settings on the Device for Internet access.
- Use the **More Connections** screen (Section 4.3 on page 36) to set up additional Internet access connections.
- Use the **3G Backup** screen (Section 4.4 on page 40) to configure your 3G backup Internet connection settings.

4.1.2 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) or PPPoA, 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 Device, which makes it accessible from an outside network. It is used by the Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the Device 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).

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 is still in wide use.

IPv6

IPv6 (Internet Protocol version 6), is designed to increase IP address space and enhance features. The Device supports IPv4/IPv6 dual stack and can connect to IPv4 and IPv6 networks.

Finding Out More

See Section 4.5 on page 42 for technical background information on WAN.

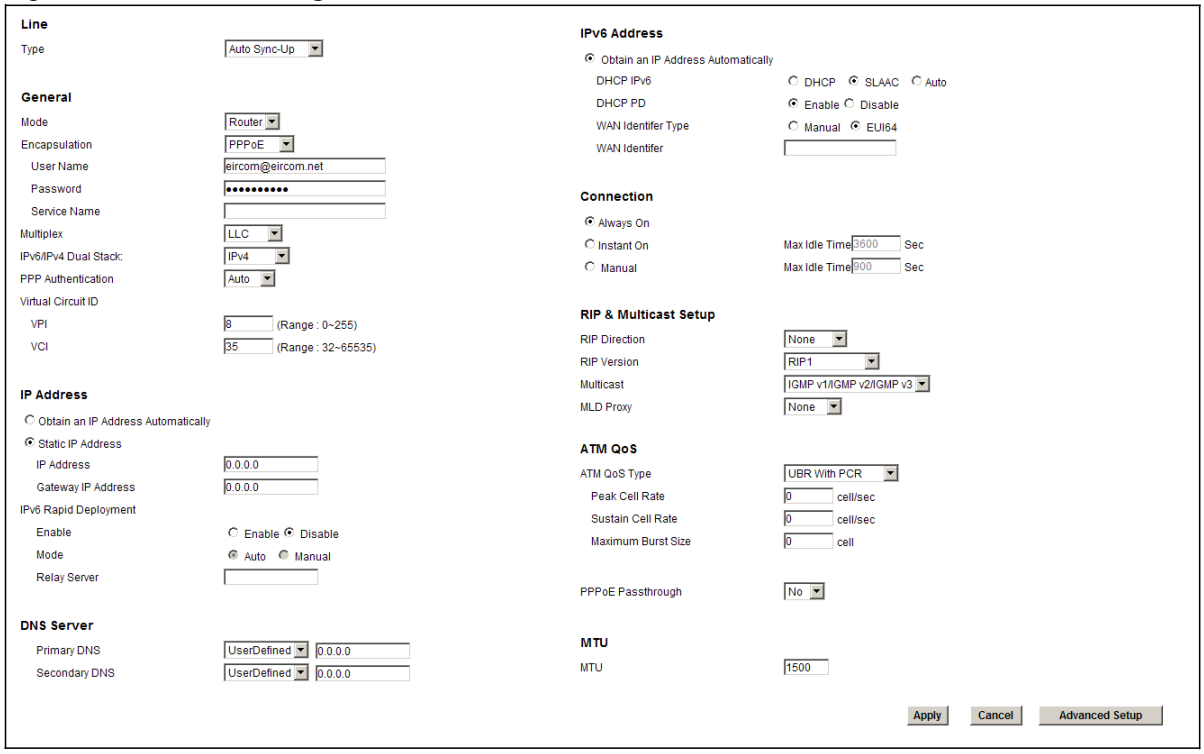
4.1.3 Before You Begin

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

4.2 The Internet Connection Screen

Use this screen to change your Device's WAN settings. Click **Network Setting > Broadband > Internet Connection**. The screen differs by the WAN type and encapsulation you select.

Figure 14 Network Setting > Broadband > Internet Connection



The following table describes the labels in this screen.

Table 3 Network Setting > Broadband > Internet Connection

LABEL	DESCRIPTION
Line	
Type	Select the mode supported by your ISP. Use **Auto Sync-Up** if you are not sure which mode to choose from. The Device dynamically diagnoses the mode supported by the ISP and selects the best compatible one for your connection. Other options are **Ethernet(ETH1)**, **ADSL2+**, **ADSL2**, **G.DMT**, **T1.413** and **G.lite**.
General	
Mode	Select **Router** (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 Device.
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 **Router** in the **Mode** field, select **IPoE**, **RFC 1483**, **PPPoE**, or **PPPoA**. If you select **Bridge** in the **Mode** field, method of encapsulation is not available.
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.

Table 3 Network Setting > Broadband > Internet Connection (continued)

LABEL	DESCRIPTION
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC-Mux** or **LLC**.
IPv6/IPv4 Dual Stack	If you select **IPv4/IPv6**, the Device can connect to both IPv4 and IPv6 networks and choose the protocol for applications according to the address type. If you select **IPv4** or **IPv6** the Device will operate in IPv4 or IPv6 mode.
PPP Authentication	The Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO** - Your Device accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your Device accepts CHAP only. **PAP** - Your Device accepts PAP only.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
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.
IP Address	This option is available if you select **Router** 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** and **Gateway IP Address** fields (supplied by your ISP) below.
IPv6 Rapid Deployment	This is available only when you select **IPv4** in the **IPv6/IPv4 Dual Stack** field. By enabling the IPv6 Rapid Deployment function, the Device uses an ISP's IPv6 address prefix instead of the 2002::/48 prefix. The operational domain of 6RD is limited to and controlled by the ISP's network. 6RD hosts are ensured to be reachable from all native IPv6 addresses as 6RD only uses relay servers within control of the ISP.
Enable	Select this option to enable IPv6 Rapid Deployment.
Mode	Select **Auto** or **Manual** mode. If you select **Manual**, enter the tunneling relay server's IPv4 address in the field below.
Relay Server	Enter the tunneling relay server's IPv4 address in this field.
DNS Server - This section is not available when you select **Bridge** in the **Mode** field.	
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
IPv6 Address (The following fields are available only when you select **IPv6** in the **IPv6/IPv4 Dual Stack** field.)	
Obtain an IP Address Automatically	Select this option if you want to have the Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.

Table 3 Network Setting > Broadband > Internet Connection (continued)

LABEL	DESCRIPTION
DHCP IPv6	Select **DHCP** if you want to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the Device using the IPv6 prefix from an RA. Select **SLAAC** (Stateless address autoconfiguration) to have the Device use the prefix to automatically generate a unique IP address that does not need to be maintained by a DHCP server. Selelct **Auto** to have the Device indicate to hosts for IPv6 address generation depending on the M/O (Managed/Other) flag values in the router advertisements sending to hosts. • If M flag is 1, the Device will indicate to hosts to obtain network settings (such as WAN IP, LAN prefix and DNS settings) through DHCPv6. • If M flag is 0, the Device will check O flag. • If O flag is 1, the Device will indicate to hosts to obtain DNS information and LAN prefix through DHCPv6. • If O flag is 0, the Device will not get information through DHCPv6.
DHCP PD	Select **Enable** to use **DHCP PD** (Prefix Delegation) to allow the Device to pass the IPv6 prefix information to its LAN hosts. The hosts can then use the prefix to generate their IPv6 addresses.
WAN Identifier Type	Select **Manual** to manually enter a WAN Identifier as the interface ID to identify the WAN interface. The WAN Identifier is appended to the IPv6 address prefix to create the routable global IPv6 address. Select **EUI64** to use the EUI-64 format to generate an interface ID from the MAC address of the WAN interface.
WAN Identifier	If you selected **Manual**, enter the WAN Identifier in this field. The WAN identifier should be unique and 64 bits in hexadecimal form. Every 16 bit block should be separated by a colon as in XXXX:XXXX:XXXX:XXXX where X is a hexadecimal character. Blocks of zeros can be represented with double colons as in XXXX:XXXX::XXXX.
Connection (PPPoA and PPPoE encapsulation only)	
Always On	Select **Always On** when you want your connection up all the time. The Device will try to bring up the connection automatically if it is disconnected.
Instant On	Select **Instant On** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Advanced Setup	Click this to display the **Advanced WAN Setup** screen and edit more details of your WAN setup. Click this button again to display less fields in this screen.
RIP & Multicast Setup	
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 Device 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**, **RIP2-B/RIP2-M**.
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 Device supports **IGMP-v1/IGMP-v2/IGMP-v3**. Select **None** to disable it.

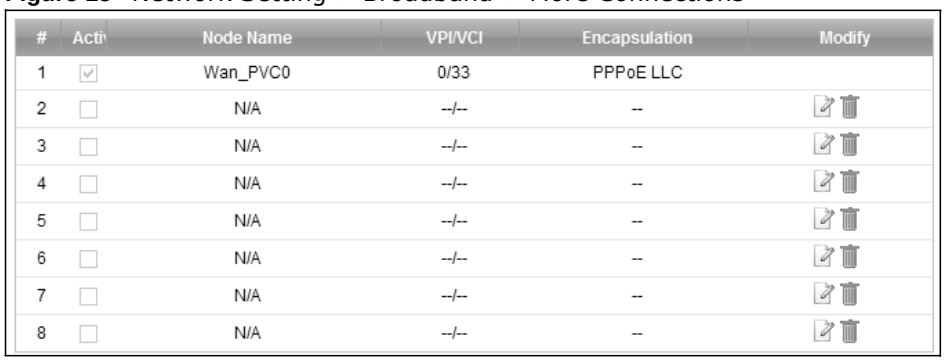
Table 3 Network Setting > Broadband > Internet Connection (continued)

LABEL	DESCRIPTION
MLD Proxy	Select the version of MLD proxy (**MLDv1** or **MLDv2**) to have the Device act as for this connection. This allows the Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly. Select **None** to turn off MLD proxy.
ATM QoS	
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR With PCR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **Realtime VBR** (real-time Variable Bit Rate) type for applications with bursty connections that require closely controlled delay and delay variation. Select **Non Realtime VBR** (non real-time Variable Bit Rate) type for connections that do not require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
PPPoE Passthrough	If encapsulation type is PPPoE, select **Yes** to enable PPPoE Passthrough. In addition to the Device's built-in PPPoE client, you can select this to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the device. Each host can have a separate account and a public WAN IP address.
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.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

4.3 The More Connections Screen

The Device allows you to configure more than one Internet access connection. To configure additional Internet access connections click **Network Setting > Broadband > More Connections**. The screen differs by the encapsulation you select. When you use the **Broadband > Internet Connection** screen to set up Internet access, you are configuring the first WAN connection.

Figure 15 Network Setting > Broadband > More Connections



#	Acti	Node Name	VPI/VCI	Encapsulation	Modify
1	☑	Wan_PVC0	0/33	PPPoE LLC	
2	☐	N/A	--/--	--	
3	☐	N/A	--/--	--	
4	☐	N/A	--/--	--	
5	☐	N/A	--/--	--	
6	☐	N/A	--/--	--	
7	☐	N/A	--/--	--	
8	☐	N/A	--/--	--	

The following table describes the labels in this screen.

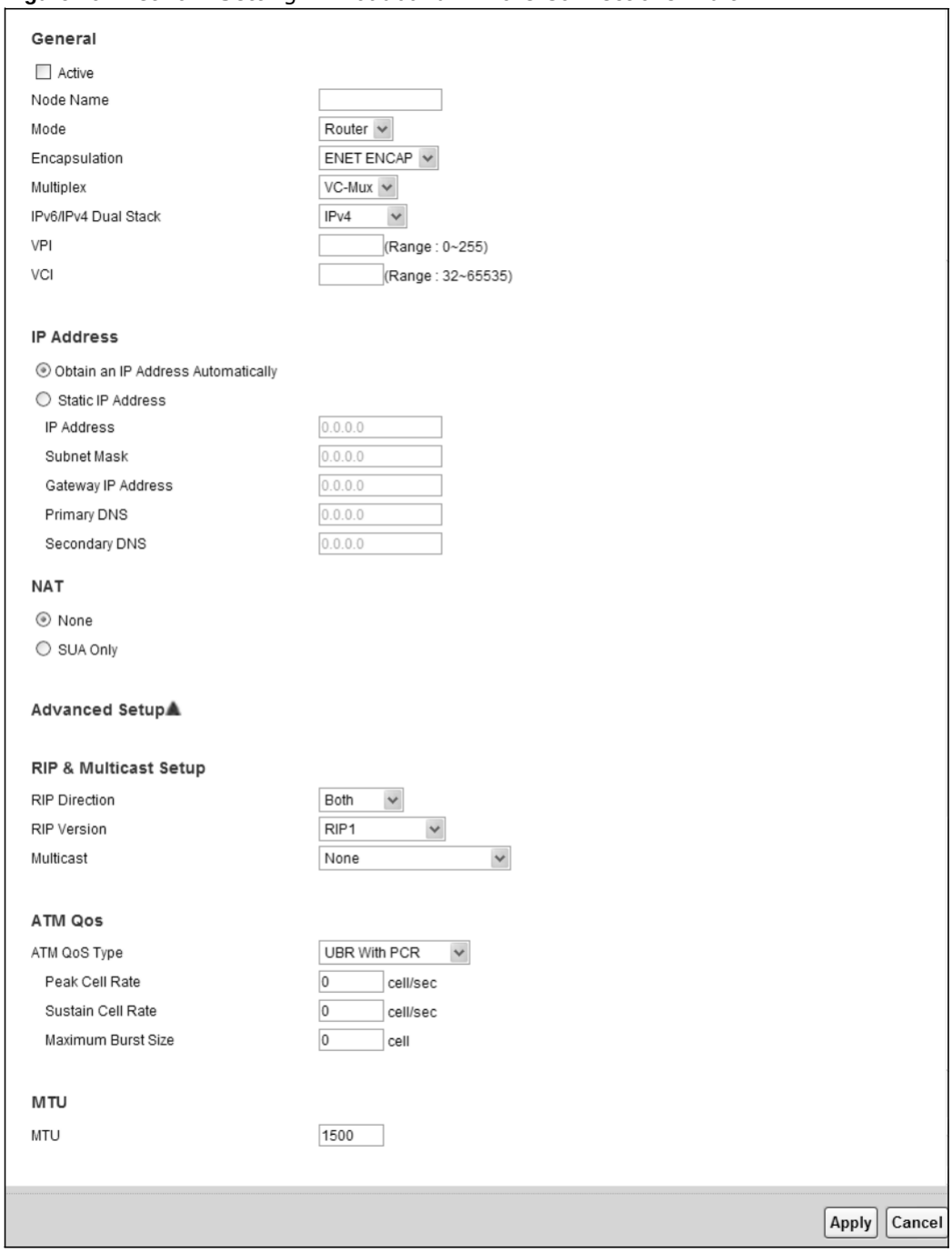
Table 4 Network Setting > Broadband > More Connections

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. Clear the check box to disable the connection. Select the check box to enable it.
Node Name	This is the name you gave to the Internet connection.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers configured for this WAN connection.
Encapsulation	This field indicates the encapsulation method of the Internet connection.
Modify	The first (ISP) connection is read-only in this screen. Use the **Broadband > Internet Connection** 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.

4.3.1 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 16 Network Setting > Broadband > More Connections: Edit



The following table describes the labels in this screen.

Table 5 Network Setting > Broadband > More Connections: Edit

LABEL	DESCRIPTION
General	
Active	Select the check box to activate or clear the check box to deactivate this connection.
Node Name	Enter a unique, descriptive name of up to 13 ASCII characters for this connection.

Table 5 Network Setting > Broadband > More Connections: Edit (continued)

LABEL	DESCRIPTION
Mode	Select **Router** from the drop-down list box if your ISP allows multiple computers to share an Internet account. If you select **Bridge**, the Device 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 **Router** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**. If you select **Bridge** in the **Mode** field, method of encapsulation is not available.
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**. By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol. For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols.
IPv6/IPv4 Dual Stack	If you select **Enable**, the Device can connect to IPv4 and IPv6 networks and choose the protocol for applications according to the address type. If you select **Disable,** the Device will operate in IPv4 mode.
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.
IP Address	This option is available if you select **Router** 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 **RFC 1483**, 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 **RFC 1483**, enter the IP address given by your ISP in the **IP Address** field.
Subnet Mask	Enter a subnet mask in dotted decimal notation.
Gateway IP Address	Specify a gateway IP address (supplied by your ISP).
Primary DNS	Enter the primary DNS server's address for the Device.
Secondary DNS	Enter the secondary DNS server's address for the Device.
NAT	**SUA Only** is available only when you select **Router** in the **Mode** field. Select **SUA Only** if you have one public IP address and want to use NAT. Otherwise, select **None** to disable NAT.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.
Advanced Setup	Click this to display more fields in this screen to configure more details of your WAN settings.
RIP & Multicast Setup	
RIP Direction	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**, **RIP2-B** and **RIP2-M**.

Table 5 Network Setting > Broadband > More Connections: Edit (continued)

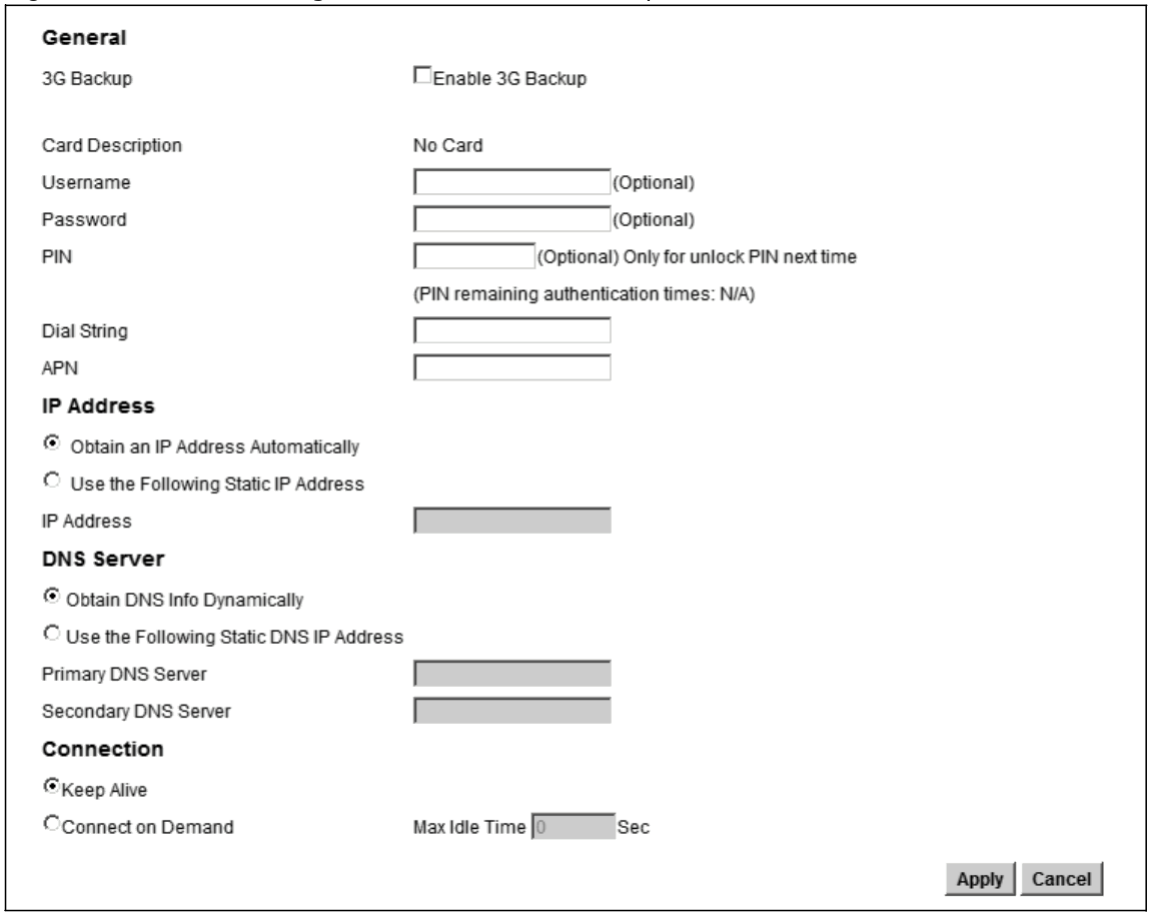
LABEL	DESCRIPTION
Multicast	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a multicast group. The Device supports **IGMP-v1**, **IGMP-v2** and **IGMP-v3**. Select **None** to disable it.
ATM QoS	
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **nrtVBR** (Variable Bit Rate-non Real Time) or **rtVBR** (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
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 100-1500.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

4.4 The 3G Backup Screen

Use this screen to configure your 3G settings. Click **Network Setting > Broadband > 3G Backup**.

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 17 Network Setting > Broadband > 3G Backup



The following table describes the labels in this screen.

Table 6 Network Setting > Broadband > 3G Backup

LABEL	DESCRIPTION
General	
3G Backup	Select **Enable** to have the Device use the 3G connection as your WAN or a backup when the wired WAN connection fails.
Card description	This field displays the manufacturer and model name of your 3G card if you inserted one in the Device. Otherwise, it displays **N/A**.
Username	Type the user name (of up to 64 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 64 ASCII printable characters) associated with the user name above.
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.
Dial string	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.

Table 6 Network Setting **>** Broadband > 3G Backup (continued)

LABEL	DESCRIPTION
APN	Enter the APN (Access Point Name) 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.
Obtain an IP Address Automatically	Select this option If your ISP did not assign you a fixed IP address.
Use the following static IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use the following static IP address**.
Obtain DNS info dynamically	Select this to have the Device get the DNS server addresses from the ISP automatically.
Use the following static DNS IP address	Select this to have the Device use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Connection	Select **Keep Alive** if you do not want the connection to time out. Select **Connect on Demand** if you do not want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	This value specifies the time in minutes that elapses before the Device automatically disconnects from the ISP.
Apply	Click **Apply** to save your changes back to the Device.
Cancel	Click **Cancel** to return to the previous configuration.

4.5 WAN Technical Reference

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

4.5.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The Device supports the following methods.

4.5.1.1 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.

4.5.1.2 PPP over Ethernet

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

4.5.1.3 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (Digital Subscriber Line (DSL) Access Multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

4.5.1.4 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.

4.5.2 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.

4.5.3 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.

4.5.4 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 PPPoA or 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 Address** assigned by your ISP, then they should also assign you a **Subnet Mask** and a **Gateway IP Address**.

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 Device 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 Device.

4.5.5 Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The Device does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the Device 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.

4.5.6 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.

4.6 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.

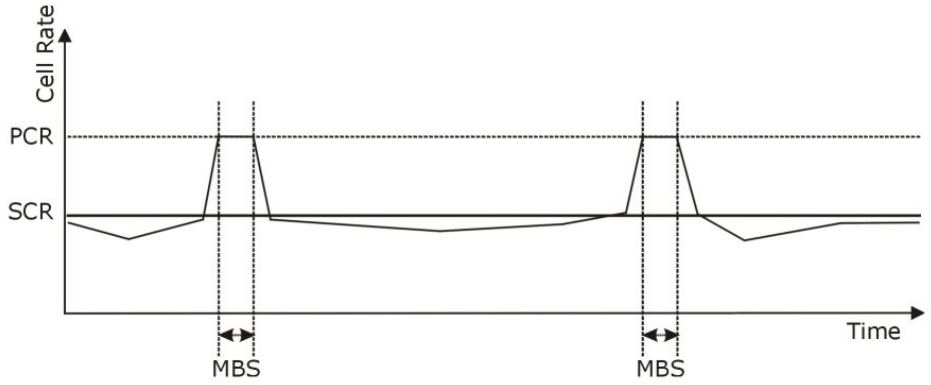
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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 18 Example of Traffic Shaping



4.6.1 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.

5

Wireless LAN

5.1 Overview

This chapter describes how to perform tasks related to setting up and optimizing your wireless network, including the following.

- Turning the wireless connection on or off.
- Configuring a name, wireless channel and security for the network.
- Using WiFi Protected Setup (WPS) to configure your wireless network.
- Setting up multiple wireless networks.
- Using a MAC (Media Access Control) address filter to restrict access to the wireless network.
- Performing other performance-related wireless tasks.

5.1.1 What You Can Do in the Wireless LAN Screens

This section describes the Device's **Network Setting > Wireless** screens. Use these screens to set up your Device's wireless connection.

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 5.2 on page 48).
- Use the **More AP** screen (see Section 5.3 on page 54) to set up multiple wireless networks on your Device.
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Device (Section 5.4 on page 56).
- Use the **WPS** screen (see Section 5.5 on page 57) to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the Device's WPS status.
- Use the **WDS** screen (see Section 5.6 on page 59) to set up a Wireless Distribution System, in which the Device acts as a bridge with other access points.
- Use the **WMM screen** to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications (Section 5.7 on page 60).
- Use the **Scheduling** screen (see Section 5.8 on page 60) to configure the dates/times to enable or disable the wireless LAN.
- Use the **Advanced** screen to configure wireless advanced features (Section 5.9 on page 61).

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and security in the **General** screen.

5.1.2 What You Need to Know About Wireless

Wireless Basics

"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Finding Out More

See Section 5.10 on page 63 for advanced technical information on wireless networks.

5.1.3 Before You Start

Before you start using these screens, ask yourself the following questions. See Section 5.1.2 on page 48 if some of the terms used here are not familiar to you.

- What wireless standards do the other wireless devices in your network support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices in your network support (WPA-PSK, for example)? What is the strongest security option supported by all the devices in your network?
- Do the other wireless devices in your network support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

  Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.
- What advanced options do you want to configure, if any? If you want to configure advanced options such as Quality of Service, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them as they are.

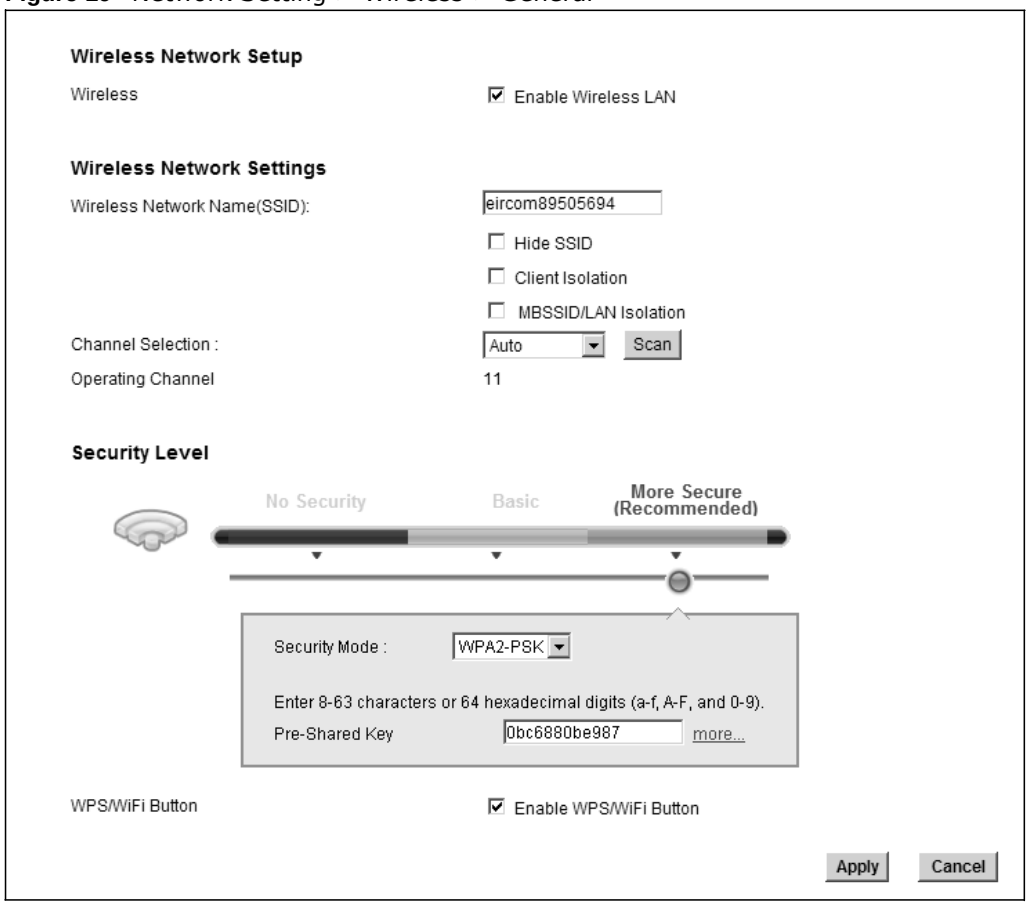
5.2 The General Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the Device from a computer connected to the wireless LAN and you change the Device's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Device's new settings.

Click **Network Setting** > **Wireless** to open the **General** screen.

Figure 19 Network Setting > Wireless > General



The following table describes the labels in this screen.

Table 7 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select **Enable Wireless LAN** to activate wireless LAN.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Client Isolation	Select this to keep the wireless clients in this SSID from communicating with each other through the Device.
MBSSID/LAN Isolation	Select this to keep the wireless clients in this SSID from communicating with clients in other SSIDs or wired LAN devices through the Device. Select both **Client Isolation** and **MBSSID/LAN Isolation** to allow this SSID's wireless clients to only connect to the Internet through the Device.
Channel Selection	Set the operating channel manually by selecting a channel from the **Channel Selection** list or use **Auto** to have it automatically determine a channel to use.

Table 7 Network Setting > Wireless > General (continued)

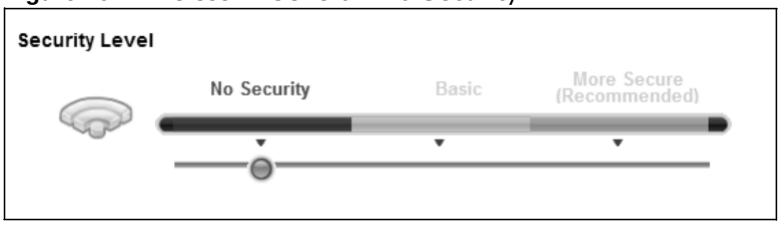
LABEL	DESCRIPTION
Operating Channel	This field displays the channel the Device is currently using.
Security Level	
Security Mode	Select **Basic** (WEP) or **More Secure** (WPA(2)-PSK, WPA(2)) to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
WPS/WiFi Button	Select the checkbox to enable the WPS/WiFi button.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

5.2.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any wireless security on your Device, your network is accessible to any wireless networking device that is within range.

Figure 20 Wireless > General: No Security



5.2.2 Basic (WEP Encryption)

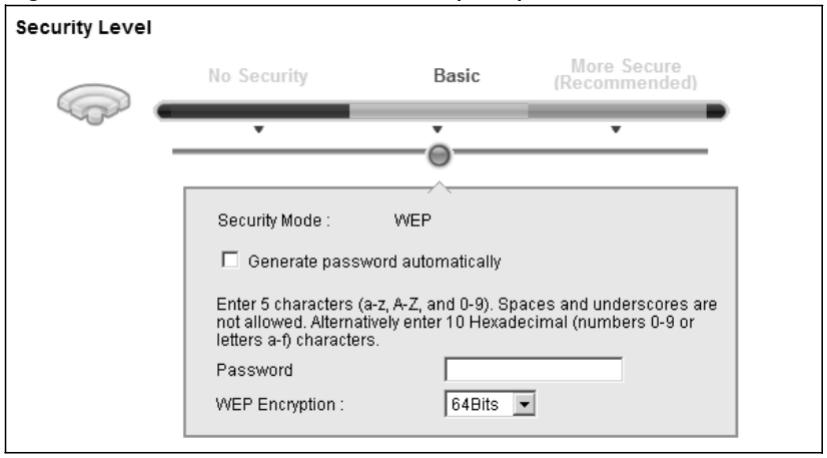
WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

Note: WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. For example, use WPA-PSK or WPA2-PSK if all your wireless devices support it, or use WPA or WPA2 if your wireless devices support it and you have a RADIUS server. If your wireless devices support nothing stronger than WEP, use the highest encryption level available.

Your Device allows you to configure one 64-bit or 128-bit WEP key.

In order to configure and enable WEP encryption, click **Network Setting** > **Wireless** to display the **General** screen, then select **Basic** as the security level.

Figure 21 Wireless > General: Basic (WEP)



The following table describes the wireless LAN security labels in this screen.

Table 8 Wireless > General: Basic (WEP)

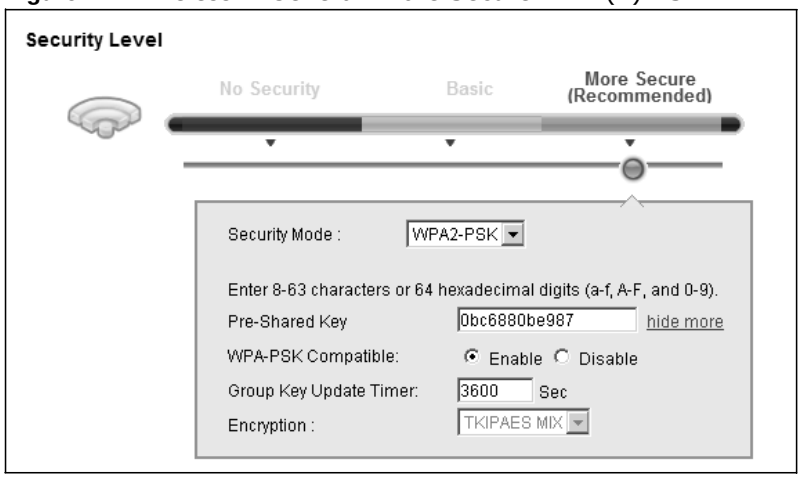
LABEL	DESCRIPTION
Security Level	Select **Basic** to enable WEP data encryption.
Generate password automatically	Select this option to have the Device automatically generate a password. The password field will not be configurable when you select this option.
Password	The password (WEP key) are used to encrypt data. Both the Device and the wireless stations must use the same password (WEP key) for data transmission. If you chose **64-bit** WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit** WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
WEP Encryption	Select **64-bits** or **128-bits**. This dictates the length of the security key that the network is going to use.

5.2.3 More Secure (WPA(2)-PSK)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

Click **Network Setting** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 22 Wireless > General: More Secure: WPA(2)-PSK



The following table describes the wireless LAN security labels in this screen.

Table 9 Wireless > General: More Secure: WPA(2)-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Select **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
Pre-Shared Key	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
more.../hide more	Click **more...** to show more fields in this section. Click **hide more** to hide them.
WPA-PSK Compatible	This field appears when you choose **WPA-PSK2** as the **Security Mode**. Select **Enable** to allow wireless devices using **WPA-PSK** security mode to connect to your Device. The Device supports WPA-PSK and WPA2-PSK simultaneously. Otherwise, select **Disable**.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients.
Encryption	This field displays the encryption type for data encryption. If you choose **WPA-PSK** as the security mode, the Device uses **TKIP** for data encryption. If you choose **WPA2-PSK** as the security mode and enable WPA-PSK Compatible, the Device uses either TKIP and AES (**TKIPAES MIX**) for data encryption. If you choose **WPA2-PSK** as the security mode but disable WPA-PSK Compatible, the Device uses **AES** for data encryption.

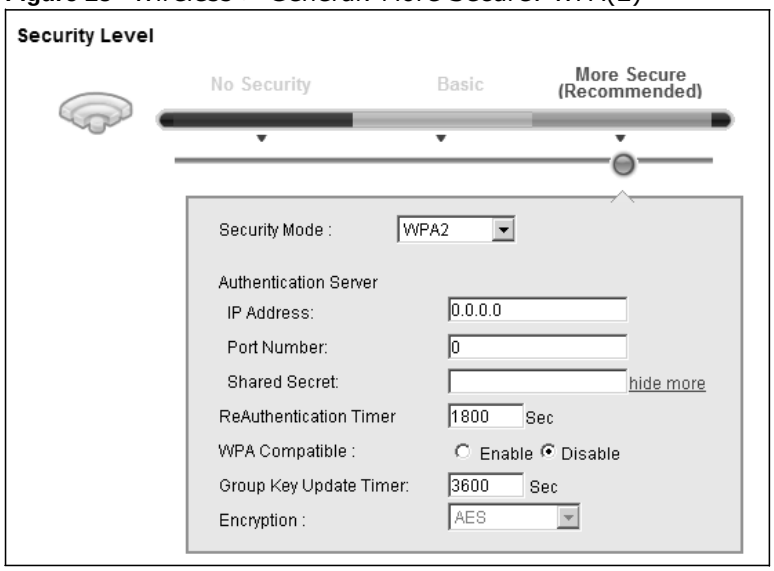
5.2.4 WPA(2) Authentication

The WPA2 security mode is currently the most robust form of encryption for wireless networks. It requires a RADIUS server to authenticate user credentials and is a full implementation the security protocol. Use this security option for maximum protection of your network. However, it is the least backwards compatible with older devices.

The WPA security mode is a security subset of WPA2. It requires the presence of a RADIUS server on your network in order to validate user credentials. This encryption standard is slightly older than WPA2 and therefore is more compatible with older devices.

Click **Network Setting** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA** or **WPA2** from the **Security Mode** list.

Figure 23 Wireless > General: More Secure: WPA(2)



The following table describes the labels in this screen.

Table 10 Wireless > General: More Secure: WPA(2)

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2) data encryption.
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Device. The key must be the same on the external authentication server and your Device. The key is not sent over the network.
more.../hide more	Click **more...** to show more fields in this section. Click **hide more** to hide them.
ReAuthentication Timer	Enter how often the external authentication server requires a connected wireless client to reauthenticate itself to the server again.
Network Re-auth Interval	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. This field is available only when you select **WPA2** as security mode. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
WPA Compatible	This field is only available for WPA2. Select this if you want the Device to support WPA and WPA2 simultaneously.

Table 10 Wireless > General: More Secure: WPA(2) (continued)

LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients.
Encryption	Select the encryption type for data encryption. If you choose **WPA** as the security mode, the Device uses **TKIP** for data encryption. If you choose **WPA2** as the security mode and enable WPA-PSK Compatible, the Device uses either TKIP and AES (**TKIPAES MIX**) for data encryption. If you choose **WPA2** as the security mode but disable WPA-PSK Compatible, the Device uses **AES** for data encryption.

5.3 The More AP Screen

This screen allows you to enable and configure multiple Basic Service Sets (BSSs) on the Device.

Click **Network Setting > Wireless** > **More AP**. The following screen displays.

Figure 24 Network Seting > Wireless > More AP

The following table describes the labels in this screen.

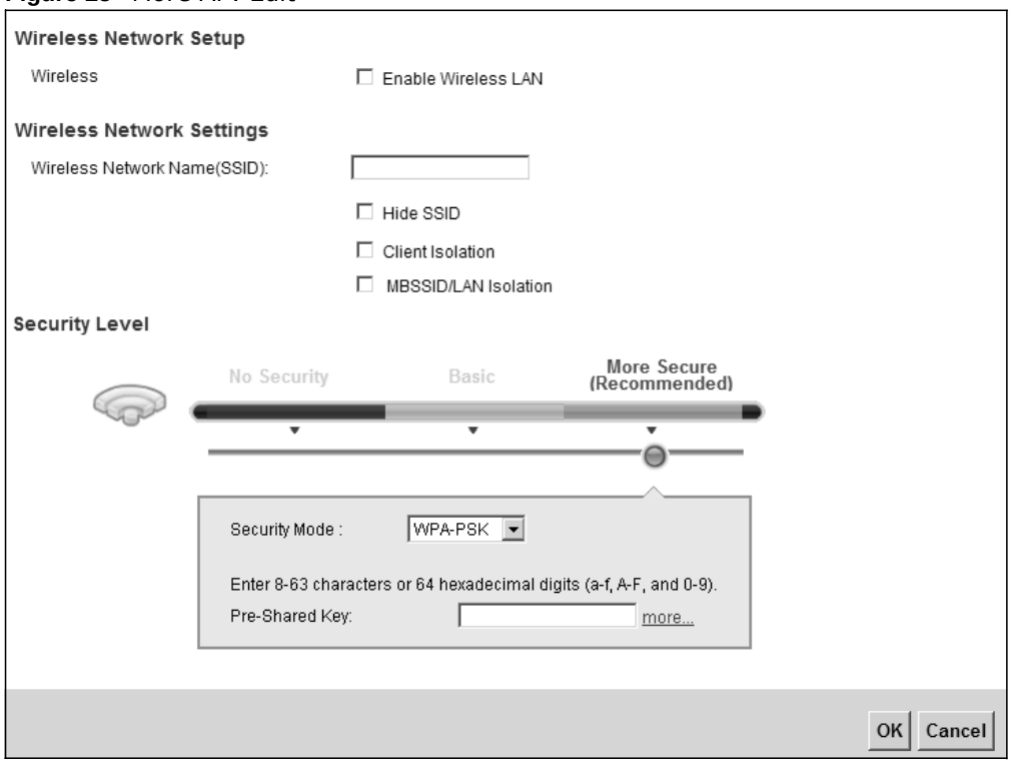
Table 11 Network Setting > Wireless > More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Active	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active. A gray bulb signifies that this SSID is not active.
SSID	An SSID profile is the set of parameters relating to one of the Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the **Edit** icon to configure the SSID profile.

5.3.1 More AP Edit

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 25 More AP: Edit



The following table describes the fields in this screen.

Table 12 More AP: Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select **Enable Wireless LAN** to activate wireless LAN.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Client Isolation	Select this to keep the wireless clients in this SSID from communicating with each other through the Device.
MBSSID/LAN Isolation	Select this to keep the wireless clients in this SSID from communicating with clients in other SSIDs or wired LAN devices through the Device. Select both **Client Isolation** and **MBSSID/LAN Isolation** to allow this SSID's wireless clients to only connect to the Internet through the Device.
Security Level	
Security Mode	Select **Basic (WEP)** or **More Secure (WPA(2)-PSK, WPA(2))** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication.

Table 12 More AP: Edit

LABEL	DESCRIPTION
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

5.4 The MAC Authentication Screen

This screen allows you to configure the Device to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the Device **(Deny)**. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Use this screen to view your Device's MAC filter settings and add new MAC filter rules. Click **Network Setting** > **Wireless > MAC Authentication**. The screen appears as shown.

Figure 26 Network Setting > Wireless > MAC Authentication

The following table describes the labels in this screen.

Table 13 Network Setting > Wireless > MAC Authentication

LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disable** to turn off MAC filtering. Select **Allow** to permit access to the Device. MAC addresses not listed will be denied access to the Device. Select **Deny** to block access to the Device. MAC addresses not listed will be allowed to access the Device.
MAC address List	
Add new MAC address	Click this if you want to add a new MAC address entry to the MAC filter list below. Enter the MAC addresses of the wireless devices that are allowed or denied access to the Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the Device.

Table 13 Network Setting > Wireless > MAC Authentication (continued)

LABEL	DESCRIPTION
Modify	Click the **Delete** icon to delete the entry.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

5.5 The WPS Screen

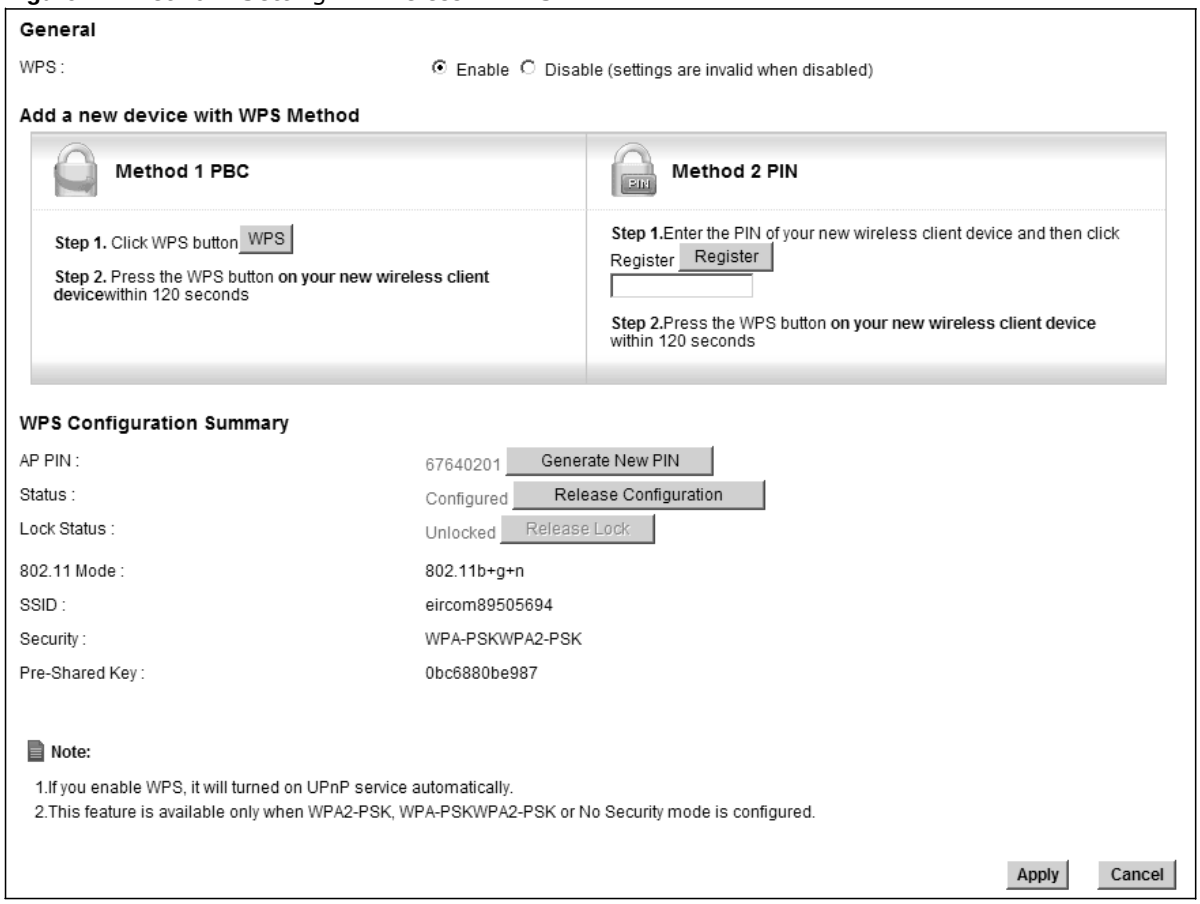
Use this screen to configure WiFi Protected Setup (WPS) on your Device.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See Section 5.10.8.3 on page 71 for more information about WPS.

Note: The Device applies the security settings configured in the General screen (see Section 5.2 on page 48). If you want to use the WPS feature, make sure you have set the security mode to **WPA-PSK**, **WPA2-PSK** or **No Security**.

Click **Network Setting > Wireless > WPS**. The following screen displays. Select **Enable** and click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 27 Network Setting > Wireless > WPS



The following table describes the labels in this screen.

Table 14 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
WPS	Select **Enable** to activate WPS on the Device. Otherwise, select **Disable** to deactivate WPS.
Add a new device with WPS Method	
Method 1 PBC	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).
WPS	Click this button to add another WPS-enabled wireless device (within wireless range of the Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **WPS button** on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2 PIN	Use this section to set up a WPS wireless network by entering the PIN of the client into the Device.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Device.
WPS Configuration Summary	
AP PIN	The PIN (Personal Identification Number) of the Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method. Click the **Generate New PIN** button to have the Device create a new PIN.
Status	This displays **Configured** when the Device has connected to a wireless network using WPS or **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there is no wireless or wireless security changes on the Device or you click **Release Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	The default WPS status is **Configured.** Click this button to remove all configured wireless and wireless security settings for WPS connections on the Device.
802.11 Mode	This field displays the Device's wireless mode that only allows the compliant WLAN devices to associate with it.
SSID	This field displays the SSID the Device is currently using.
Security	This field displays the security mode the Device is currently using.
Pre-Shared Key	This field displays the pre-shared key the Device uses when the security mode is set to WPA(2)-PSK.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

5.6 The WDS Screen

An AP using the Wireless Distribution System (WDS) can function as a wireless network bridge allowing you to wirelessly connect wired network segments. The **WDS** screen allows you to configure the Device to connect to other APs wirelessly when WDS is enabled.

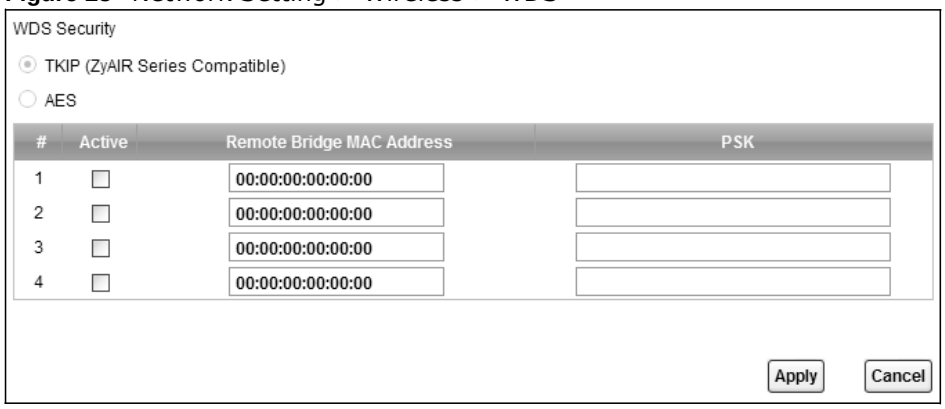
Use this screen to set up your WDS (Wireless Distribution System) links between the Device and other wireless APs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between devices is made.

Note: WDS security is independent of the security settings between the Device and any wireless clients.

Note: Not all APs support WDS links. Check your other AP's documentation.

Click **Network Setting > Wireless > WDS**. The following screen displays.

Figure 28 Network Setting > Wireless > WDS



The following table describes the labels in this screen.

Table 15 Network Setting > Wireless > WDS

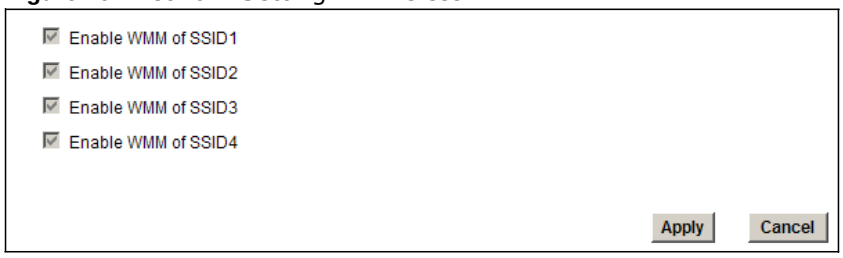
LABEL	DESCRIPTION
WDS Security	Select the type of the key used to encrypt data between APs. All the wireless APs (including the Device) must use the same pre-shared key for data transmission. The option is available only when you set the security mode to **WPA(2)** or **WPA(2)-PSK** in the **Wireless > General** screen.
TKIP	Select this to use TKIP (Temporal Key Integrity Protocol) encryption.
AES	Select this to use AES (Advanced Encryption Standard) encryption.
#	This is the index number of the individual WDS link.
Active	Select this to activate the link between the Device and the peer device to which this entry refers. When you do not select the check box this link is down.
Remote Bridge MAC Address	Type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc).
PSK	Enter a Pre-Shared Key (PSK) from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

5.7 The WMM Screen

Currently, the Wi-Fi MultiMedia (WMM) feauture of SSID1-4 is enabled and this screen is read-only.

Click **Network Setting** > **Wireless > WMM**. The following screen displays.

Figure 29 Network Setting > Wireless > WMM



The following table describes the labels in this screen.

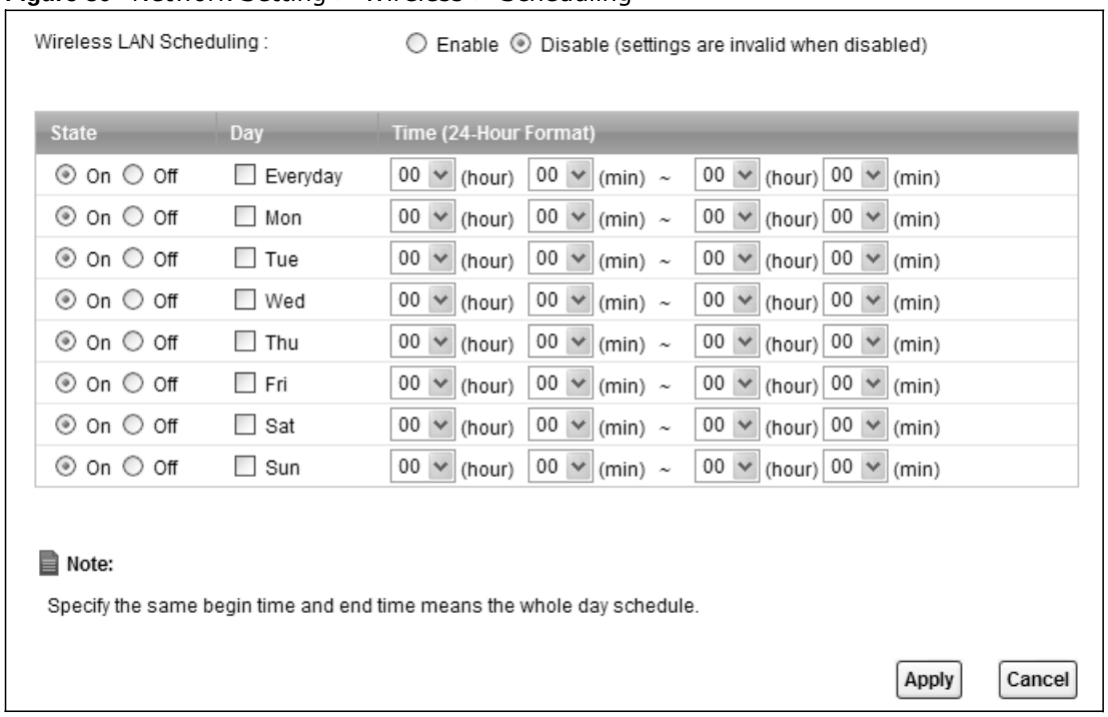
Table 16 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
Enable WMM of SSID1~4	Determine whether to have the Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends for a wireless network. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

5.8 The Scheduling Screen

Use the wireless LAN scheduling to configure the days you want to enable or disable the wireless LAN. Click **Network Setting > Wireless > Scheduling**. The following screen displays.

Figure 30 Network Setting > Wireless > Scheduling



The following table describes the labels in this screen.

Table 17 Network Setting > Wireless > Scheduling

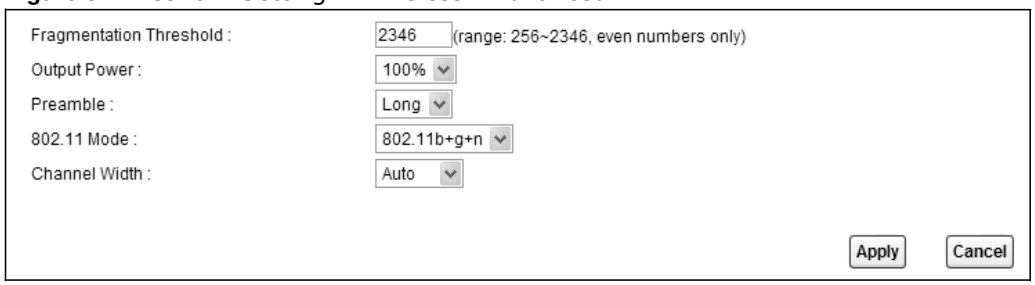
LABEL	DESCRIPTION
Wireless LAN Scheduling	Select **Enable** or **Disable** to activate or deactivate wireless LAN scheduling on your Device.
State	Select **On** or **Off** to enable or disable the wireless LAN.
Day	Check the day(s) you want to turn the wireless LAN on or off.
Time (24-Hour Format)	Specify a time frame during which the schedule would apply. For example, if you set the time range from 12:00 to 23:00, the wireless LAN will be turned on only during this time period.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

5.9 The Advanced Screen

Use this screen to configure advanced wireless settings. Click **Network Setting** > **Wireless** > **Advanced**, the screen appears as shown.

See Section 5.10.2 on page 64 for detailed definitions of the terms listed in this screen.

Figure 31 Network Setting > Wireless> Advanced



The following table describes the labels in this screen.

Table 18 Network Setting > Wireless> Advanced

LABEL	DESCRIPTION
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	Set the output power of the Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: **100%**, **75%, 50%** or **25%**.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long** or **Short**.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Device. Select **802.11b+g** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Device. The transmission rate of your Device might be reduced. Select **802.11n** to allow only IEEE 802.11n compliant WLAN devices to associate with the Device. Select **802.11g+n** to allow either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the Device. The transmission rate of your Device might be reduced. Select **802.11b+g+n** to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the Device. The transmission rate of your Device might be reduced.
Channel Width	Select whether the Device uses a wireless channel width of **20MHz** or **Auto**. If **Auto** is selected, the Device will use 40MHz if it is supported. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. This field is available only when you set the **802.11 Mode** to **802.11n** or **802.11b+g+n** in the **Advanced Setup** screen.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

5.10 Wireless LAN Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

5.10.1 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

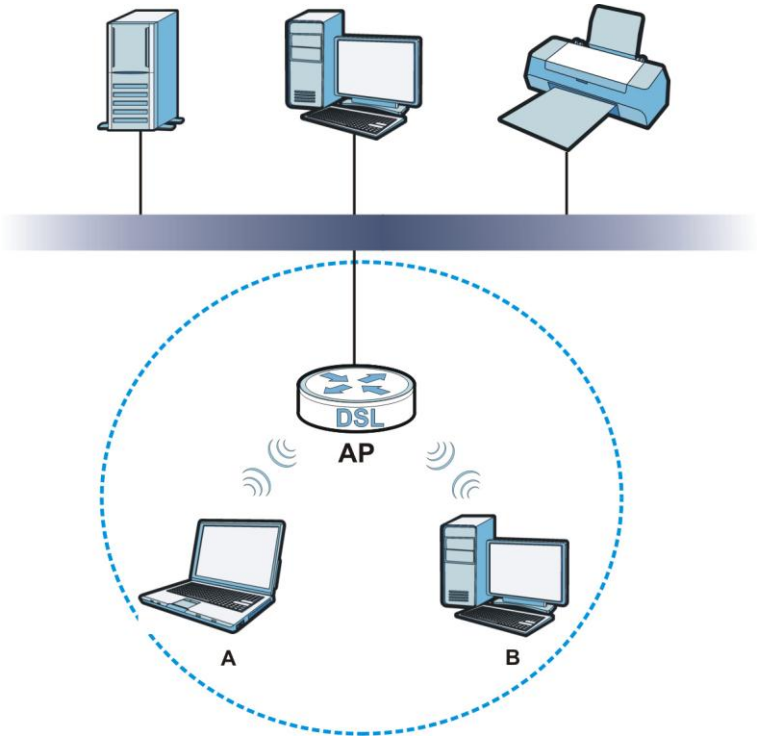
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 32 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

5.10.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the Device's Web Configurator.

Table 19 Additional Wireless Terms

TERM	DESCRIPTION
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the Device does, it cannot communicate with the Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

5.10.3 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only

people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

5.10.3.1 SSID

Normally, the Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

5.10.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

5.10.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

5.10.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 5.10.3.3 on page 66 for information about this.)

Table 20 Types of Encryption for Each Type of Authentication

	No Authentication	**RADIUS Server**
Weakest	No Security	WPA
	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA-PSK. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

5.10.4 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

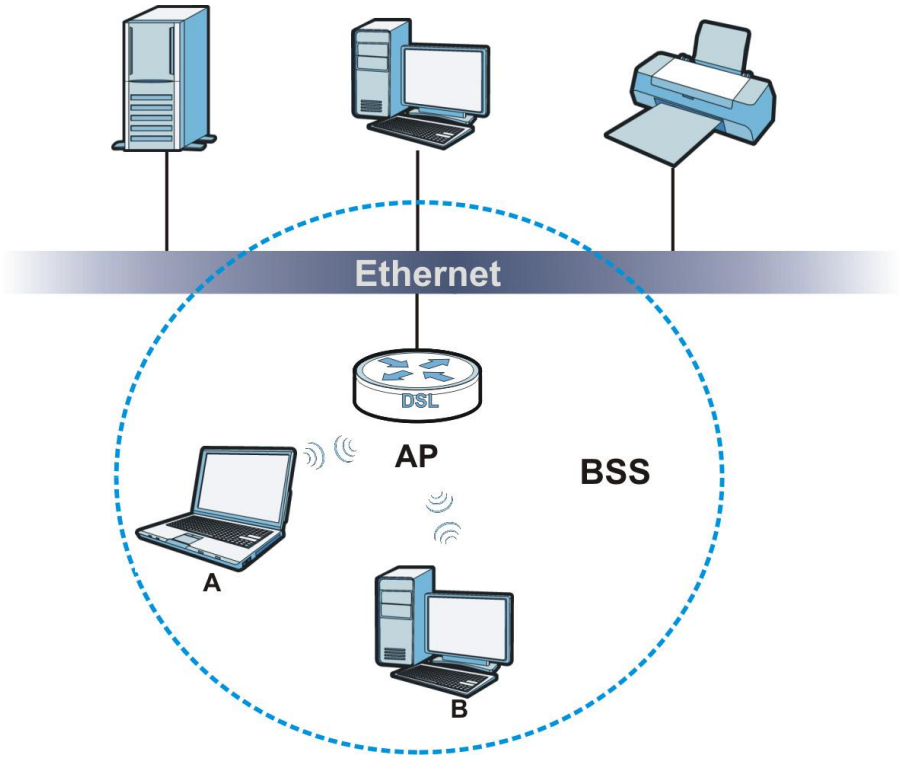
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

5.10.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 33 Basic Service set



5.10.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The Device's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

5.10.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

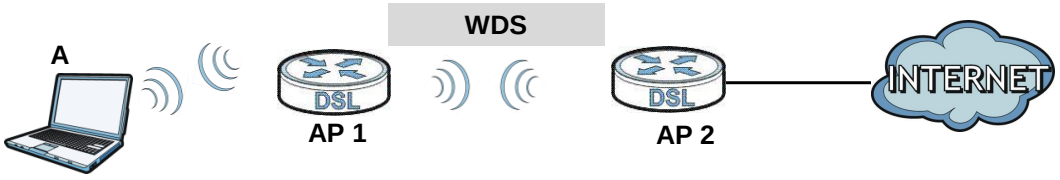
5.10.7 Wireless Distribution System (WDS)

The Device can act as a wireless network bridge and establish WDS (Wireless Distribution System) links with other APs. You need to know the MAC addresses of the APs you want to link to. Once the security settings of peer sides match one another, the connection between devices is made.

At the time of writing, WDS security is not compatible with all access points. Refer to your other access point's documentation for details.

The following figure illustrates how WDS link works between APs. Notebook computer **A** is a wireless client connecting to access point **AP 1**. **AP 1** has no wired Internet connection, but it can establish a WDS link with access point **AP 2**, which has a wired Internet connection. When **AP 1** has a WDS link with **AP 2**, the notebook computer can access the Internet through **AP 2**.

Figure 34 WDS Link Example



5.10.8 WiFi Protected Setup (WPS)

Your Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two

minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

5.10.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the Device, see Section 5.6 on page 59).
3. Press the button on one of the devices (it doesn't matter which). For the Device you must press the WPS button for more than three seconds.
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

   If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

5.10.8.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1. Ensure WPS is enabled on both devices.
2. Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.

3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the Device, see Section 5.5 on page 57).

4 Enter the client's PIN in the AP's configuration interface.

5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

6 Start WPS on both devices within two minutes.

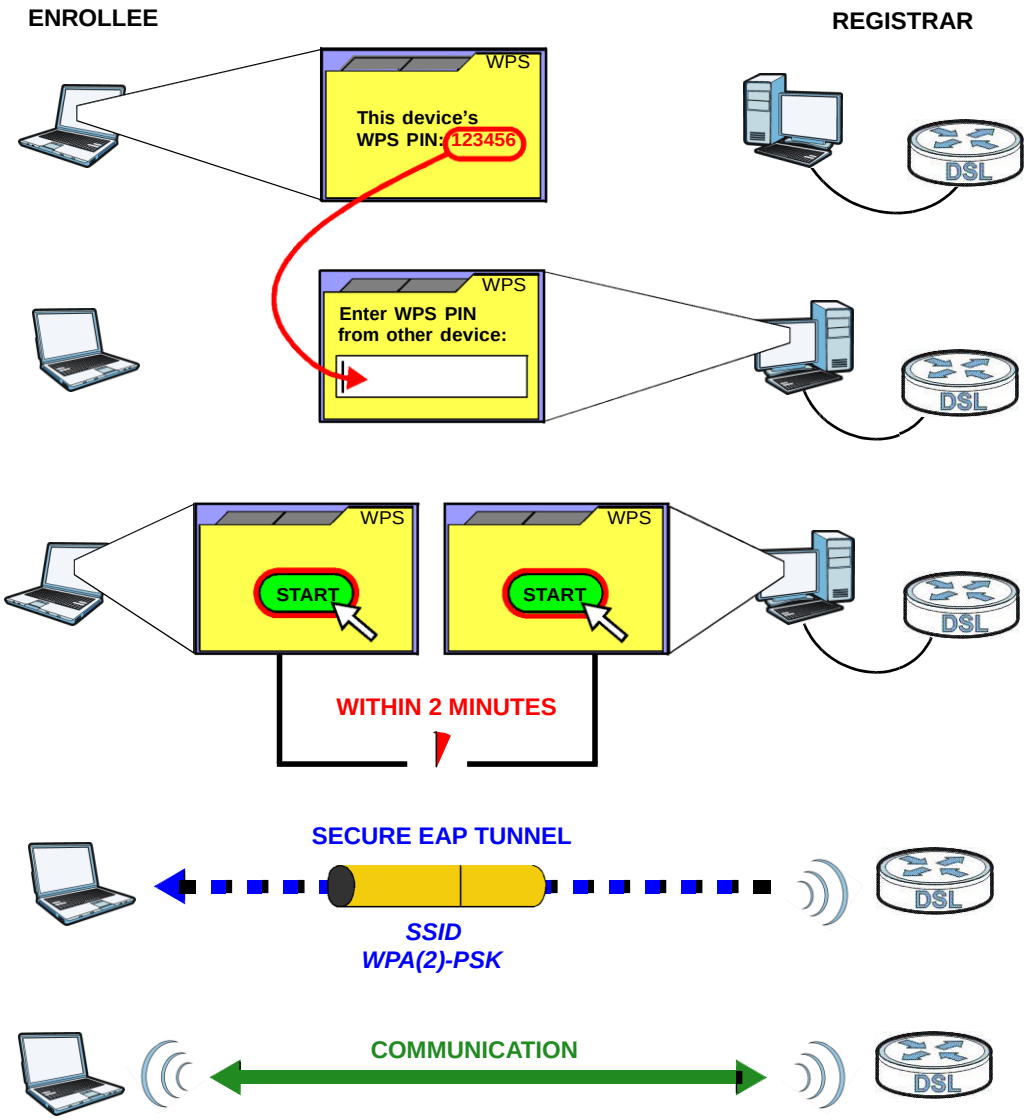
7 Use the configuration utility to activate WPS, not the push-button on the device itself.

8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

   If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

   The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 35 Example WPS Process: PIN Method

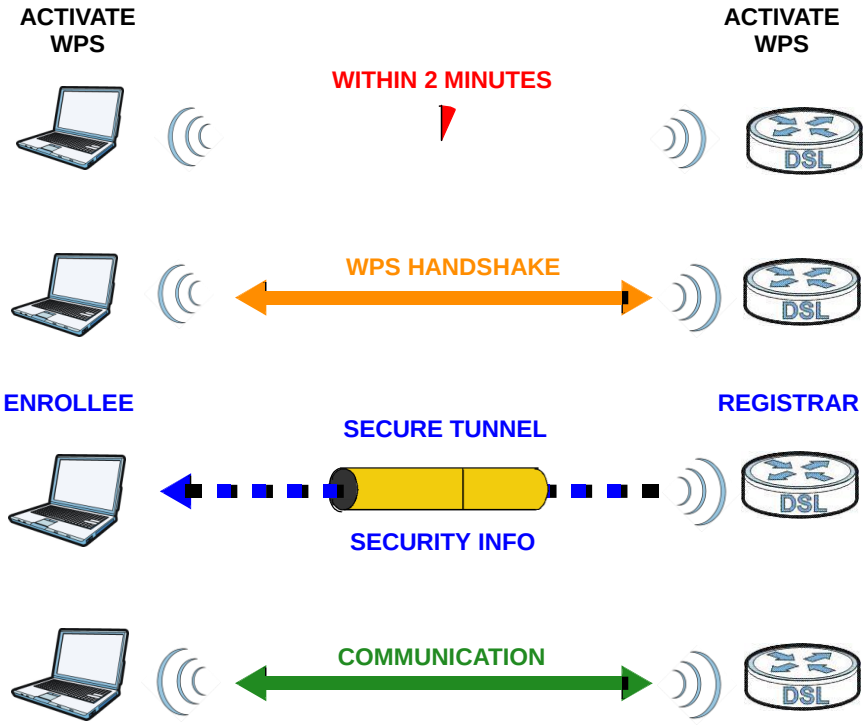


5.10.8.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 36 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

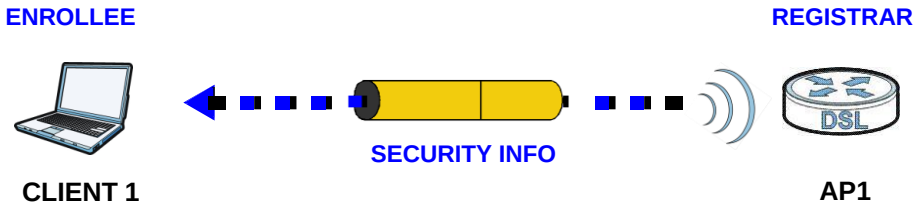
By default, a WPS devices is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

5.10.8.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

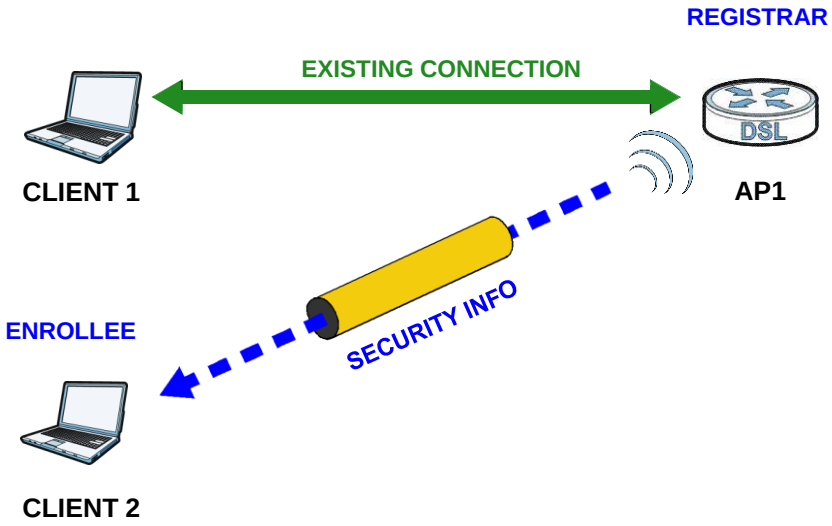
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 37 WPS: Example Network Step 1



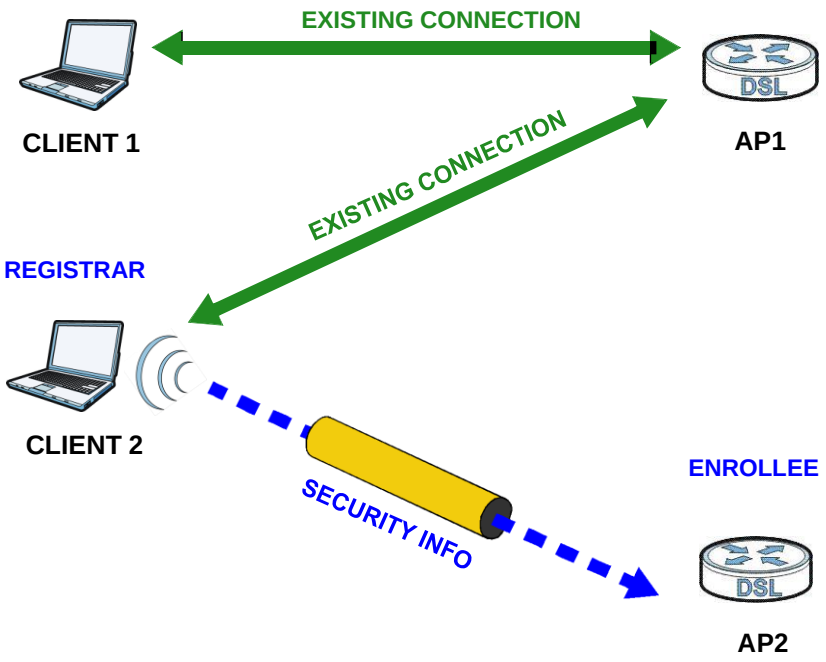
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 38 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 39 WPS: Example Network Step 3



5.10.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).
- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the

access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

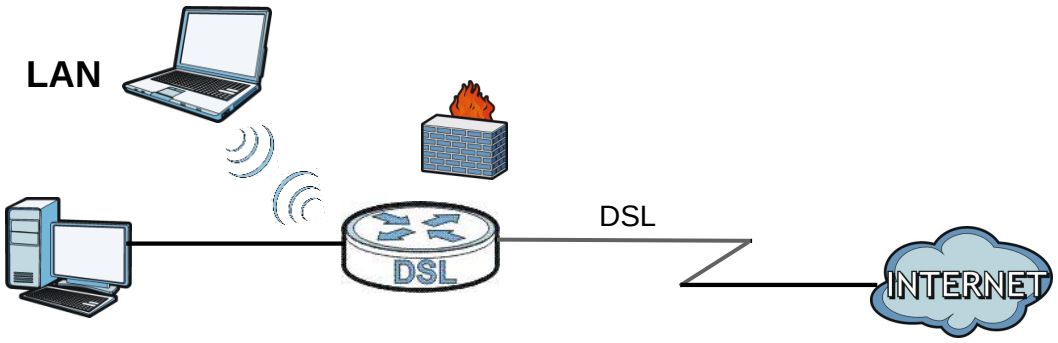
6

Home Networking

6.1 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.



6.1.1 What You Can Do in the LAN Screens

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your Device (Section 6.2 on page 79).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 6.3 on page 81).
- Use the **IP Alias** screen (Section 6.6 on page 84) to change your Device's IP alias settings.
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the Device (Section 6.5 on page 83).
- Use the **IPv6 LAN Setup** screen (Section 6.6 on page 84) to configure the IPv6 settings on your Device's LAN interface.
- Use the **File Sharing** screen (Section 6.7 on page 88) to set up file sharing via the Device.
- Use the **Print Server** screen (Section 6.8 on page 91) to enable the print server function on the Device.

6.1.2 What You Need To Know

6.1.2.1 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 Device an IP address, subnet mask, DNS and other routing information when it's turned on.

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.

6.1.2.2 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.

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 Device 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.

Finding Out More

See Section 6.11 on page 103 for technical background information on LANs.

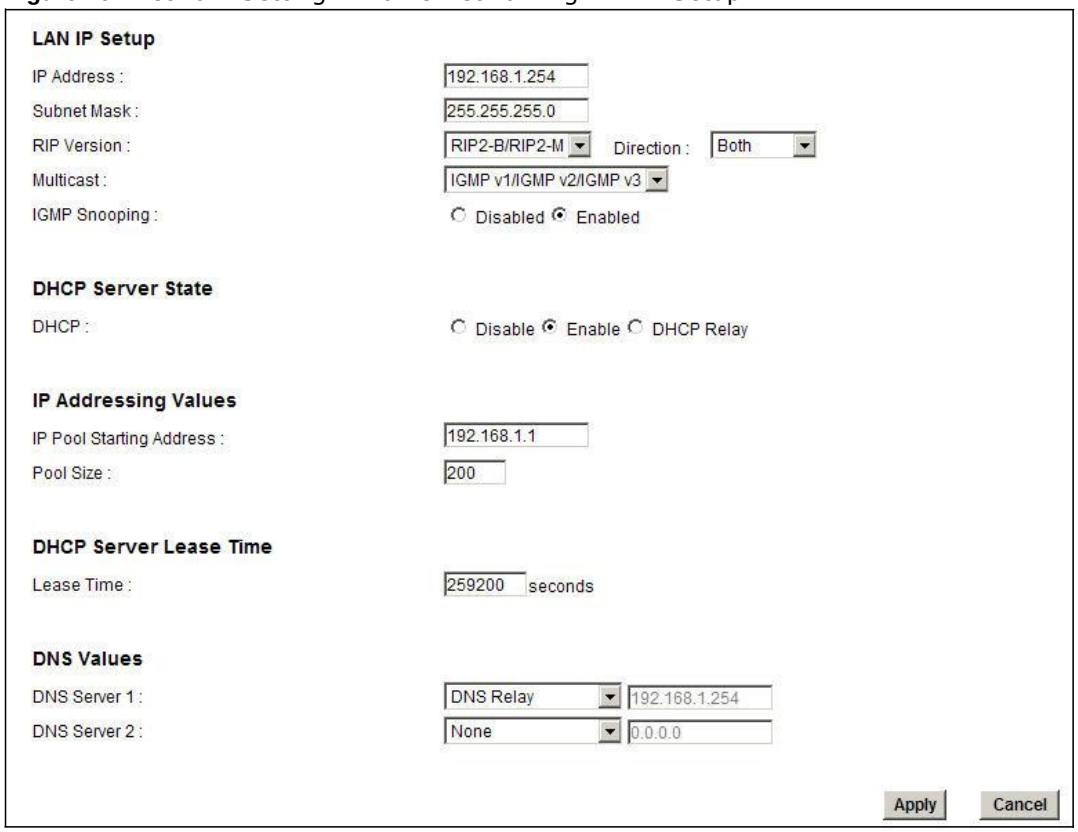
6.1.3 Before You Begin

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

6.2 The LAN Setup Screen

Use this screen to set the Local Area Network IP address, subnet mask and advanced networking settings such as RIP, multicast of your Device. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

Figure 40 Network Setting > Home Networking > LAN Setup



The following table describes the fields in this screen.

Table 21 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your Device in dotted decimal notation, for example, 192.168.1.254 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Device 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.
RIP Version	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Select the RIP version from **RIP1** and **RIP2-B/RIP2-M**.
Direction	Use this field to control how much routing information the VDSL Router sends and receives on the subnet. Select the **RIP Direction** from **None**, **Both**, **IN Only** and **OUT Only**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The Device supports **IGMP v1/IGMP v2/IGMP v3**. Select **None** to disable it.
IGMP Snooping	Select **Enabled** to activate IGMP Snooping. This allows the Device to passively learn memberships in multicast groups. Otherwise, select **Disabled** to deactivate it.
DHCP Server State	

Table 21 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DHCP	If set to **Enable**, your Device 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 **Disable**, the DHCP server will be disabled. If set to **DHCP Relay**, the Device 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 Addressing Values	
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.
DHCP Server Lease Time	
Lease Time	This field specifies the lease time in seconds of an IP address assigned by the DHCP server.
DNS Values	
DNS Server 1 DNS Server 2	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the Device'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 Device act as a DNS proxy only when the ISP uses IPCP DNS server extensions. The Device's LAN IP address displays in the field to the right (read-only). The Device tells the DHCP clients on the LAN that the Device itself is the DNS server. When a computer on the LAN sends a DNS query to the Device, the Device 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 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.

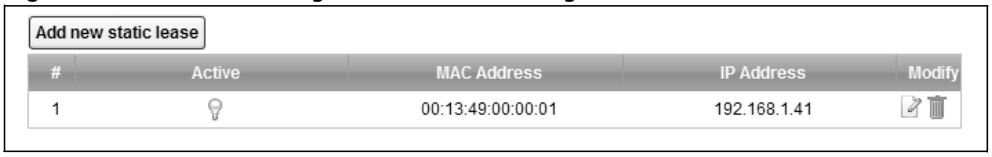
6.3 The Static DHCP Screen

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 Device's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Figure 41 Network Setting > Home Networking > Static DHCP



The following table describes the labels in this screen.

Table 22 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Add new static lease	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Active	This field displays whether the client is connected to the Device.
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.
IP Address	This field displays the IP address relative to the # field listed above.
Modify	Click the **Edit** icon to have the IP address field editable and change it. Click the **Delete** icon to delete a static DHCP entry. A window displays asking you to confirm that you want to delete the selected entry.

If you click **Add new static lease** in the **Static DHCP** screen or the **Edit** icon next to a static DHCP entry, the following screen displays.

Figure 42 Static DHCP: Add/Edit

The following table describes the labels in this screen.

Table 23 Static DHCP: Add/Edit

LABEL	DESCRIPTION
MAC Address	If you select **Manual Input** in the **Select Device Info** field, enter the MAC address of a computer on your LAN.
IP Address	If you select **Manual Input** in the **Select Device Info** field, enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

6.4 The IP Alias Screen

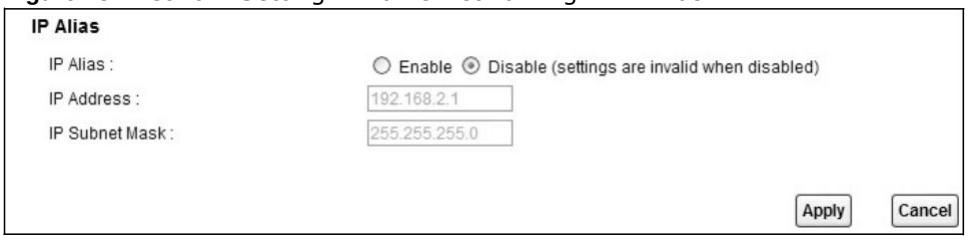
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Device supports multiple logical LAN interfaces via its physical Ethernet interface with the Device itself as the gateway for the LAN network.

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

6.4.1 Configuring the LAN IP Alias Screen

Use this screen to change your Device's IP alias settings. Click **Network Setting** > **Home Networking** > **IP Alias** to open the following screen.

Figure 43 Network Setting > Home Networking > IP Alias



The following table describes the labels in this screen.

Table 24 Network Setting > Home Networking > IP Alias

LABEL	DESCRIPTION
IP Alias	Select **Enable** to configure a LAN network for the Device.
IP Address	Enter the IP address of your Device in dotted decimal notation.
IP Subnet Mask	Your Device 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 Device.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

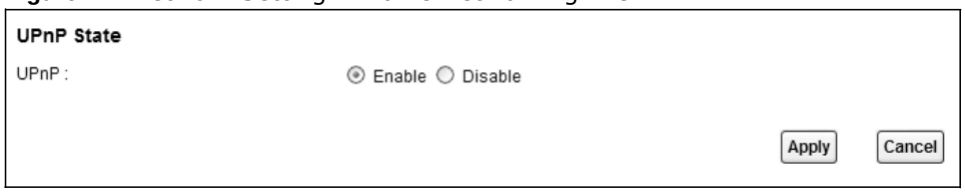
6.5 The UPnP Screen

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.

See page 78 for more information on UPnP.

Use the following screen to enable or disable the UPnP function on your Device. Click **Network Setting > Home Networking > UPnP** to display the screen shown next.

Figure 44 Network Setting > Home Networking > UPnP



The following table describes the labels in this screen.

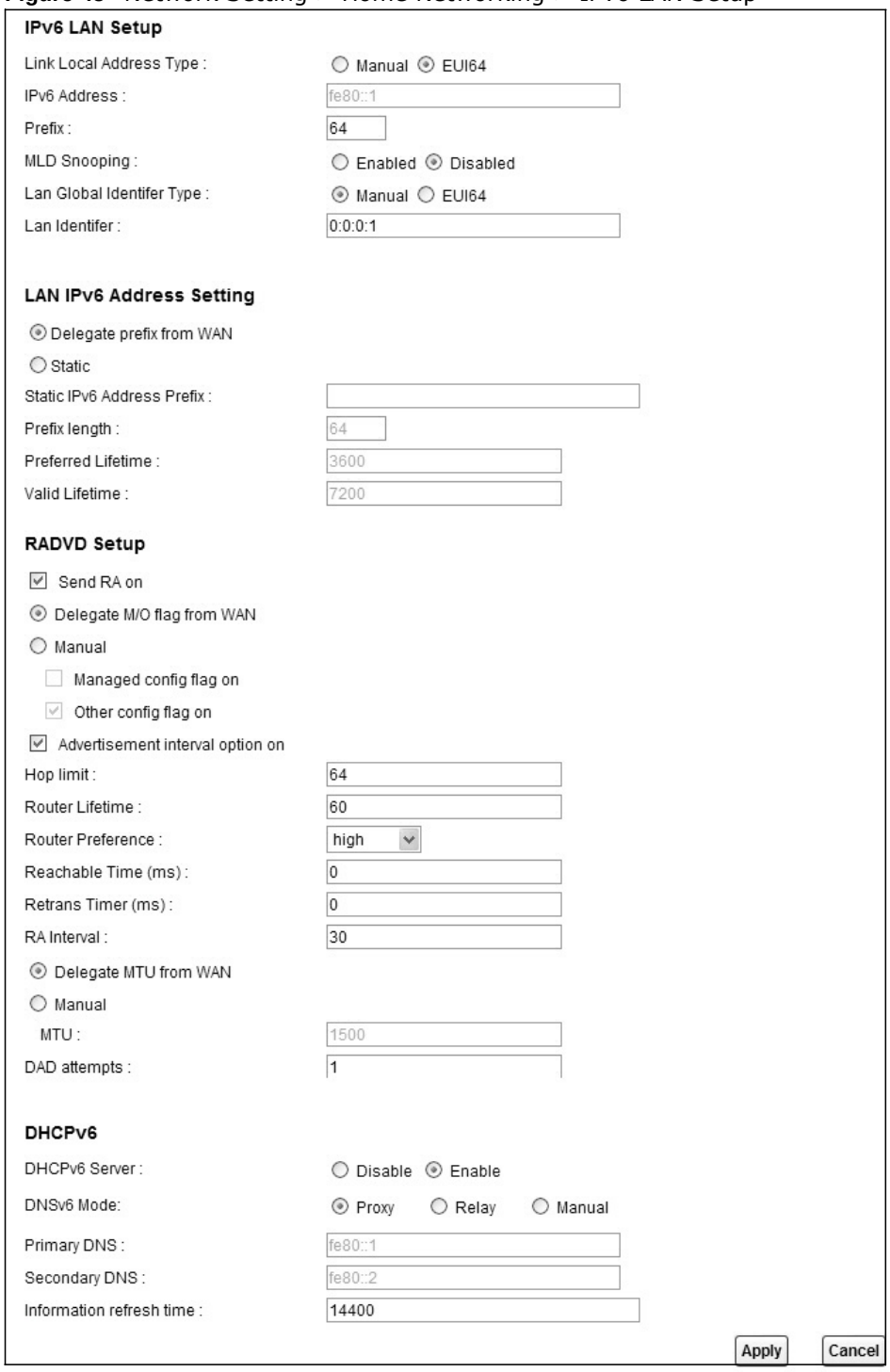
Table 25 Network Setting > Home Networking > UPnP

LABEL	DESCRIPTION
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Device's IP address (although you must still enter the password to access the web configurator). Otherwise, select **Disable** to deactivate UPnP.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

6.6 The IPv6 LAN Setup Screen

Use this screen to configure the IPv6 settings for your Device’s LAN interface.

Figure 45 Network Setting > Home Networking > IPv6 LAN Setup



The following table describes the labels in this screen.

Table 26 Network Setting > Home Networking > IPv6 LAN Setup

LABEL	DESCRIPTION
IPv6 LAN Setup	
Link Local Address Type	Select **Manual** to manually enter a link local address. Select **EUI64** to use the EUI-64 format to generate a link local address from the Ethernet MAC address.
IPv6 Address	If you selected **Manual** in the **Link Local Address Type** field, enter the LAN IPv6 address you want to assign to your Device in hexadecimal notation, for example, fe80::1 (factory default).
Prefix	Enter the address prefix to specify how many most significant bits in an IPv6 address compose the network address.
MLD Snooping	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network. Select **Enabled** to activate MLD Snooping on the Device. This allows the Device to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.
Lan Global Identifier Type	Select **Manual** to manually enter a LAN Identifier as the interface ID to identify the LAN interface. The LAN Identifier is appended to the IPv6 address prefix to create the routable global IPv6 address. Select **EUI64** to use the EUI-64 format to generate an interface ID from the Ethernet MAC address.
Lan Identifier	If you selected **Manual**, enter the LAN Identifier in this field. The LAN identifier should be unique and 64 bits in hexadecimal form. Every 16 bit block should be separated by a colon as in XXXX:XXXX:XXXX:XXXX where X is a hexadecimal character. Blocks of zeros can be represented with double colons as in XXXX:XXXX::XXXX.
LAN IPv6 Address Setting	
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the Device's LAN IPv6 address.
Static IPv6 Address Prefix	If you select static IPv6 address, enter the IPv6 address prefix that the Device uses for the LAN IPv6 address.
Prefix length	If you select static IPv6 address, enter the IPv6 prefix length that the Device uses to generate the LAN IPv6 address. An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
Preferred Lifetime	Enter the preferred lifetime for the prefix.
Valid Lifetime	Enter the valid lifetime for the prefix.
RADVD Setup	
Send RA on	Select this to have the Device send router advertisement messages to the LAN hosts. Router advertisement is a response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters, such as IPv6 prefix and DNS information. Router solicitation is a request from a host to locate a router that can act as the default router and forward packets. Note: The LAN hosts neither generate global IPv6 addresses nor communicate with other networks if you disable this feature.
Delegate M/O flag from WAN	Select this to have the Device obtain the M/O (Managed/Other) flag setting from the service provider or uplink router.
Manual	Select this to specify the M/O flag setting manually.

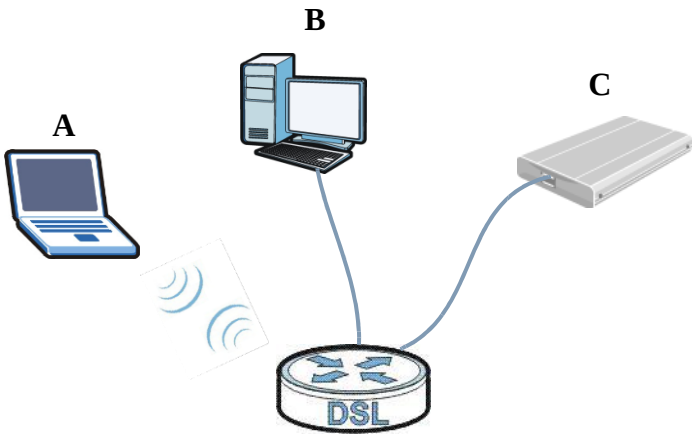
Table 26 Network Setting > Home Networking > IPv6 LAN Setup (continued)

LABEL	DESCRIPTION
Managed config flag on	Select this to have the Device indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the Device indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Other config flag on	Select this to have the Device indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the Device indicate to hosts that DNS information is not available in this network.
Advertisement interval option on	Select this to have the Router Advertisement messages the VDSL Router sends specify the allowed interval between Router Advertisement messages.
Hop limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0. Possible value for this field are 0-255.
Router Lifetime	Enter the time in seconds that hosts should consider the Device to be the default router. Possible values for this field are 0-9000.
Router Preference	Select the router preference (**Low**, **Medium** or **High**) for the Device. The Device sends this preference in the router advertisements to tell hosts what preference they should use for the Device. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network. Note: Make sure the hosts also support router preference to make this function work.
Reachable Time (ms)	Enter the time in milliseconds that can elapse before a neighbor is detected. Possible values for this field are 0-3600000.
Retrans Timer (ms)	Enter the time in milliseconds between neighbor solicitation packet retransmissions. Possible values for this field are 1000-4294967295.
RA Interval	Enter the time in seconds between router advertisement messages. Possible values for this field are 4-1800.
Delegate MTU from WAN	Select this to have the Device obtain the MTU setting from the service provider or uplink router.
Manual	Select this to specify the MTU manually.
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the Device divides it into smaller fragments.
DAD attempts	Specify the number of DAD (Duplicate Address Detection) attempts before an IPv6 address is assigned to the Device LAN interface. Possible values for this field are 1-7.
DHCPv6	
DHCPv6 Server	Use this field to **Enable** or **Disable** DHCPv6 server on the Device.
DNSv6 Mode	Select the DNS role (**Proxy** or **Relay**) that you want the Device to act in the IPv6 LAN network. Alternatively, select Manual and specify the DNS servers' IPv6 address in the fields below.
Primary DNS	This field is available if you choose **Manual** as the DNSv6 mode. Enter the first DNS server IPv6 address the Device passes to the DHCP clients.
Secondary DNS	This field is available if you choose **Manual** as the DNSv6 mode. Enter the second DNS server IPv6 address the Device passes to the DHCP clients.
Information refresh time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

6.7 The File Sharing Screen

Share files on a USB memory stick or hard drive connected to your Device with users on your network. The following figure is an overview of the Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the Device.

Figure 46 File Sharing Overview



6.7.1 What You Need to Know

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the Device is given a folder, called a "share". If a USB hard drive connected to the Device has more than one partition, then each partition will be allocated a share. You can also configure a "share" to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file-sharing feature on your Device supports File Allocation Table (FAT) and FAT32 file systems.

Windows/CIFS

Common Internet File System (CIFS) is a standard protocol supported by most operating systems in order to share files across the network.

CIFS runs over TCP/IP but uses the SMB (Server Message Block) protocol found in Microsoft Windows for file and printer access; therefore, CIFS will allow all applications, not just Web browsers, to open and share files across the Internet.

The Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

NFS

Network File System (NFS) is a protocol most commonly used on Unix-like systems in order to share files across the network.

Samba

SMB is a client-server protocol used by Microsoft Windows systems for sharing files, printers, and so on.

Samba is a free SMB server that runs on most Unix and Unix-like systems. It provides an implementation of an SMB client and server for use with non-Microsoft operating systems.

File Transfer Protocol

This is a method of transferring data from one computer to another over a network such as the Internet.

6.7.2 Before You Begin

Make sure the Device is connected to your network and turned on.

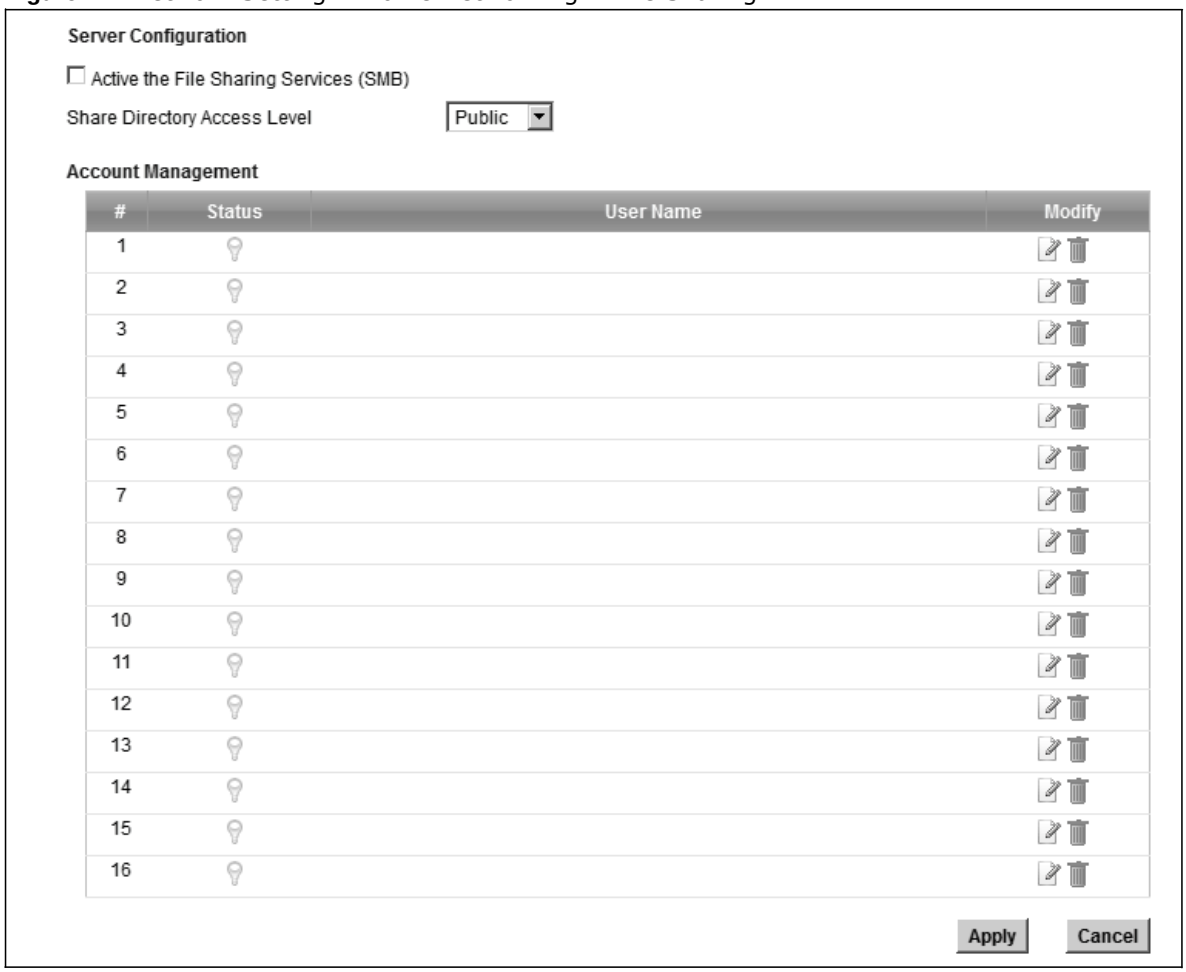
1. Connect the USB device to one of the Device's USB ports. Make sure the Device is connected to your network.
2. The Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the Device, try disconnecting and reconnecting it.

6.7.3 The File Sharing Screen

Use this screen to set up file sharing via the Device. To access this screen, click **Network Setting** > **Home Networking** > **File Sharing**.

Figure 47 Network Setting > Home Networking > File Sharing



Each field is described in the following table.

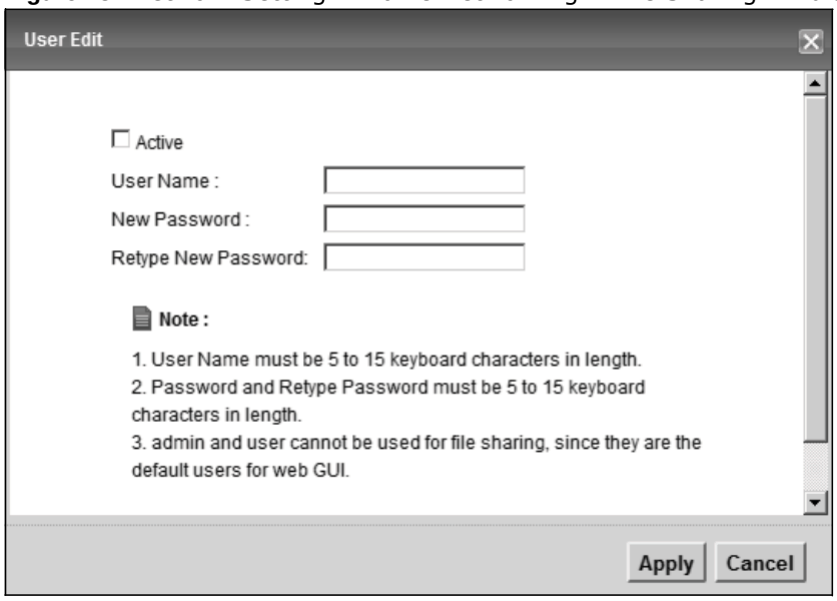
Table 27 Network Setting > Home Networking > File Sharing

LABEL	DESCRIPTION
Server Configuration	
Active the File Sharing Services	Select this to enable file sharing through the Device.
Share Directory Access Level	Select **Public** to allow all users on the network to access the shared files. Select **Security** to require users to log in to access shared files. Set up user accounts in the Account Management section.
Account Management	
Status	This field displays whether a user account is activated or not. Select the check box to enable the account. Clear the check box to disable the account.
User Name	This displays the user name that has been configured on the Device for file sharing.
Edit	Click this to go to the screen for editing user account information.
Delete	Click this to remove a user account from the list.
Apply	Click this to save your changes to the Device.
Cancel	Click this to set every field in this screen to its last-saved value.

6.7.4 User Edit

Click **Edit** in the **File Sharing** screen to edit a user's information on the Device.

Figure 48 Network Setting > Home Networking > File Sharing > Edit



Each field is described in the following table.

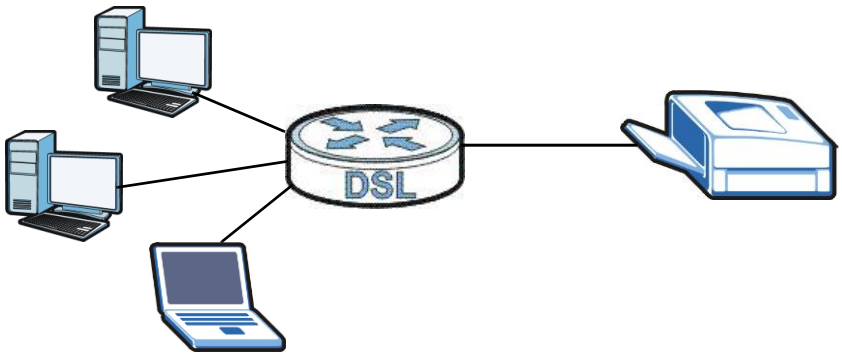
Table 28 Network Setting > Home Networking > File Sharing > Edit

LABEL	DESCRIPTION
Active	Select the check box to enable the account. Clear the check box to disable the account.
User Name	Enter a user name that will be allowed to access shares. You can enter up to 16 characters. Only letters and numbers allowed.
New Password	Enter the password used to access the share. You can enter up to 15 characters. Only letters and numbers are allowed. The password is case sensitive.
Retype New Password	Retype the password that you entered above.
Back	Click this to return to the previous screen.
Apply	Click this to save your changes to the Device.
Cancel	Click this to restore your previously saved settings.

6.8 Print Server

The Device allows you to share a USB printer on your LAN. You can do this by connecting a USB printer to one of the USB ports on the Device and then allowing the computers connected to your network to communicate with the print server (Device) using the Internet Printing Protocol.

Figure 49 Sharing a USB Printer



6.8.1 What You Need to Know

Print Server

This is a computer or other device which manages one or more printers, and which sends print jobs to each printer from the computer itself or other devices.

Operating System

An operating system (OS) is the interface which helps you manage a computer. Common examples are Microsoft Windows, Mac OS or Linux.

Port

A port maps a network service such as http to a process running on your computer, such as a process run by your web browser. When traffic from the Internet is received on your computer, the port number is used to identify which process running on your computer it is intended for.

Internet Printing Protocol

The Internet Printing Protocol (IPP) uses TCP and UDP with port 631. It can run locally or over the Internet on top of HTTP. It allows users to send print jobs to a printer, cancel a previous print job, and know the status of the printer and print jobs.

Supported OSs

The following OSs support Device's printer sharing feature.

- Microsoft Windows 2000, Windows XP, Windows 7, Windows Vista or Macintosh OS X and later versions.

6.8.2 Before You Begin

To configure the print server you need the following:

- Your Device must be connected to your computer and any other devices on your network. The USB printer must be connected to your Device.
- The computers on your network must have the printer software already installed before they can use the printer. Follow your printer manufacturers instructions on how to install the printer software on your computer.

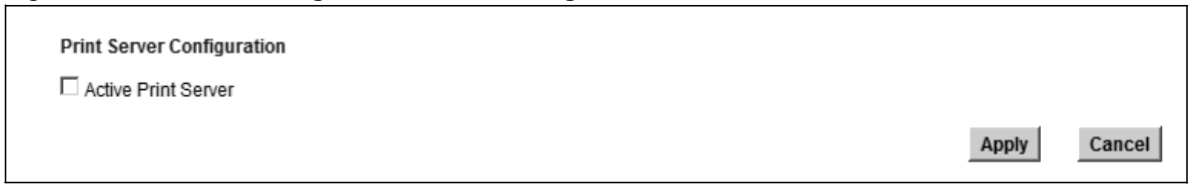
Note: Your printer's installation instructions may ask that you connect the printer to your computer. Connect your printer to the Device instead.

6.8.3 The Print Server Screen

The print server screen is used to enable the print server function on the Device.

Click **Network Setting** > **Home Networking** > **Print Server** to display the **Print Server** screen.

Figure 50 Network Setting > Home Networking > Print Server



The following table describes the labels in this screen.

Table 29 Network Setting > Home Networking > Print Server

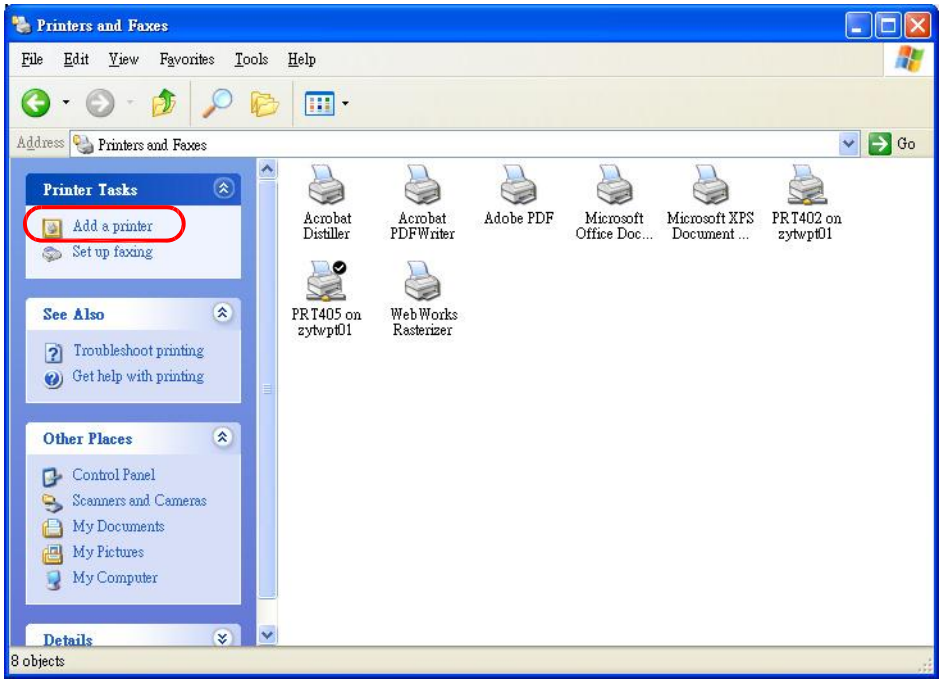
LABEL	DESCRIPTION
Active Print Server	Select this option to have the Device act as a print server.
Apply	Click **Apply** to save your changes back to the Device.
Cancel	Click **Cancel** to return to the previous configuration.

6.9 Add a New Printer Using Windows

This example shows how to connect a printer behind the Device to your computer using the Windows XP Professional operating system. Some menu items may look different on your operating system.

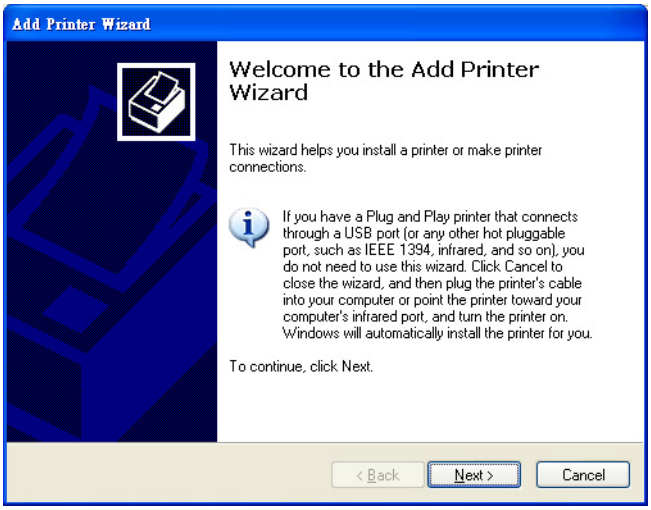
1 Click **Start** > **Control Panel** > **Printers and Faxes** to open the **Printers and Faxes** screen. Click **Add a Printer**.

Figure 51 Printers Folder



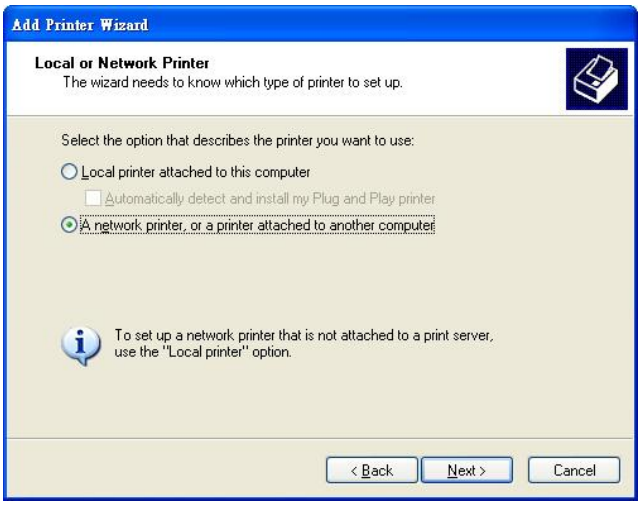
2 The **Add Printer Wizard** screen displays. Click **Next**.

Figure 52 Add Printer Wizard: Welcome



3 Select **A network printer, or a printer attached to another computer** and click **Next**.

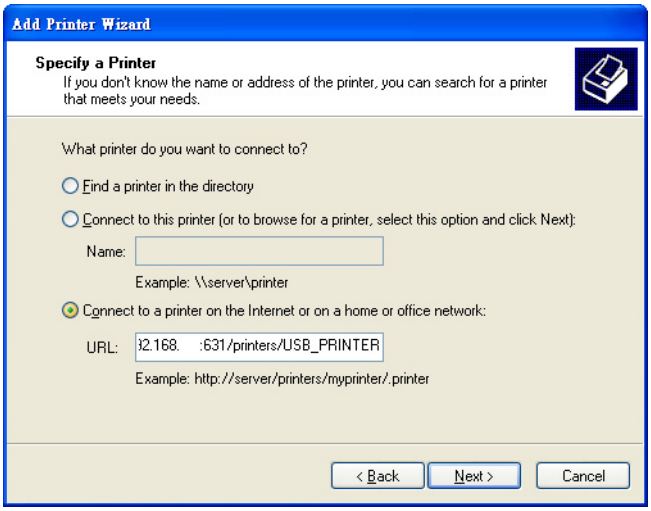
Figure 53 Add Printer Wizard: Local or Network Printer



4 Select **Connect to a printer on the Internet or on a home or office network:** and enter "http://192.168.1.254:631/printers/USB_PRINTER" as the URL to access the print server (Device). Click **Next**.

Note: If you change the Device's LAN IP address, use the new IP address in the URL to access the print server.

Figure 54 Add Printer Wizard: Specify a Printer



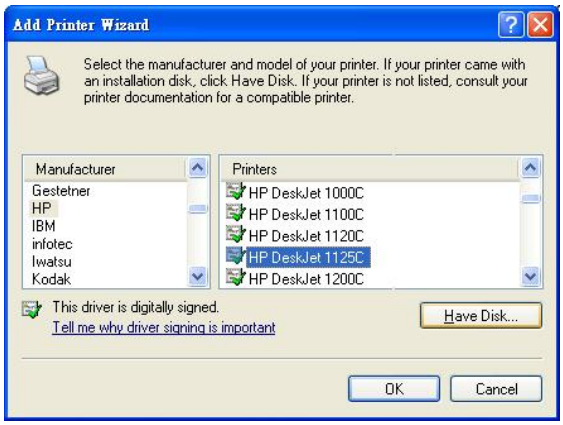
5 Select the make of the printer that you want to connect to the print server in the **Manufacturer** list of printers.

6 Select the printer model from the list of **Printers**.

7 If your printer is not displayed in the list of **Printers**, you can insert the printer driver installation CD/disk or download the driver file to your computer, click **Have Disk...** and install the new printer driver.

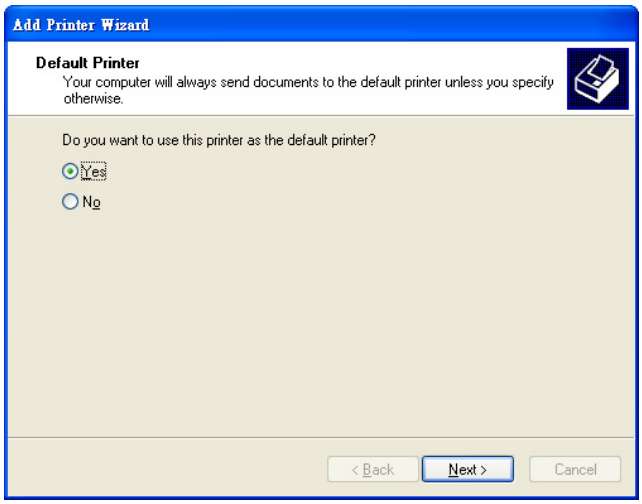
8 Click **Next** to continue.

Figure 55 Add Printer Wizard: Printer Model



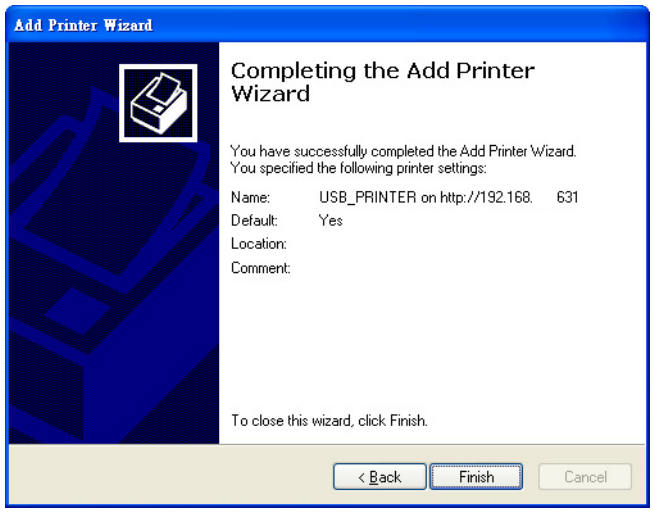
9 Select **Yes** and then click the **Next** button if you want to use this printer as the default printer on your computer. Otherwise select **No** and then click **Next** to continue.

Figure 56 Add Printer Wizard: Default Printer



10 The following screen shows your current printer settings. Select **Finish** to complete adding a new printer.

Figure 57 Add Printer Wizard Complete



6.10 Add a New Printer Using Macintosh OS X

Complete the following steps to set up a print server driver on your Macintosh computer.

6.10.1 Mac OS 10.3 and 10.4

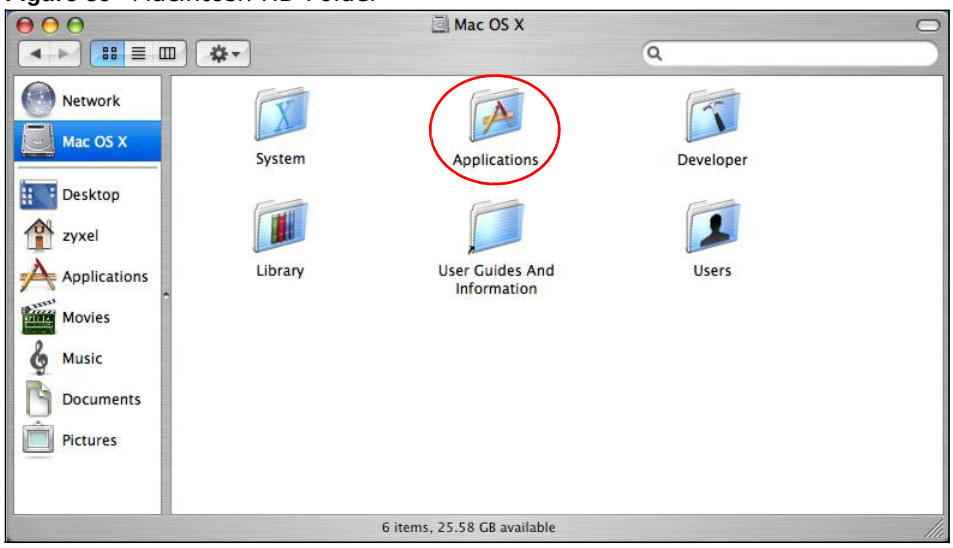
This example shows how to connect a printer behind the Device to your computer using Mac OS X v10.4.11. Some menu items may look different on your operating system.

11 Click the Finder icon on the Dock (a place holding a series of icons/shortcuts at the bottom of the desktop) or double-click your Mac hard disk icon (**Mac OS X** in this example) on your desktop to open the Mac HD window.

Figure 58 Mac OS X HD

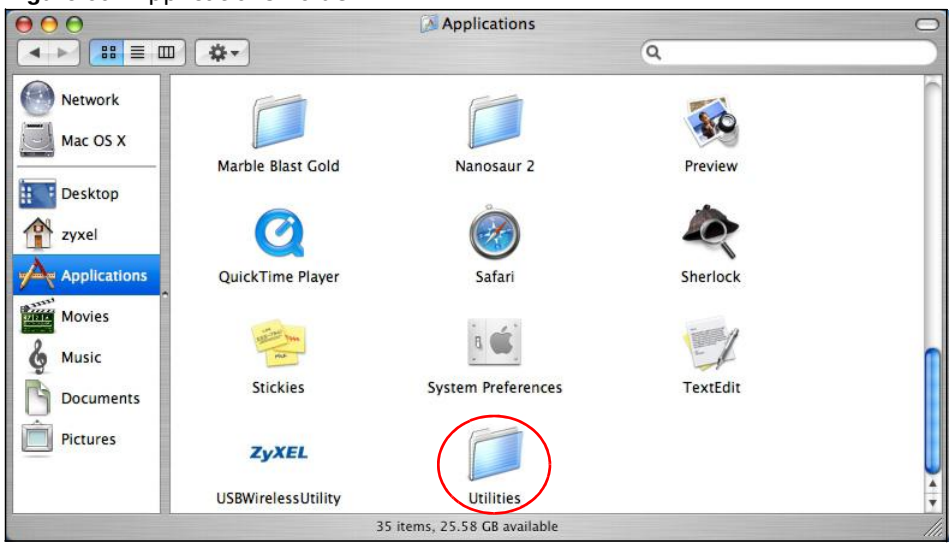
12 Open the **Applications** folder.

Figure 59 Macintosh HD Folder



13 Open the **Utilities** folder.

Figure 60 Applications Folder

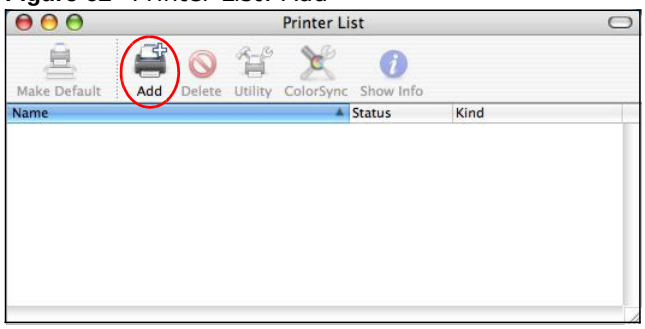


14 Double-click the **Printer Setup Utility** icon.

Figure 61 Utilities Folder

15 Click the **Add** icon at the top of the screen.

Figure 62 Printer List: Add



16 Click the **IP Printer** tab to set up your printer.

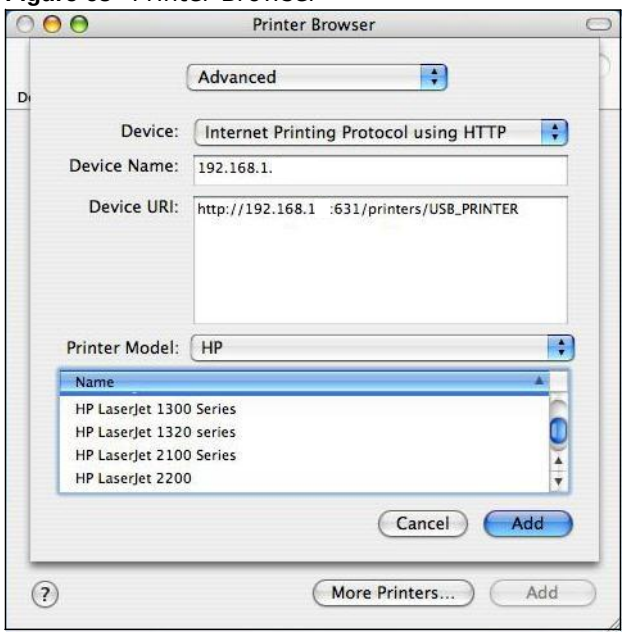
- Press the `alt` key and click **More Printers** in the **Printer Browser** screen.

- Select **Advanced** from the top drop-down list.
- Select **Internet Printing Protocol using HTTP** from the **Device** drop-down list.
- Enter a descriptive name for the printer in the **Device Name** field.
- In the **Device URL** field, enter "http://192.168.1.254:631/printers/USB_PRINTER" as the URL to access the print server (Device).

Note: If you change the Device's LAN IP address, use the new IP address in the URL to access the print server.

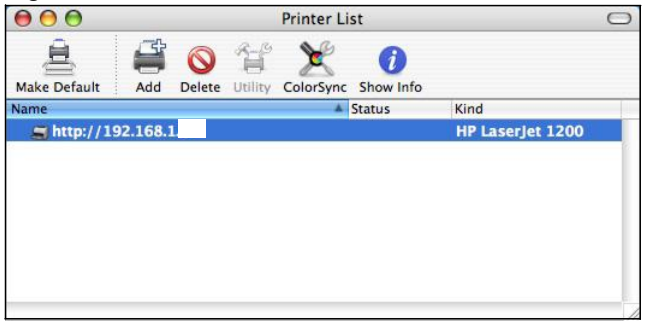
- Select your printer manufacturer from the **Printer Model** drop-down list and then select a printer model. Click **Add** to save and close the **Printer Browser** configuration screen.

Figure 63 Printer Browser



17 The new network printer displays in the **Printer List**. The default printer **Name** displays in bold type.

Figure 64 Printer List



18 Your print server driver setup is complete. You can now use the Device's print server to print from a Mac computer.

6.10.2 Mac OS 10.5 and 10.6

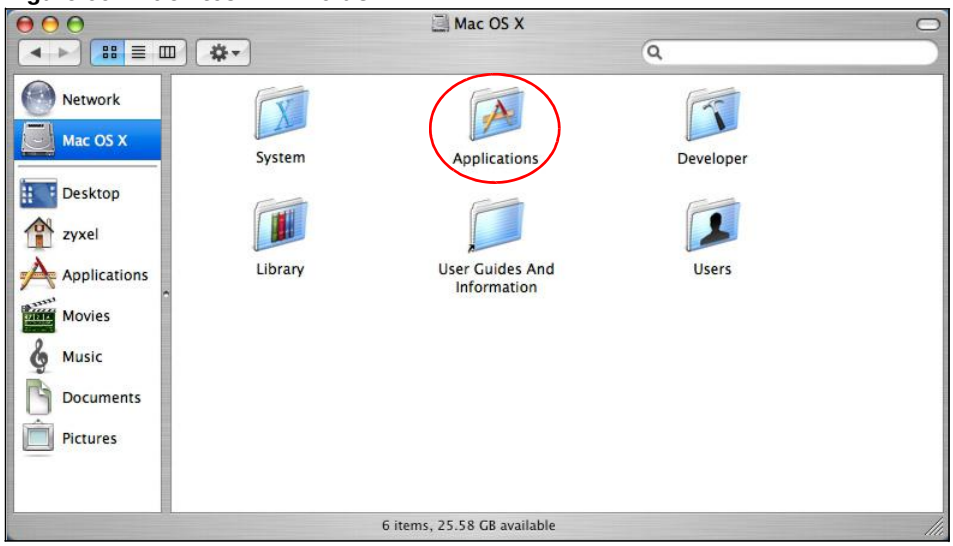
This example shows how to connect a printer behind the Device to your computer using Mac OS X v10.6.2. Some menu items may look different on your operating system.

1 Click the Finder icon on the Dock or double-click your Mac hard disk icon (**Mac OS X** in this example) on your desktop to open the Mac HD window.

Figure 65 Mac OS X HD

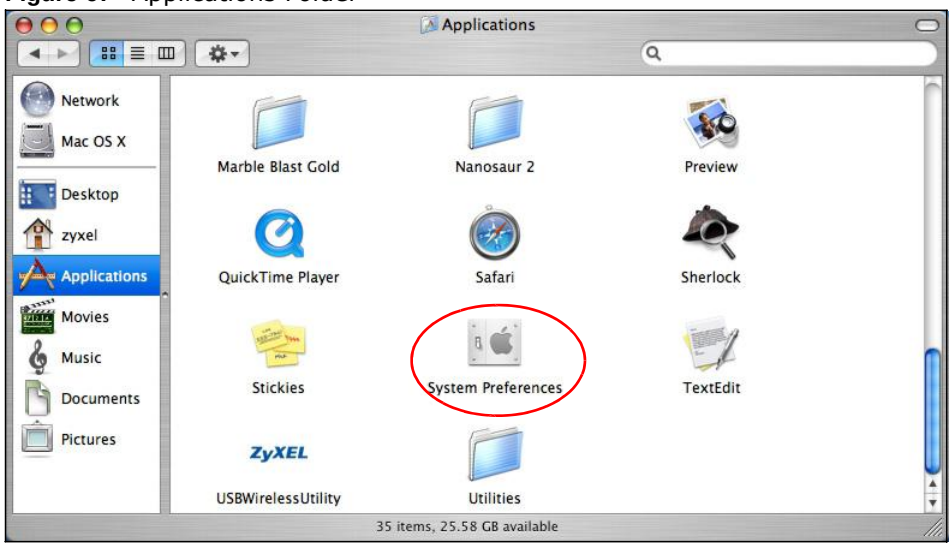
2 Open the **Applications** folder.

Figure 66 Macintosh HD Folder



3 Double-click the **System Preferences** icon.

Figure 67 Applications Folder

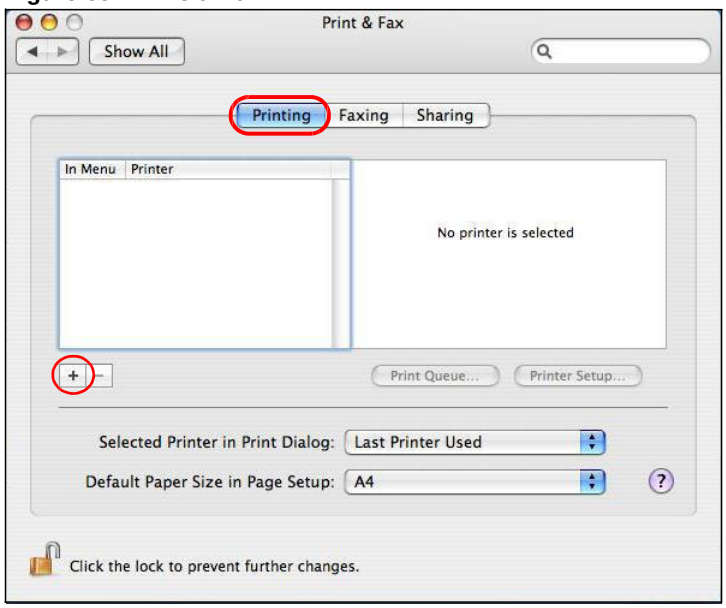


4 Click the **Print & Fax** icon.

Figure 68 System Preferences

5 Select the **Printing** tab and click the **+** icon to add a new printer.

Figure 69 Print & Fax



6 Click the **Advanced** button on the **Add Printer** toolbar to set up your printer.

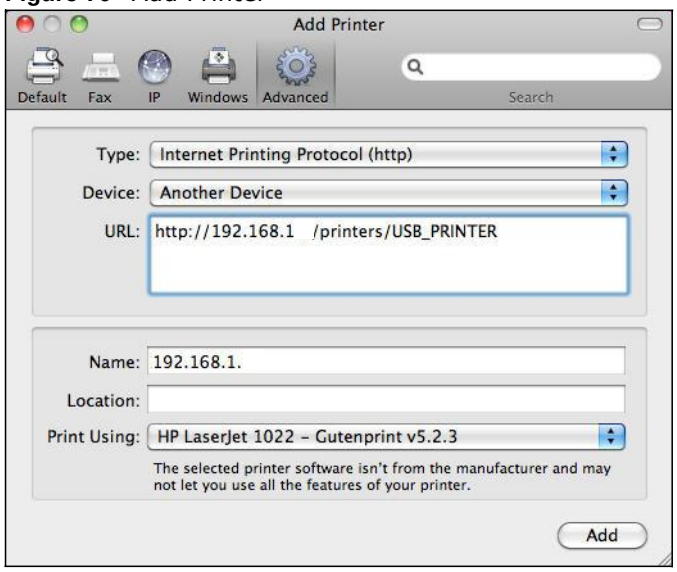
If the **Advanced** button doesn't appear, Ctrl-click the toolbar, select **Customize Toolbar...** and then drag the **Advanced** button onto the toolbar.

- Select **Internet Printing Protocol (HTTP)** from the **Type** drop-down list.
- Select **Another Device** from the **Device** drop-down list.
- In the **URL** field, enter "http://192.168.1.254:631/printers/USB_PRINTER" as the URL to access the print server (Device).

Note: If you change the Device's LAN IP address, use the new IP address in the URL to access the print server.

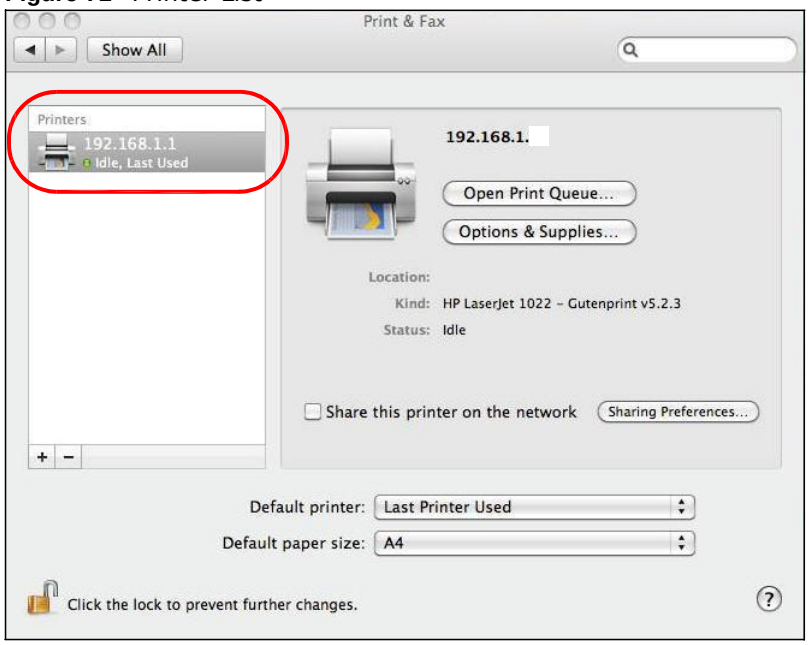
- Enter a descriptive name for the printer and where it is located.
- Select your printer manufacturer from the **Print Using** drop-down list and then select a printer model. Click **Add** to save and close the **Printer Browser** configuration screen.

Figure 70 Add Printer



7 The new network printer displays in the **Printers** list.

Figure 71 Printer List



8 Your print server driver setup is complete. You can now use the Device's print server to print from a Mac computer.

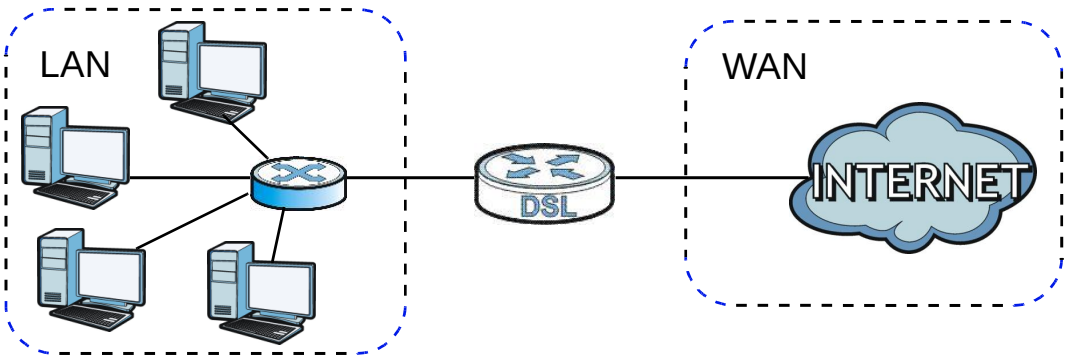
6.11 Home Networking Technical Reference

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

6.11.1 LANs, WANs and the Device

The actual physical connection determines whether the Device 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 72 LAN and WAN IP Addresses



6.11.2 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 Device as a DHCP server or disable it. When configured as a server, the Device 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 Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). Do not assign static IP addresses from the DHCP pool to your LAN computers.

6.11.3 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 Device supports the IPCP DNS server extensions through the DNS proxy feature.

  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.

6.11.4 LAN TCP/IP

The Device 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 Device. 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, 192.168.1.254, for your Device, 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 Device 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 Device 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".

6.11.5 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 Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only -** the Device will not send any RIP packets but will accept all RIP packets received.
- **Out Only -** the Device will send out RIP packets but will not accept any RIP packets received.
- **None -** the Device 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 Device sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

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

6.11.6 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.

At start up, the Device queries all directly connected networks to gather group membership. After that, the Device periodically updates this information. IP multicasting can be enabled/disabled on the Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

7

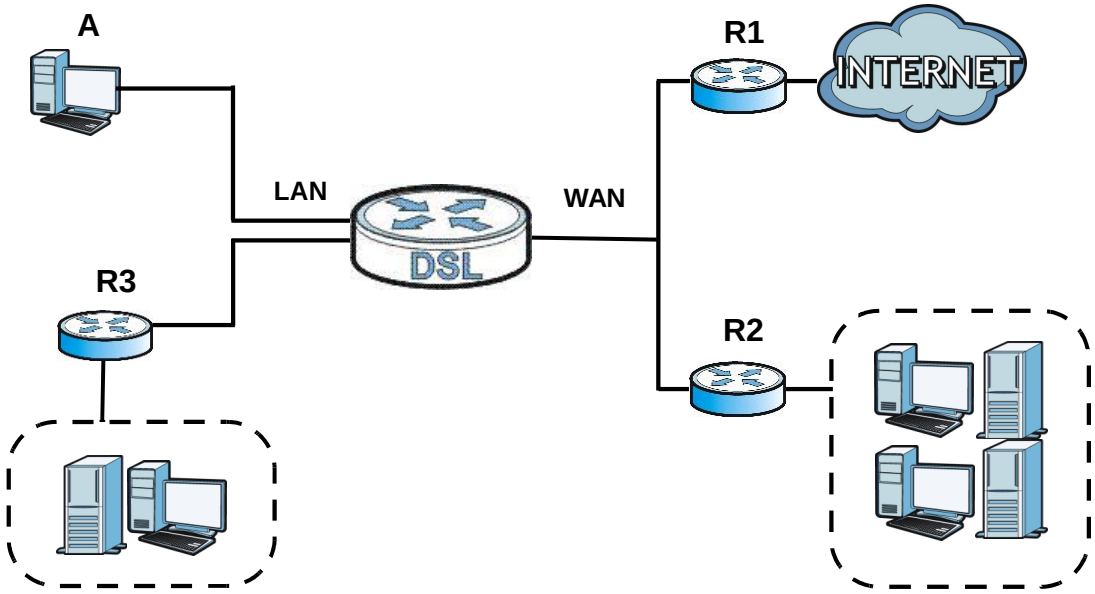
Static Route

7.1 Overview

The Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Device 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 Device's LAN interface. The Device routes most traffic from **A** to the Internet through the Device'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 73 Example of Static Routing Topology



7.1.1 What You Can Do in the Static Route Screens

- Use the **Static Route** screens (Section 7.2 on page 110) to view and configure IP static routes on the Device.
- Use the **IPv6 Static Route** screens (Section 7.3 on page 111) to view and configure IPv6 static routes on the Device.

7.2 The Static Route Screen

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

Figure 74 Network Setting > Static Route

The following table describes the labels in this screen.

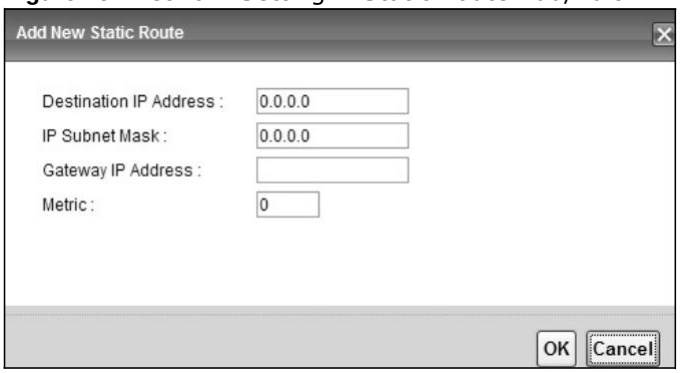
Table 30 Network Setting > Static Route

LABEL	DESCRIPTION
Add new static route	Click this to configure a new static route.
#	This is the number of an individual static route.
Destination IP	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.
Metric	This is the number of transmission hops between this Device and the destination.
Modify	Click the **Edit** icon to go to the screen where you can set up a static route on the Device. Click the **Delete** icon to remove a static route from the Device. A window displays asking you to confirm that you want to delete the route.

7.2.1 Static Route Add/Edit

Use this screen to add or edit a static route. Click **Add new Static Route Entry** in the **Routing** screen or the **Edit** icon next to the static route you want to edit. The screen shown next appears.

Figure 75 Network Setting > Static Route Add/Edit



The following table describes the labels in this screen.

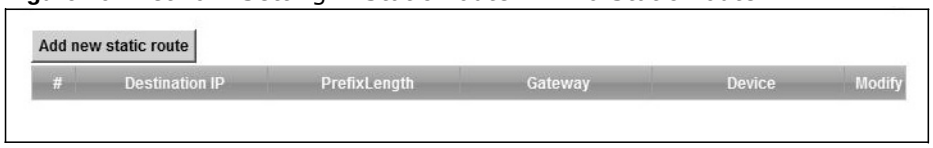
Table 31 Network Setting > Static Route Add/Edit

LABEL	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Enter the number of transmission hops (routers) that need to accross from the Device to the destination.
OK	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.3 IPv6 Static Route

Use this screen to view the IPv6 static route rules. Click **Network Setting > Static Route > IPv6 Static Route** to open the **IPv6 Static Route** screen.

Figure 76 Network Setting > Static Route > IPv6 Static Route



The following table describes the labels in this screen.

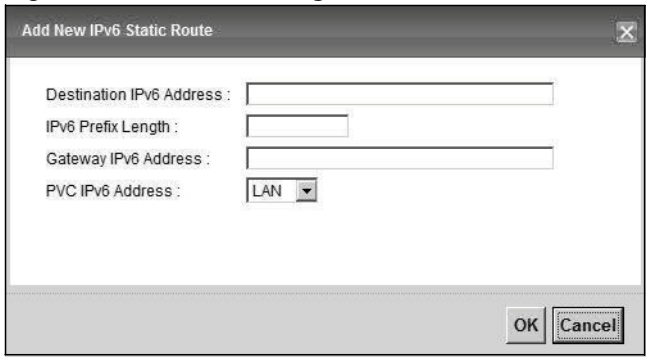
Table 32 Network Setting > Static Route > IPv6 Static Route

LABEL	DESCRIPTION
Add new static route	Click this to configure a new IPv6 static route.
#	This is the number of an individual static route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Prefix Length	An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
Gateway	This is the IPv6 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 has a route to the destination network and helps forward packets to their destinations.
Device	This specifies the LAN or WAN PVC.
Modify	Click the **Edit** icon to go to the screen where you can set up a static route on the Device. Click the **Remove** icon to remove a static route from the Device. A window displays asking you to confirm that you want to delete the route.

7.3.1 IPv6 Static Route Edit

Use this screen to configure the required information for an IPv6 static route. Click **Add new static route** or select an IPv6 static route index number and click **Edit**. The screen shown next appears.

Figure 77 Network Setting > Static Route > IPv6 Static Route: Add/Edit



The following table describes the labels in this screen.

Table 33 Network Setting > Static Route > IPv6 Static Route: Add/Edit

LABEL	DESCRIPTION
Destination IPv6 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 prefix length of 128 in the prefix length field to force the network number to be identical to the host ID.
IPv6 Prefix Length	Enter the address prefix to specify how many most significant bits compose the network address.
Gateway IPv6 Address	Enter the IPv6 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 has a route to the destination network and helps forward packets to their destinations. If a link local address is used, the interface should also be specified.
PVC IPv6 Address	Select the interface through which the traffic is routed.
OK	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

8

Quality of Service (QoS)

8.1 Overview

Use the **QoS** screen to set up your Device to use QoS for traffic management.

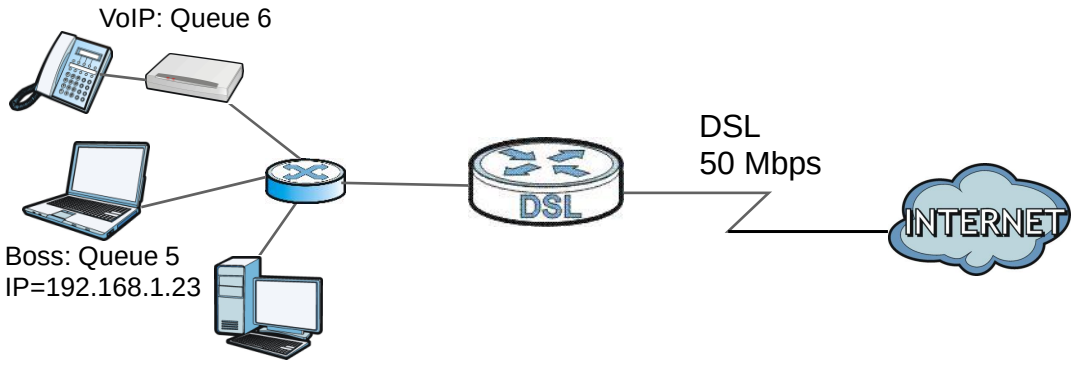
Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control bandwidth. QoS allows the Device to group and prioritize application traffic and fine-tune network performance.

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 Device 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.

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 Device.

Figure 78 QoS Example



8.1.1 What You Can Do in the QoS Screens

- Use the **General** screen (Section 8.2 on page 114) to enable QoS on the Device, and specify the type of scheduling.

- Use the **Queue Setup** screen (Section 8.3 on page 115) to configure QoS settings on the Device.
- Use the **Class Setup** screen (Section 8.4 on page 117) to configure QoS settings on the Device.
- Use the **Game List** screen (Section 8.5 on page 121) to to give priority to traffic for specific games.

8.1.2 What You Need to Know About QoS

802.1p

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. 802.1p 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 802.1p to give different priorities to different packet types.

Tagging and Marking

In a QoS class, you can configure whether to add or change the DiffServ Code Point (DSCP) value and IEEE 802.1p priority level 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

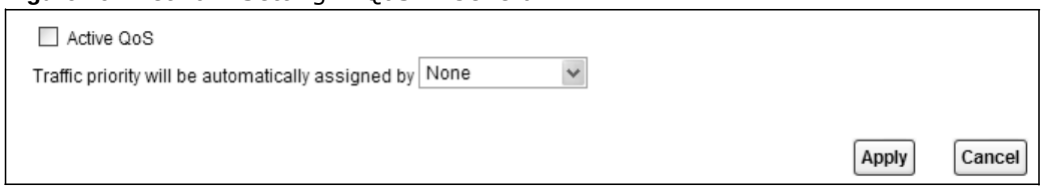
See Section 8.6 on page 122 for advanced technical information on QoS.

8.2 The Quality of Service General Screen

Use this screen to enable or disable QoS and set the upstream bandwidth.

Click **Network Setting > QoS > General** to open the screen as shown next.

Figure 79 Network Setting > QoS > General



The following table describes the labels in this screen.

Table 34 Network Setting > QoS > General

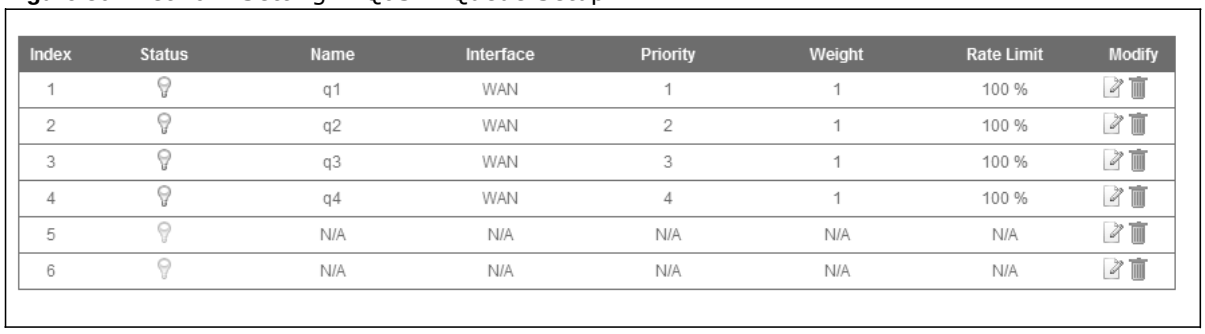
LABEL	DESCRIPTION
Active QoS	Use this field to turn on QoS to improve your network performance.
Traffic priority will be automatically assigned by	Select how the Device assigns priorities to various incoming and outgoing traffic flows. • **None**: Disables auto priority mapping and has the Device put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. • **Ethernet Priority**: Automatically assign priority based on the IEEE 802.1p priority level. • **IP Precedence**: Automatically assign priority based on the first three bits of the TOS field in the IP header. • **Packet Length**: Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

8.3 The Queue Setup Screen

Use this screen to configure QoS queue assignment disciplines and priorities.

Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Figure 80 Network Setting > QoS > Queue Setup



Index	Status	Name	Interface	Priority	Weight	Rate Limit	Modify
1		q1	WAN	1	1	100 %	
2		q2	WAN	2	1	100 %	
3		q3	WAN	3	1	100 %	
4		q4	WAN	4	1	100 %	
5		N/A	N/A	N/A	N/A	N/A	
6		N/A	N/A	N/A	N/A	N/A	

The following table describes the labels in this screen.

Table 35 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Index	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.

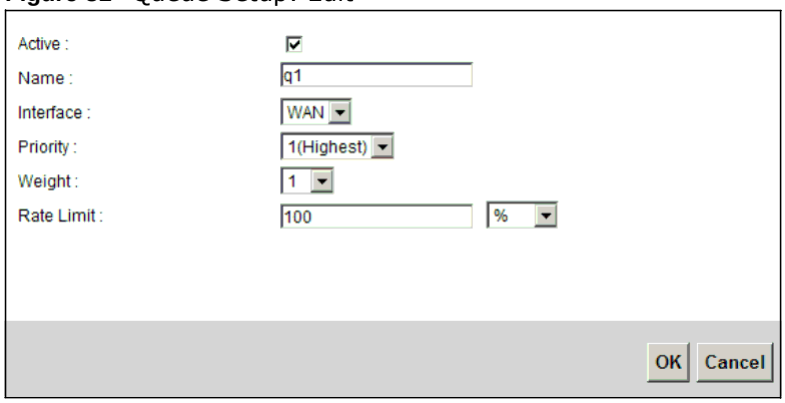
Table 35 Network Setting > QoS > Queue Setup (continued)

LABEL	DESCRIPTION
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

8.3.1 Adding a QoS Queue

Click the edit icon in the **Queue Setup** screen to configure a queue.

Figure 81 Queue Setup: Edit



The following table describes the labels in this screen.

Table 36 Queue Setup: Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 3) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

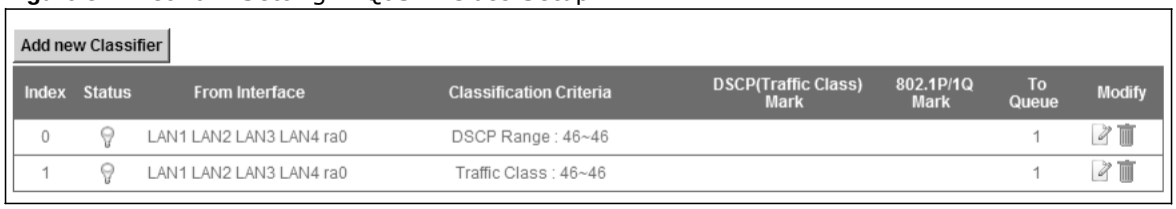
8.4 The Class Setup Screen

Use this screen to add, edit or delete QoS 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.

You can give different priorities to traffic that the Device 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.

Click **Network Setting > QoS > Class Setup** to open the screen as shown next.

Figure 82 Network Setting > QoS > Class Setup



The following table describes the labels in this screen.

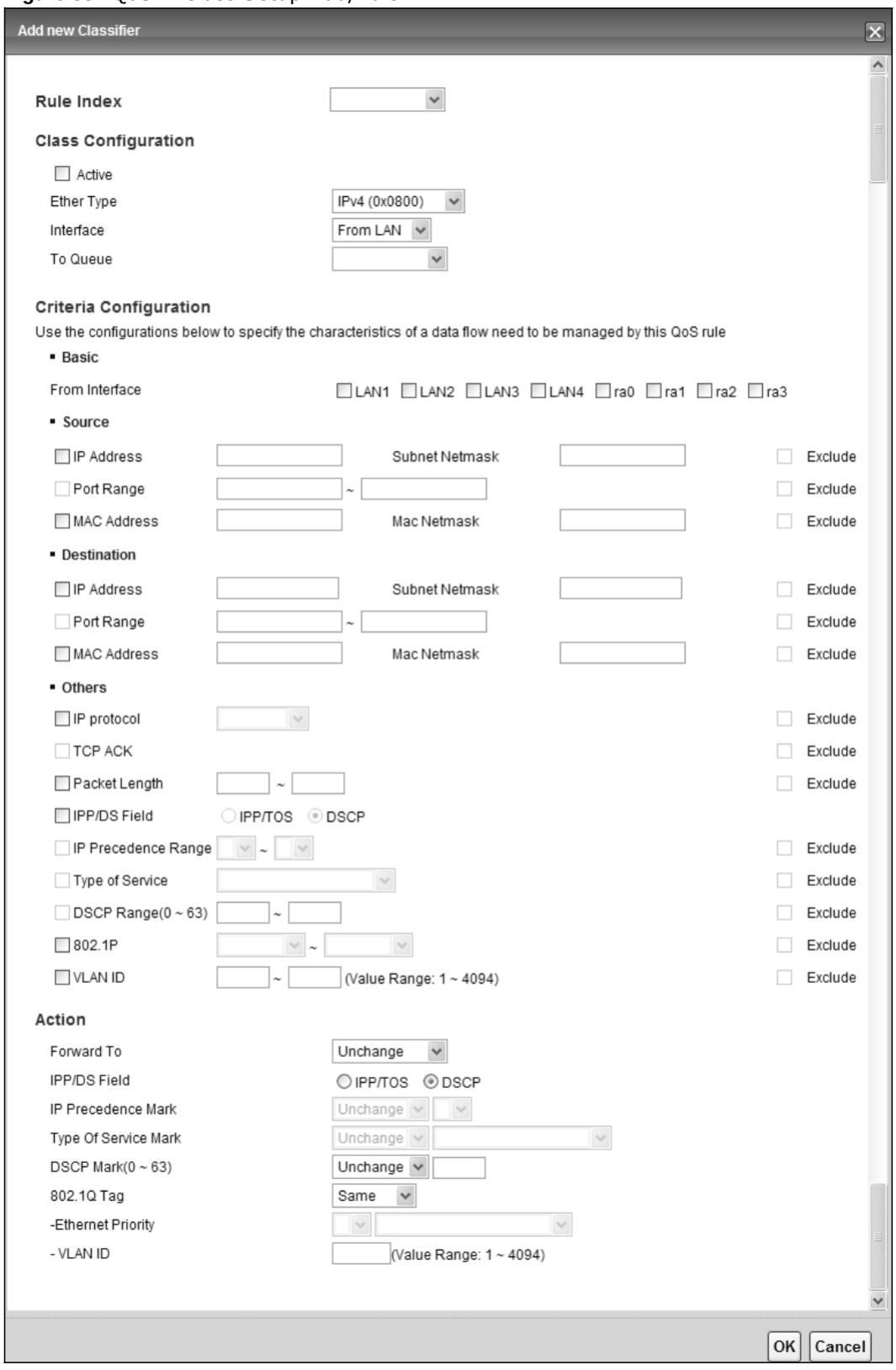
Table 37 Network Setting > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
Index	This is the index number of the entry.
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
From Interface	This shows the interface from which traffic of this class should come.
Classification Criteria	This shows criteria specified in this classifier, for example the type and the source MAC address of traffic that matches this classifier.
DSCP (Traffic Class) Mark	This is the DSCP number added to traffic of this classifier.
802.1P/1Q Mark	This is the IEEE 802.1p priority level and 802.1Q VLAN tag assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to edit the classifier. Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

8.4.1 Class Setup Add/Edit

Click **Add new Classifier** in the **Network Setting > QoS > Class Setup** screen or click the **Edit** icon next to a class, the screen appears as shown next.

Figure 83 QoS > Class Setup Add/Edit



The following table describes the labels in this screen.

Table 38 QoS > Class Setup Add/Edit

LABEL	DESCRIPTION
Rule Index	Select the rule's index number from the drop-down list box. This field is available only when you are adding a new QoS class.
Class Configuration	
Active	Use this field to enable or disable the QoS class rule.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IPv4 or IPv6**, you also need to configure source or destination IP address, MAC address, DHCP options, DSCP value or the protocol type. If you select **ARP**, you also need to configure source or destination MAC address. If you select **802.1Q**, you can configure an 802.1p priority level and VLAN ID.
Interface	Select an interface if you want to classify the traffic received by it.
To Queue	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Criteria Configuration	
Basic	
From Interface	If you select **From LAN** in the **Interface** field, you can select specific interface(s) from which traffic is received. **ra0** ~ **ra3** means wireless interfaces WLAN0 to WLAN3. If you select **From WAN** in the **Interface** field, you can select a specific WAN connection (PVC0~PVC2) from which traffic is received.
Source	
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank IP address means any source IP address.
Subnet Netmask/ Source Prefix Length	Enter the source subnet mask if you select **IPv4** as the **Ether Type**. Enter the source prefix length if you select **IPv6** as the **Ether Type**.
Port Range	If you select **TCP/UDP**, **TCP** or **UDP** in the **IP protocol** field, select the check box and enter the port number(s) of the source.
MAC Address	Select the check box and enter the source MAC address of the packet.
Mac Netmask	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	
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank IP address means any destination IP address.
Subnet Netmask/ Destination Prefix Length	Enter the destination subnet mask if you select **IPv4** as the **Ether Type**. Enter the destination prefix length if you select **IPv6** as the **Ether Type**.
Port Range	If you select **TCP/UDP**, **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.

Table 38 QoS > Class Setup Add/Edit (continued)

LABEL	DESCRIPTION
MAC Address	Select the check box and enter the destination MAC address of the packet.
Mac Netmask	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.
Others	
IP Protocol	This field is available only when you select **IPv4 or IPv6** in the **Ether Type** field. If you select **IPv4**, select this option and select the protocol (service type) from **TCP/UDP**, **TCP**, **UDP** or **ICMP**.If you select **IPv6**, select this option and select the protocol (service type) from **TCP/UDP**, **TCP**, **UDP** or **ICMPv6**.
TCP ACK	This field is available only when you select **TCP** in the **IP protocol** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
Packet Length	This field is available only when you select **IPv4 or IPv6** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.
IPP/DS Field	Select **IPP/TOS** to specify an IP precedence range and type of services. Select **DSCP** to specify a DiffServ Code Point (DSCP) range.
IP Precedence Range	Enter a range from 0 to 7 for IP precedence. 0 is the lowest priority and 7 is the highest.
Type of Service	Select a type of service from the drop-down list box. Available options are: **Normal service**, **Minimize delay**, **Maximize throughput**, **Maximize reliability** and **Minimize monetary cost**.
DSCP Range	Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
802.1P	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 enter the source VLAN ID in this field.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Action	
Forward To	Select the interface through which traffic that matches the rule is forwarded out. If you select **Unchange**, the Device forwards traffic of this class according to the default routing table. If traffic of this class comes from a WAN interface and is in a queue that forwards traffic through the LAN/WLAN interface, the Device ignores the setting here.
IPP/DS Field	Select **IPP/TOS** to specify an IP precedence range and type of services. Select **DSCP** to specify a DiffServ Code Point (DSCP) range.

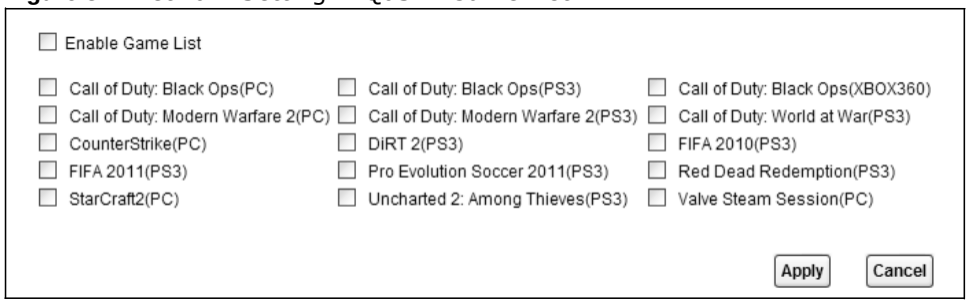
Table 38 QoS > Class Setup Add/Edit (continued)

LABEL	DESCRIPTION
IP Precedence Mark	Enter a range from 0 to 7 to re-assign IP precedence to matched traffic. 0 is the lowest priority and 7 is the highest.
Type Of Service Mark	Select a type of service to re-assign the priority level to matched traffic. Available options are: **Normal service**, **Minimize delay**, **Maximize throughput**, **Maximize reliability** and **Minimize monetary cost**.
DSCP Mark(0~63)	This field is available only when you select **IP** in the **Ether Type** field. If you select **Mark**, enter a DSCP value with which the Device replaces the DSCP field in the packets. If you select **Unchange**, the Device keep the DSCP field in the packets.
802.1Q Tag	If you select **Remark**, select a priority level (in the **Ethernet Priority** field) and enter a VLAN ID number (in the **VLAN ID** field) with which the Device replaces the IEEE 802.1p priority field and VLAN ID of the frames. If you select **Remove**, the Device deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the Device treat all matched traffic untagged and add a second priority level and VLAN ID that you specify in the **Ethernet Priority** and **VLAN ID** fields. If you select **Same**, the Device keep the Ethernet Priority and VLAN ID in the packets. To configure the Ethernet Priority, you can either select a priority number in the first drop-down list box (7 is the highest and 0 is the lowest priority) or select an application from the second drop-down list box which automatically maps to the corresponding priority number. (Key Net Traffic: 7; Voice: 6; Video: 5;IGMP: 4; Key Data: 3)
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

8.5 The QoS Game List Screen

Use this screen to give priority to traffic for specific games. Click **Network Setting > QoS > Game List** to open the screen as shown next.

Figure 84 Network Setting > QoS > Game List



The following table describes the labels in this screen.

Table 39 Network Setting > QoS > Game List

LABEL	DESCRIPTION
Enable Game List	Select this to have QoS give the highest priority to traffic for the games you specify. This priority is higher than the other QoS queues. Select the games below.
Apply	Click this to save your changes.
Cancel	Click this to restore previously saved settings.

8.6 QoS Technical Reference

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

8.6.1 IEEE 802.1p

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 40 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.

8.6.2 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.

8.6.3 Automatic Priority Queue Assignment

If you enable QoS on the Device, the Device 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 Device. On the Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 41 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	

9

Network Address Translation (NAT)

9.1 Overview

This chapter discusses how to configure NAT on the Device. 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 126) to activate/deactivate NAT for the default WAN connection (PVC0).
- Use the **Port Forwarding** screen (Section 9.3 on page 127) to configure forward incoming service requests to the server(s) on your local network.
- Use the **DMZ** screen to configure a default server (Section 9.4 on page 129).
- Use the **ALG** screen to enable and disable the SIP (VoIP) ALG in the Device (Section 9.5 on page 130).

9.1.2 What You Need To Know About NAT

Inside/Outside

Inside/outside denotes where a host is located relative to the Device, 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.

Finding Out More

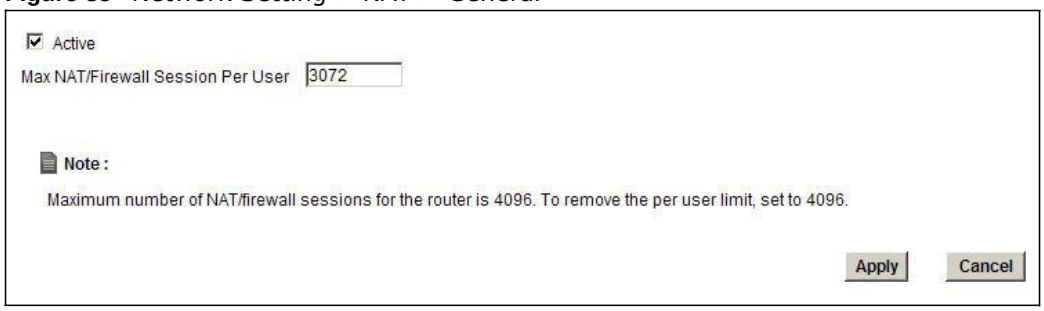
See Section 9.6 on page 130 for advanced technical information on NAT.

9.2 The NAT General Screen

Use this screen to activate NAT for the default WAN connection (PVC0). Click **Network Setting > NAT** to open the following screen.

Note: You must create an IP filter rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the Device.

Figure 85 Network Setting > NAT > General



The following table describes the labels in this screen.

Table 42 Network Setting > NAT > General

LABEL	DESCRIPTION
Active	Select this check box to enable NAT.
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 Device. 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

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.

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.

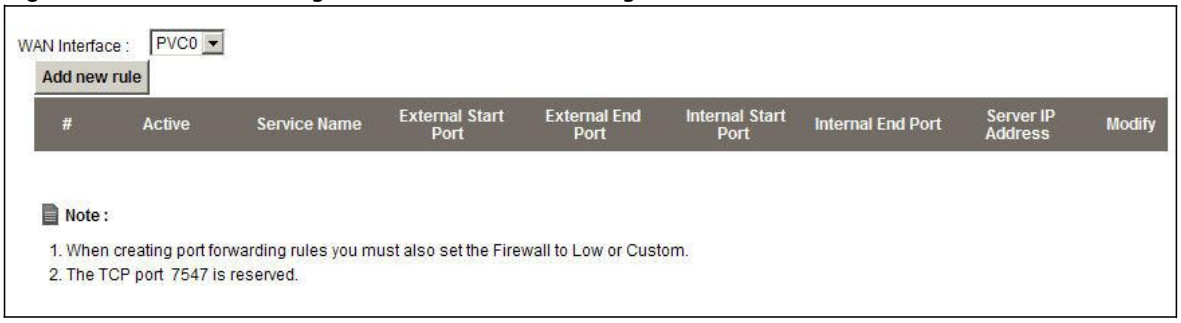
Note: If you do not assign a **Default Server** IP address, the Device discards all packets received for ports that are not specified here or in the remote management setup.

9.3.1 Configuring the Port Forwarding Screen

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

Note: Make sure NAT is activated on the WAN connection before you configure a port forwarding rule for it. For the default WAN connection (PVC0), activate NAT in the **Network Setting > NAT > General** screen. For other WAN connections (PVC1~PVC7), activate NAT for an individual WAN connection in the **Broadband** > **More Connections** > **Edit** screen.

Figure 86 Network Setting > NAT > Port Forwarding



The following table describes the fields in this screen.

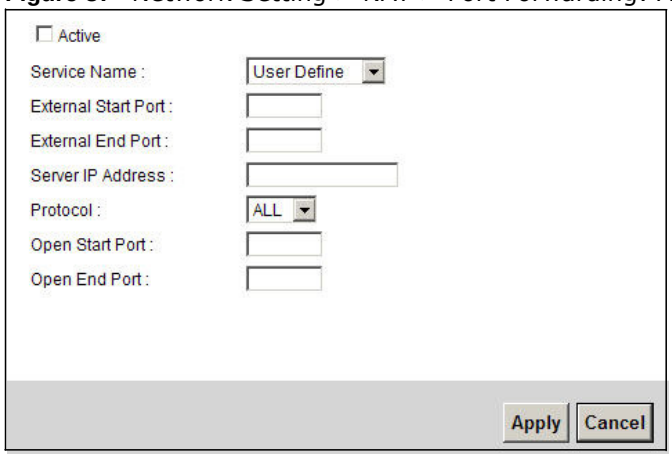
Table 43 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
WAN Interface	Select a WAN connection for which you want to configure a port forwarding rule.
Add new rule	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.
External Start Port	This is the first port number of a port range that incoming service requests may use to access the service in your local network.
External End Port	This is the last port number of a port range that incoming service requests may use to access the service in your local network.
Internal Start Port	This is the starting port number that the device translates for the service in your local network.
Internal End Port	This is the ending port number that the device translates for the service in your local network.
Server IP Address	This is the server's IP address in your local network.
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.

9.3.2 Port Forwarding Rule Add/Edit

Use this screen to add or edit a port forwarding rule. Click the **Add new rule** button or a rule's edit icon in the **Port Forwarding** screen to display the screen as shown next.

Figure 87 Network Setting > NAT > Port Forwarding: Add/Edit



The following table describes the fields in this screen.

Table 44 Network Setting > NAT > Port Forwarding: Edit

LABEL	DESCRIPTION
Active	Click this check box to enable the rule.
Service Name	Select the name of this port-forwarding rule.

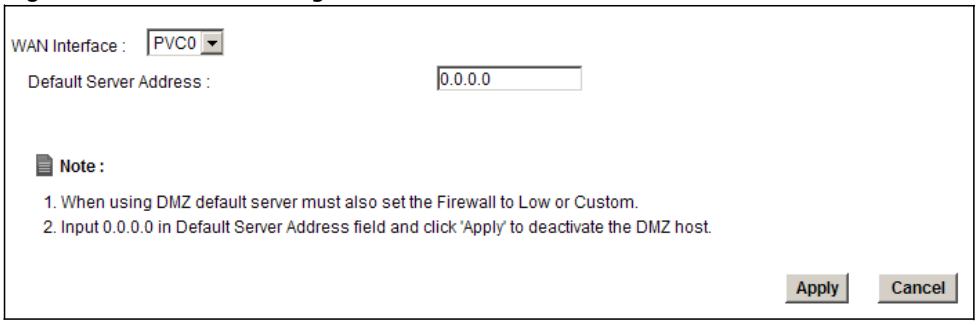
Table 44 Network Setting > NAT > Port Forwarding: Edit (continued)

LABEL	DESCRIPTION
External 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.
External End Port	Enter a port number in this field. To forward only one port, enter the port number 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 IP address of the server in your local network.
Protocol	Select the protocol of the service, **TCP**, **UDP** or **ALL** (TCP+UDP).
Open Start Port	Enter the first port number here to which you want the device to translate the incoming port. For a range of ports, you only need to enter the first number of the range to which you want the incoming ports translated, the device automatically calculates the last port of the translated port range.
Open End Port	Enter the last port number here to which you want the device to translate the incoming port. For a range of ports, you only need to enter the first number of the range to which you want the incoming ports translated, the device automatically calculates the last port of the translated port range.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.4 The DMZ Screen

If you need to allow packets from a specific WAN connection to your local network, NAT supports a default server IP address. A default server receives packets from the specified WAN connection and the ports that are not specified in the **NAT Port Forwarding Setup** screen.

Figure 88 Network Setting > NAT > DMZ



The following table describes the fields in this screen.

Table 45 Network Setting > NAT > DMZ

LABEL	DESCRIPTION
WAN Interface	Select a WAN PVC connection (**PVC0**~**PVC7**) from which you want to forward the traffic to the specified default server.
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **NAT > Port Forwarding** screen. Note: If you do not assign a **Default Server Address**, the Device discards all packets received for ports that are not specified in the **NAT Port Forwarding** screen.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** 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 Device registers with the SIP register server, the SIP ALG translates the Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if you enable this Device's SIP ALG.

Use the **ALG** screen to enable and disable the SIP (VoIP) ALG in the Device. To access this screen, click **Network Setting** > **NAT** > **ALG**.

Figure 89 Network Setting > NAT > ALG

The following table describes the fields in this screen.

Table 46 Network Setting > NAT > ALG

LABEL	DESCRIPTION
ALG	Select **Enable** to make sure SIP (VoIP) works correctly with NAT.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** 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 Device, 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 47 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.

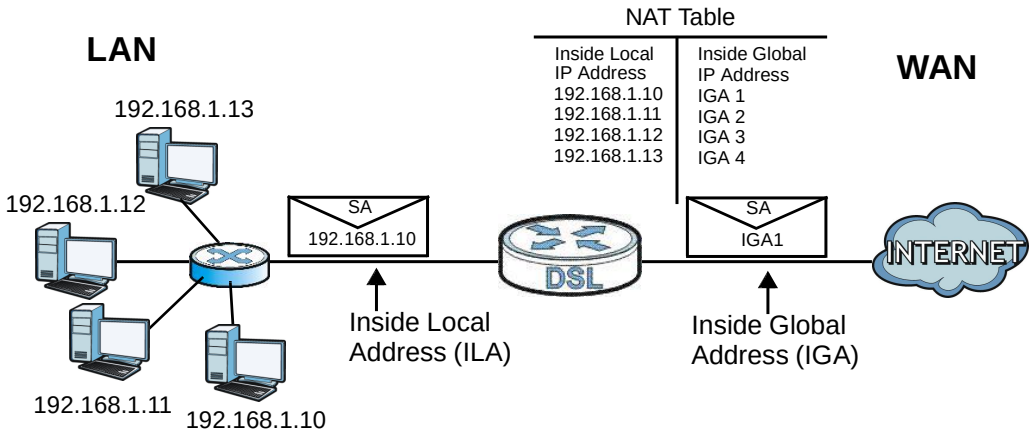
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see *Table 48 on page 133*), NAT offers the additional benefit of firewall protection. With no servers defined, your Device 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

Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

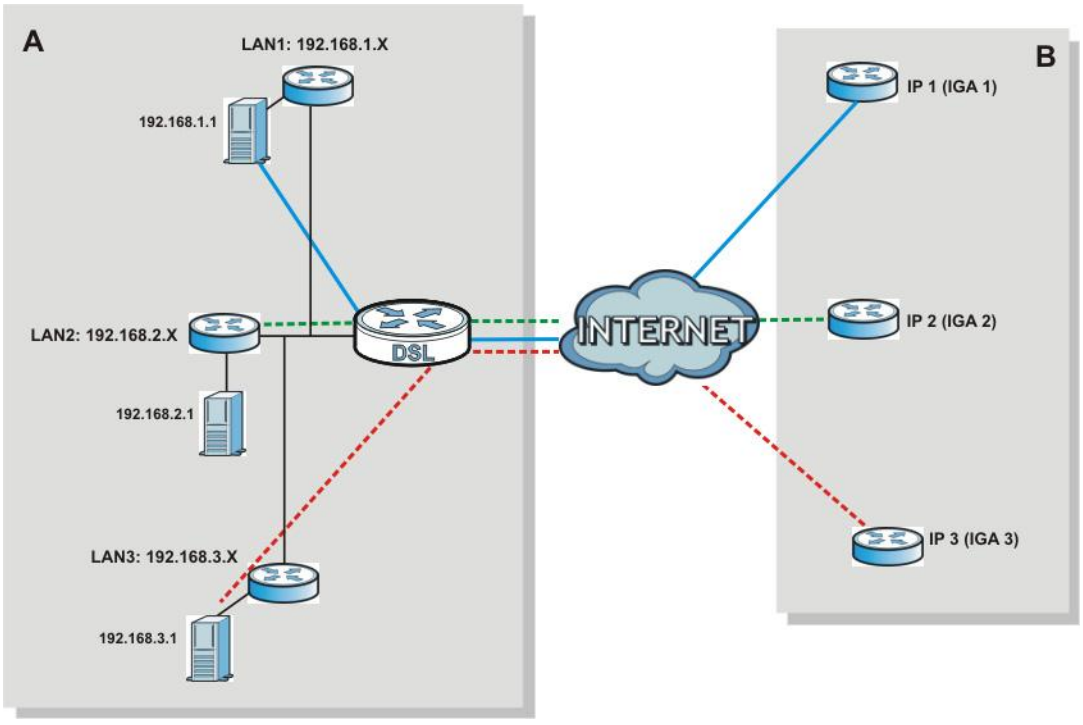
Figure 90 How NAT Works



9.6.4 NAT Application

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

Figure 91 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 Device maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the Device maps multiple local IP addresses to one global IP address.
- **Many to Many Overload**: In Many-to-Many Overload mode, the Device maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the Device 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 48 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

Port Isolation

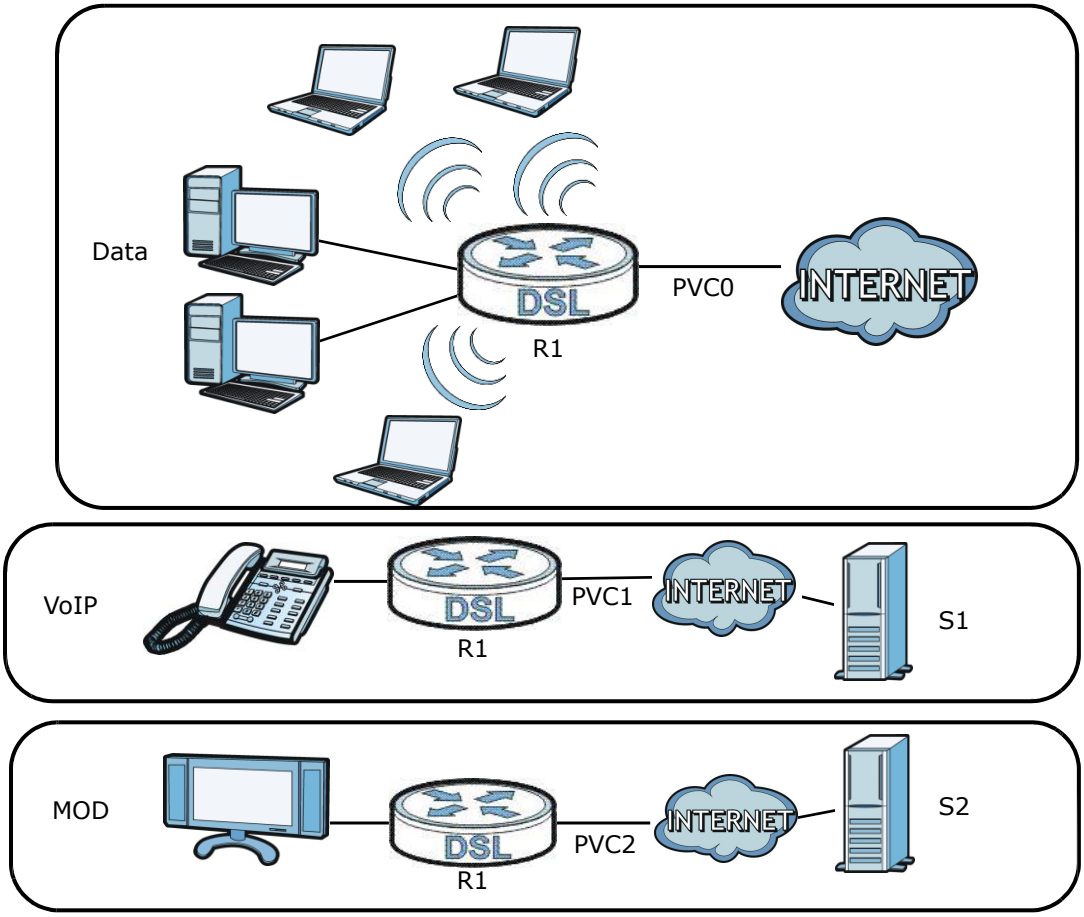
10.1 Overview

This chapter describes how to configure the port isolation settings.

Port isolation allows you to aggregate port connections into logical groups. You may bind WAN PVCs to Ethernet ports and WLANs to specify how traffic is forwarded. Different ATM QoS settings can be specified for each WAN PVC to meet bandwidth requirements for the type of traffic to be transferred.

For example, three port isolation groups could be created on the device (R1) for three different WAN PVC connections. The first PVC (PVC0) is for non time-sensitive data traffic. The second and third PVCs (PVC1 and PVC2) are for time sensitive Media-On-Demand (MOD) video traffic and VoIP traffic, respectively.

Figure 92 Port Isolation Groups



If a WAN PVC is bound to an Ethernet port, traffic from the Ethernet port will only be forwarded through the specified WAN PVC and vice versa. If a port is not in a port isolation group, traffic to and from the port will be forwarded according to the routing table.

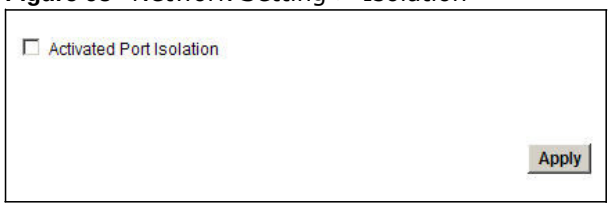
10.1.1 What You Can Do in the Port Isolation Screens

- Use the **General** screen (Section 10.3 on page 136) to activate port isolation.
- Use the **Port Isolation** screen (Section 10.3 on page 136) to set up port isolation groups.
- Use the **Port Isolation Summary** screen (Section 10.3.1 on page 137) to view configured port isolation groups.

10.2 The Port Isolation General Screen

Use this screen to activate port isolation and set up port isolation groups. Click **Network Setting > Port Isolation** to display the following screen.

Figure 93 Network Setting > Isolation



The following table describes the labels in this screen.

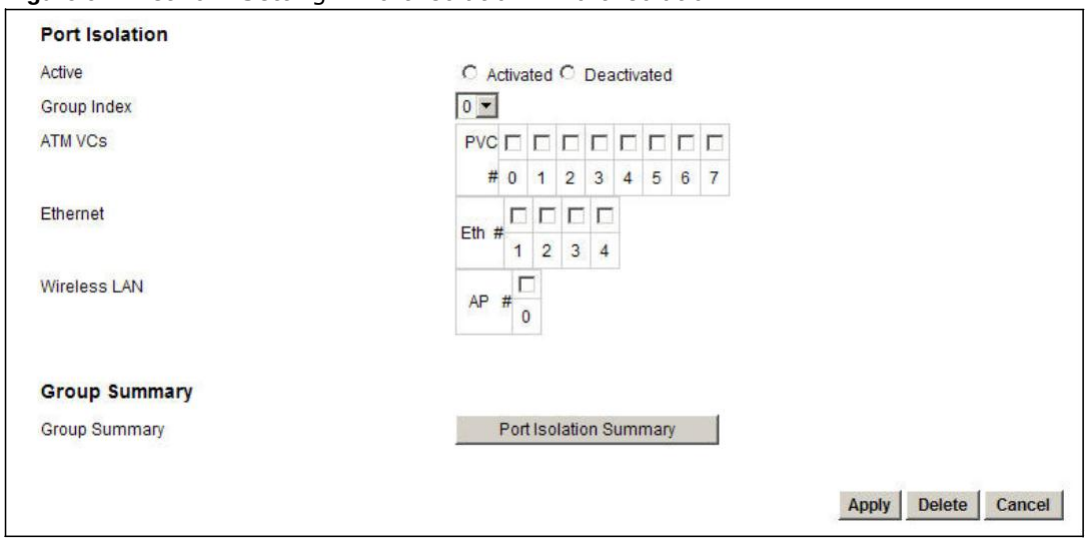
Table 49 Network Setting > Port Isolation

LABEL	DESCRIPTION
Activated Port Isolation	Activate or deactivate the port isolation feature.
Apply	Add the selected port isolation group configuration.

10.3 The Port Isolation Screen

Use this screen to set up port isolation groups. Click **Network Setting > Port Isolation > Port Isolation** to display the following screen.

Figure 94 Network Setting > Port Isolation > Port Isolation



The following table describes the labels in this screen.

Table 50 Network Setting > Port Isolation > Port Isolation

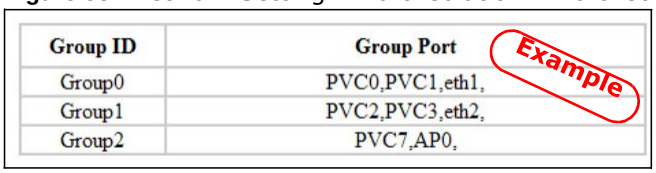
LABEL	DESCRIPTION
Port Isolation	
Active	Activate or deactivate port isolation for the port isolation group.
Group Index	Select the index number for the port isolation group. When a port is assigned to a port isolation group, traffic will be forwarded to the other ports in the group, but not to ports in other groups. If a port is not included in any groups, traffic will be forwarded according to the routing table.
ATM VCs	Select the ATM VC (PVC) to include in the port isolation group. Each ATM VC can only be bound to one group.
Ethernet	Select the Ethernet (Eth) ports to include in the port isolation group. Each Ethernet port can only be bound to one group.
Wireless LAN	Select the WLAN (AP) connection to include in the port isolation group. Additional APs can be enabled on the **More AP** screen (Section 5.3 on page 54).
Group Summary	
Port Isolation Summary	Click this to view a summary of configured port isolation groups.
Apply	Add the selected port isolation group configuration.
Delete	Delete the selected port isolation group configuration.
Cancel	Click this to restore your previously saved settings.

10.3.1 Port Isolation Summary Screen

Use this screen to view configured port isolation groups.

In the **Port Isolation** screen, click the **Port Isolation Summary** button in the **Group Summary** section to display the following screen.

Figure 95 Network Setting > Port Isolation > Port Isolation Summary



The following table describes the labels in this screen.

Table 51 Network Setting > Port Isolation > Port Isolation Summary

LABEL	DESCRIPTION
Group ID	This field displays the group index number.
Group Port	This field displays the ports included in the group.

11

Dynamic DNS Setup

11.1 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.

11.1.1 What You Can Do in the DDNS Screen

Use the **Dynamic DNS** screen (Section 11.2 on page 139) to enable DDNS and configure the DDNS settings on the Device.

11.1.2 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.

11.2 The Dynamic DNS Screen

Use this screen to change your Device’s DDNS. Click **Network Setting > Dynamic DNS**. The screen appears as shown.

Figure 96 Network Setting > Dynamic DNS

The following table describes the fields in this screen.

Table 52 Network Setting > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	This is the website of your Dynamic DNS service p rovider.
Host Name	Type the domain name assigned to your Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Username	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

12 Filter

12.1 Overview

This chapter introduces the filters supported by the Device. You can configure rules to restrict traffic by IP addresses, MAC addresses, and/or IPv6 addresses.

12.1.1 What You Can Do in the Filter Screens

- Use the **IP/MAC Filter** screen (Section 12.2 on page 141) to create IP and MAC filter rules.
- Use the **IPv6/MAC Filter** screen (Section 12.3 on page 143) to create IPv6 and MAC filter rules.

12.1.2 What You Need to Know About Filtering

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.

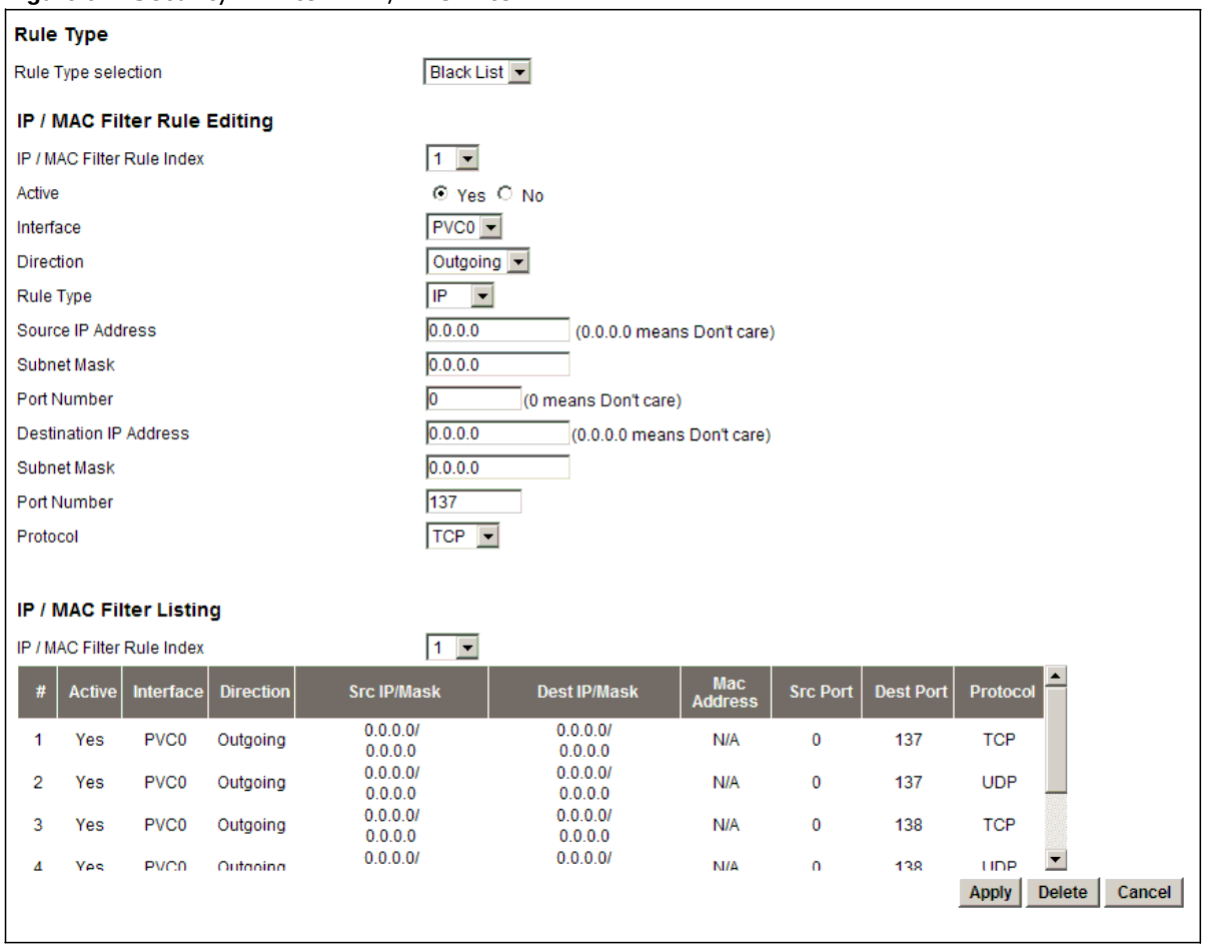
URL and IP Filter Structure

The URL, IP and IPv6 filters have individual rule indexes. The Device allows you to configure each type of filter with its own respective set of rules.

12.2 The IP/MAC Filter Screen

Use this screen to create and apply IP and MAC filters. Click **Security** > **Filter** > **IP/MAC Filter**. The screen appears as shown.

Figure 97 Security > Filter > IP/MAC Filter



The following table describes the labels in this screen.

Table 53 Security > Filter > IP/MAC Filter

LABEL	DESCRIPTION
Rule Type	
Rule Type selection	Select **White List** to specify traffic to allow and **Black List** to specify traffic to disallow.
IP / MAC Filter Rule Editing	
IP / MAC Filter Rule Index	Select the index number of the filter rule.
Active	Use this field to enable or disable the filter rule.
Interface	Select the PVC to which to apply the filter.
Direction	Apply the filter to **Incoming** or **Outgoing** traffic direction.
Rule Type	Select **IP** or **MAC** type to configure the rule. Use the **IP** Filter to block or allow traffic by IP addresses. Use the **MAC** Filter to block or allow traffic by MAC address.
Source IP Address	Enter the source IP address of the packets you wish to filter. This field is ignored if it is 0.0.0.0.
Subnet Mask	Enter the IP subnet mask for the source IP address

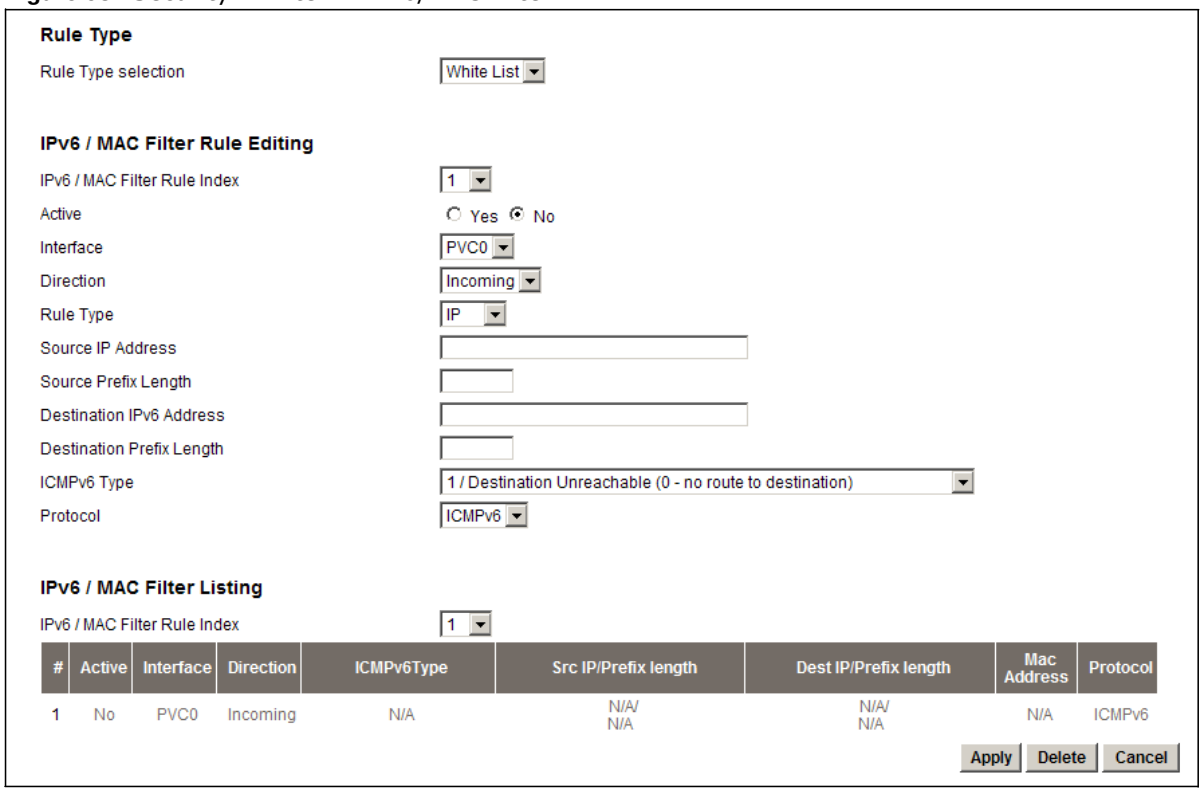
Table 53 Security > Filter > IP/MAC Filter (continued)

LABEL	DESCRIPTION
Port Number	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.
Destination IP Address	Enter the destination IP address of the packets you wish to filter. This field is ignored if it is 0.0.0.0.
Subnet Mask	Enter the IP subnet mask for the destination IP address.
Port Number	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.
Protocol	Select **ICMP**, **TCP** or **UDP** for the upper layer protocol.
IP / MAC Filter Listing	
IP / MAC Filter Rule Index	Select the index number of the filter set from the drop-down list box.
#	This is the index number of the rule in a filter set.
Active	This field shows whether the rule is activated.
Interface	This is the interface that the filter set applies to.
Direction	The filter set applies to this traffic direction.
Src IP/Mask	This is the source IP address and subnet mask when you select **IP** as the rule type.
Dest IP/Mask	This is the destination IP address and subnet mask.
Mac Address	This is the MAC address of the packets being filtered.
Src Port	This is the source port number.
Dest Port	This is the destination port number.
Protocol	This is the upper layer protocol.
Apply	Click this to apply your changes.
Delete	Click this to remove the filter rule.
Cancel	Click this to restore your previously saved settings.

12.3 IPv6/MAC Filter

Use this screen to create and apply IPv6 filters. Click **Security** > **Filter** > **IPv6/MAC Filter**. The screen appears as shown.

Figure 98 Security > Filter > IPv6/MAC Filter



The following table describes the labels in this screen.

Table 54 Security > Filter > IPv6/MAC Filter

LABEL	DESCRIPTION
Rule Type	
Rule Type selection	Select **White List** to specify traffic to allow and **Black List** to specify traffic to block.
IPv6 / MAC Filter Rule Editing	
IPv6 / MAC Filter Rule Index	Select the index number of the filter rule.
Active	Use this field to enable or disable the filter rule.
Interface	Select the PVC to which to apply the filter.
Direction	Apply the filter to **Incoming** or **Outgoing** traffic direction.
Rule Type	Select **IP** or **MAC** type to configure the rule. Use the **IP** Filter to block or allow traffic by IPv6 addresses. Use the **MAC** Filter to block or allow traffic by MAC address.
Source IP Address	Enter the source IPv6 address of the packets you wish to filter. This field is ignored if it is ::.
Source Prefix Length	Enter the prefix length for the source IPv6 address
Destination IPv6 Address	Enter the destination IPv6 address of the packets you wish to filter. This field is ignored if it is ::.
Destination Prefix Length	Enter the prefix length for the destination IPv6 address.

Table 54 Security > Filter > IPv6/MAC Filter (continued)

LABEL	DESCRIPTION
ICMPv6 Type	Select the ICMPv6 message type to filter. The following message types can be selected: **1 / Destination Unreachable:** 0 **-** no route to destination; 1 - communication with destination administratively prohibited; 3 - address unreachable; 4 - port unreachable **2 / Packet Too Big** **3 / Time Exceeded:** 0 - hop limit exceeded in transit; 1 - fragment reassembly time exceeded **4 / Parameter Problem**: 0 - erroneous header field encountered; 1 - unrecognized Next Header type encountered; 2 - unrecognized IPv6 option encountered **128 / Echo Request** **129 / Echo Response** **130 / Listener Query -** Multicast listener query **131 / Listener Report -** Multicast listener report **132 / Listener Done** - Multicast listener done **143 / Listener Report v2 -** Multicast listener report v2 **133 / Router Solicitation** **134 / Router Advertisement** **135 / Neighbor Solicitation** **136 / Neighbor Advertisement** **137 / Redirect -** Redirect message
Protocol	This is the (upper layer) protocol that defines the service to which this rule applies. By default it is ICMPv6.
IPv6 / MAC Filter Listing	
IPv6 / MAC Filter Rule Index	Select the index number of the filter set from the drop-down list box.
#	This is the index number of the rule in a filter set.
Active	This field shows whether the rule is activated.
Interface	This is the interface that the rule applies to.
Direction	The filter set applies to this traffic direction.
Rule Type	The ICMPv6 message type to filter.
Src IP/PrefixLength	This displays the source IPv6 address and prefix length.
Dest IP/PrefixLength	This displays the destination IPv6 address and prefix length.
Mac Address	This is the MAC address of the packets being filtered.
Protocol	This is the (upper layer) protocol that defines the service to which this rule applies. By default it is ICMPv6.
Apply	Click this to apply your changes.
Delete	Click this to remove the filter rule.
Cancel	Click this to restore your previously saved settings.

13 Firewall

13.1 Overview

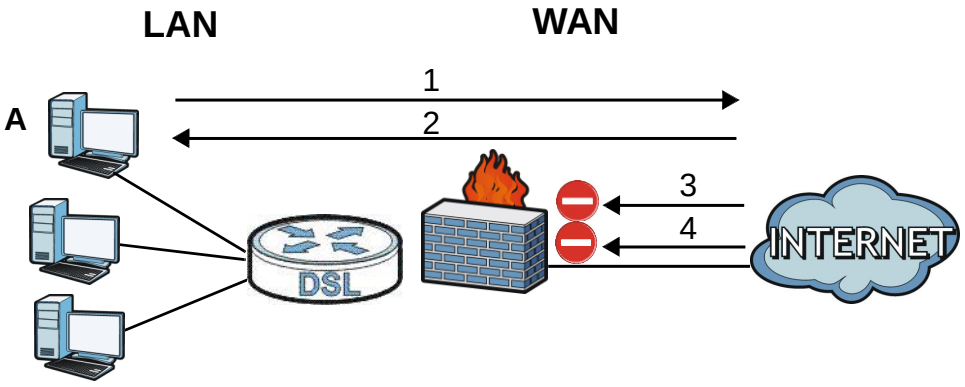
This chapter shows you how to enable the Device firewall. Use the firewall to protect your Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- 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.
- blocks SYN and port scanner attacks.

By default, the Device blocks DDOS, LAND and Ping of Death attacks whether the firewall is enabled or disabled.

The following figure illustrates the 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 99 Default Firewall Action



13.1.1 What You Can Do in the Firewall Screens

- Use the **General** screen (Section 13.2 on page 149) to select the firewall protection level on the Device.
- Use the **Default Action** screen (Section 13.3 on page 150) to set the default action that the firewall takes on packets that do not match any of the firewall rules.
- Use the **Rules** screen (Section 13.4 on page 151) to view the configured firewall rules and add, edit or remove a firewall rule.
- Use the **DoS** screen (Section 13.5 on page 156) to set the thresholds that the Device uses to determine when to start dropping sessions that do not become fully established (half-open sessions).

13.1.2 What You Need to Know About Firewall

SYN Attack

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

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 Device is pre-configured to automatically detect and thwart all known DoS attacks.

DDoS

A Distributed DoS (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

LAND Attack

In a Local Area Network Denial (LAND) attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

RFC 4890 SPEC Traffic

RFC 4890 specifies the filtering policies for ICMPv6 messages. This is important for protecting against security threats including DoS, probing, redirection attacks and renumbering attacks that can be carried out through ICMPv6. Since ICMPv6 error messages are critical for establishing and maintaining communications, filtering policy focuses on ICMPv6 informational messages.

Anti-Probing

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

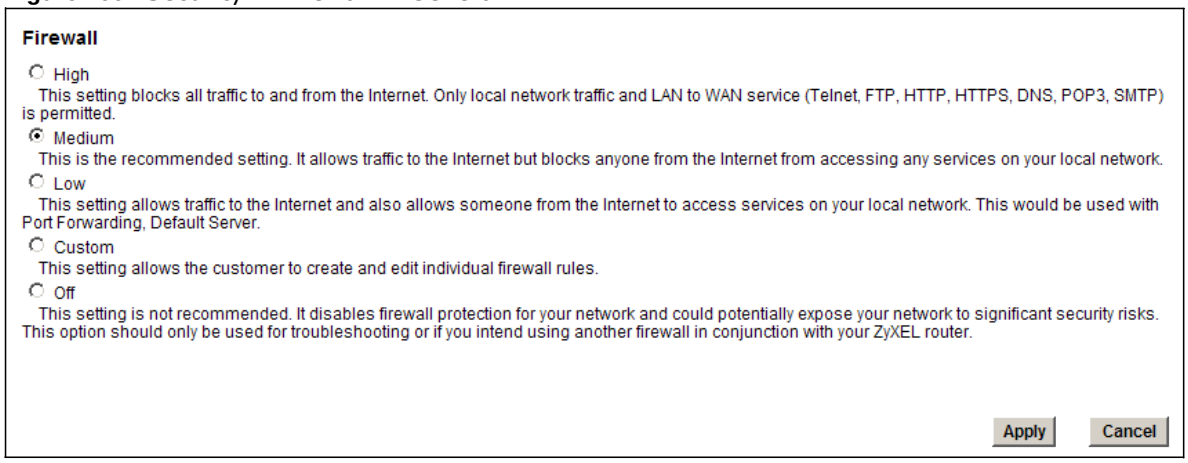
DoS Thresholds

For DoS attacks, the Device 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.

13.2 The Firewall General Screen

Use this screen to select the firewall protection level on the Device. Click **Security > Firewall > General** to display the following screen.

Figure 100 Security > Firewall > General



The following table describes the labels in this screen.

Table 55 Security > Firewall > General

LABEL	DESCRIPTION
High	This setting blocks all traffic to and from the Internet. Only local network traffic and LAN to WAN service (Telnet, FTP, HTTP, HTTPS, DNS, POP3, SMTP) is permitted.
Medium	This is the recommended setting. It allows traffic to the Internet but blocks anyone from the Internet from accessing any services on your local network.

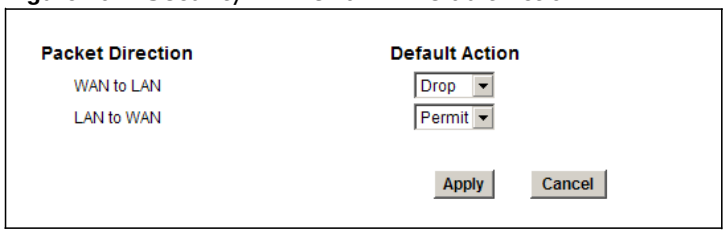
Table 55 Security > Firewall > General (continued)

LABEL	DESCRIPTION
Low	This setting allows traffic to the Internet and also allows someone from the Internet to access services on your local network. This would be used with Port Forwarding, Default Server.
Custom	This setting allows the customer to create and edit individual firewall rules. Firewall rules can be created in the Default Action screen (Section 13.3 on page 150) and Rules screen (Section 13.4 on page 151).
Off	This setting is not recommended. It disables firewall protection for your network and could potentially expose your network to significant security risks. This option should only be used for troubleshooting or if you intend using another firewall in conjunction with your router.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

13.3 The Default Action Screen

Use this screen to set the default action that the firewall takes on packets that do not match any of the firewall rules. Click **Security > Firewall > Default Action** to display the following screen.

Figure 101 Security > Firewall > Default Action



The following table describes the labels in this screen.

Table 56 Security > Firewall > Default Action

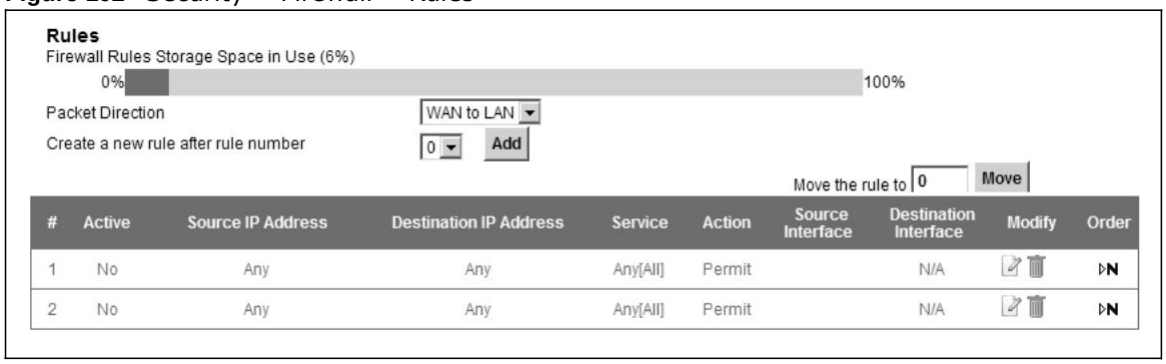
LABEL	DESCRIPTION
Packet Direction	This is the direction of travel of packets (**WAN to LAN**, **LAN to WAN)**. Firewall rules are grouped based on the direction of travel of packets to which they apply.
Default Action	Use the drop-down list boxes to select the default action that the firewall is to 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.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

13.4 The Rules Screen

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

Note: The firewall configuration screen shown in this section is specific to the following devices: P-The ordering of your rules is very important as rules are applied in turn.

Figure 102 Security > Firewall > Rules



The following table describes the labels in this screen.

Table 57 Security > Firewall > Rules

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the Device's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
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 Address	This column 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 Address	This column 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 column displays the services to which this firewall rule applies.
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**).

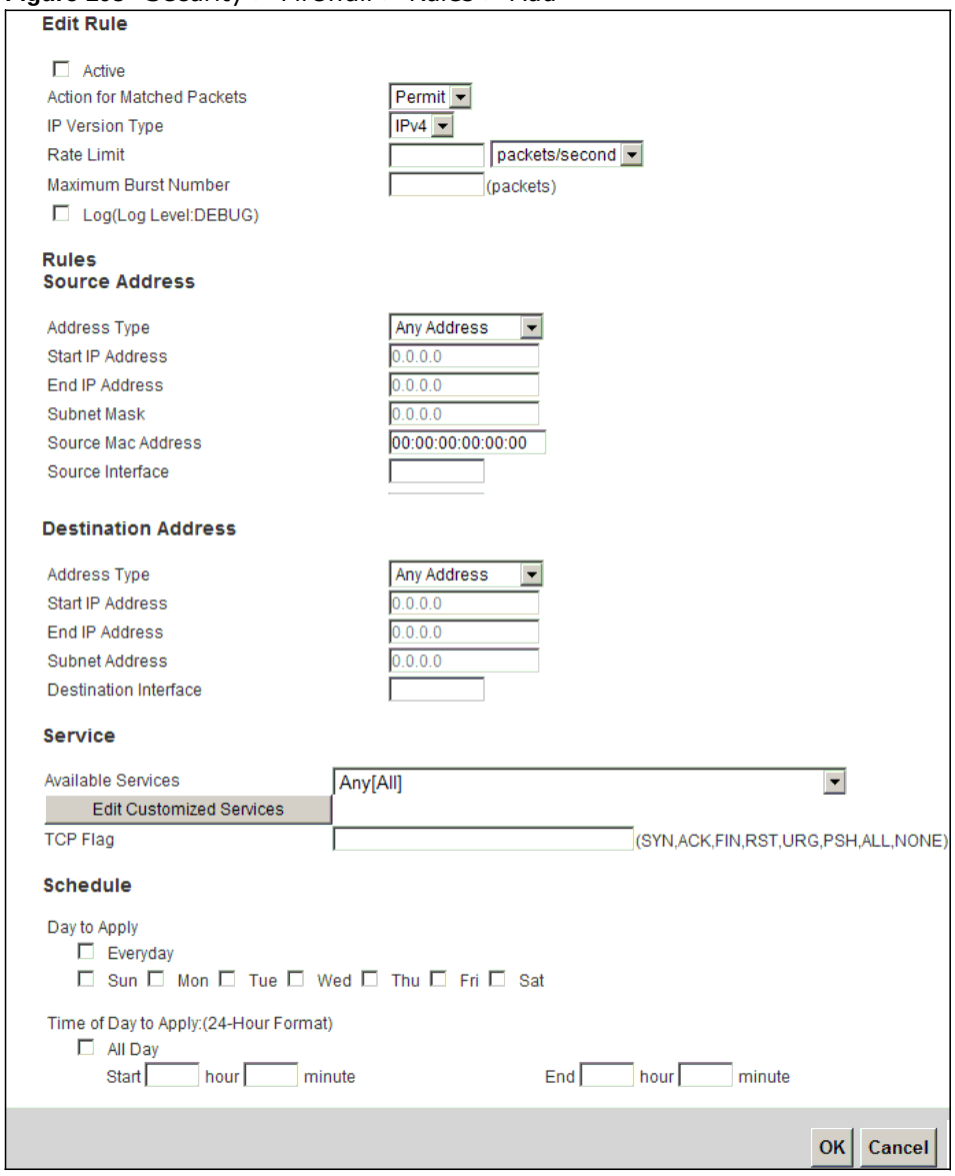
Table 57 Security > Firewall > Rules (continued)

LABEL	DESCRIPTION
Source Interface	This column displays the source interface to which this firewall rule applies. This is the interface through which the traffic entered the Device. Please note that a blank source interface is equivalent to **Any**.
Destination Interface	This column displays the destination interface to which this firewall rule applies. This is the interface through which the traffic is destined to leave the Device. Please note that a blank source interface is equivalent to **Any**.
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 **Order** 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.

13.4.1 The Rules Add Screen

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 103 Security > Firewall > Rules > Add



The following table describes the labels in this screen.

Table 58 Security > Firewall > Rules > Add

LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Action for Matched Packets	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.
IP Version Type	Select the IP version, **IPv4** or **IPv6**, to apply this firewall rule to.
Rate Limit	Set a maximum number of packets per second, minute, or hour to limit the throughput of traffic that matches this rule.
Maximum Burst Number	Set the maximum number of packets that can be sent at the peak rate.
Log	This field determines if a log for packets that match the rule is created or not.

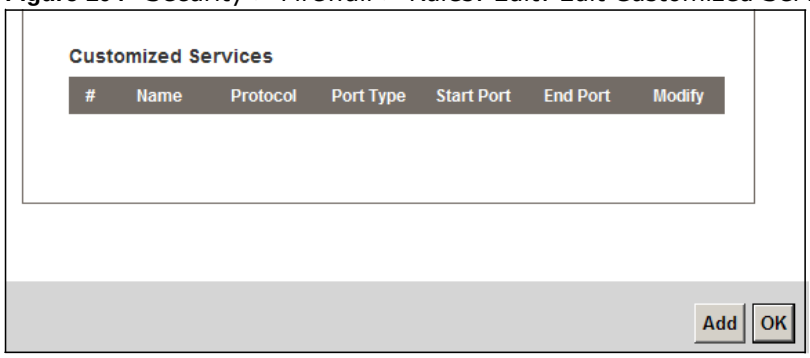
Table 58 Security > Firewall > Rules > Add (continued)

LABEL	DESCRIPTION
Rules Source/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.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Source Mac Address	Specify a source MAC address of traffic to which to apply this firewall rule applies. Please note that a blank source MAC address is equivalent to any.
Source Interface	Specify a source interface to which this firewall rule applies. This is the interface through which the traffic entered the Device. Please note that a blank source interface is equivalent to any.
Destination Interface	Specify a destination interface to which this firewall rule applies. This is the interface through which the traffic is destined to leave the Device. Please note that a blank source interface is equivalent to any.
Services	
Available Services	Select a service from the **Available Services** box.
Edit Customized Service	Click the **Edit Customized Service** button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
TCP Flag	Specify any TCP flag bits the firewall rule is to check for.
Schedule	Select the days and time during which to apply the rule. Select **Everyday** and **All Day** to always apply the rule.
OK	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

13.4.2 Customized Services

Configure customized services and port numbers not predefined by the Device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. Click the **Edit Customized Services** button while editing a firewall rule to configure a custom service port. This displays the following screen.

Figure 104 Security > Firewall > Rules: Edit: Edit Customized Services



The following table describes the labels in this screen.

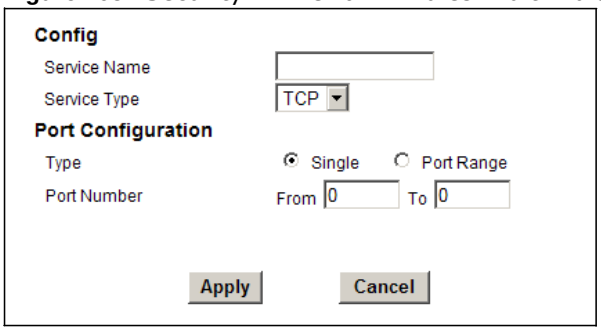
Table 59 Security > Firewall > Rules: Edit: Edit Customized Services

LABEL	DESCRIPTION
#	This is the number of your customized port.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol (**TCP** or **UDP**) that defines your customized service.
Port Type	This is the port number or range that defines your customized service.
Start Port	This is a single port number or the starting port number of a range that defines your customized service.
End Port	This is a single port number or the ending port number of a range that defines your customized service.
Modify	Click this to edit a customized service.
Add	Click this to configure a customized service.
OK	Click this to confirm and save your settings.

13.4.3 Customized Service Add/Edit

Use this screen to add a customized rule or edit an existing rule. Click **Add** or the **Edit** icon next to a rule number in the **Firewall Customized Services** screen to display the following screen.

Figure 105 Security > Firewall > Rules: Edit: Edit Customized Services: Add/Edit



The following table describes the labels in this screen.

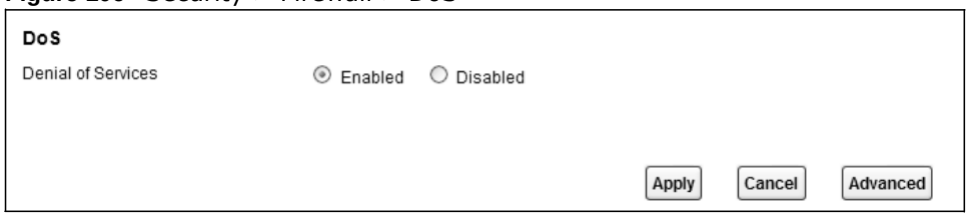
Table 60 Security > Firewall > Rules: Edit: Edit Customized Services: Add/Edit

LABEL	DESCRIPTION
Config	
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port (**TCP** or **UDP**) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click **Single** to specify one port only or **Port Range** to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
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.

13.5 The DoS Screen

Use this screen to enable DoS protection. Click **Security > Firewall > Dos** to display the following screen.

Figure 106 Security > Firewall > DoS



The following table describes the labels in this screen.

Table 61 Security > Firewall > DoS

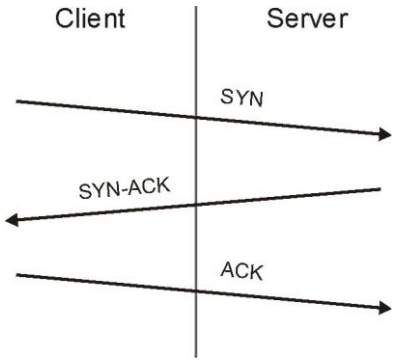
LABEL	DESCRIPTION
Denial of Services	Enable this to protect against DoS attacks. The Device will drop sessions that surpass maximum thresholds.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced	Click this to go to a screen to specify maximum thresholds at which the Device will start dropping sessions.

13.5.1 The DoS Advanced Screen

For DoS attacks, the Device 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 107 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.

13.5.1.1 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 Device has been receiving DoS attacks that are not recorded in the logs or the logs show that the Device 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.

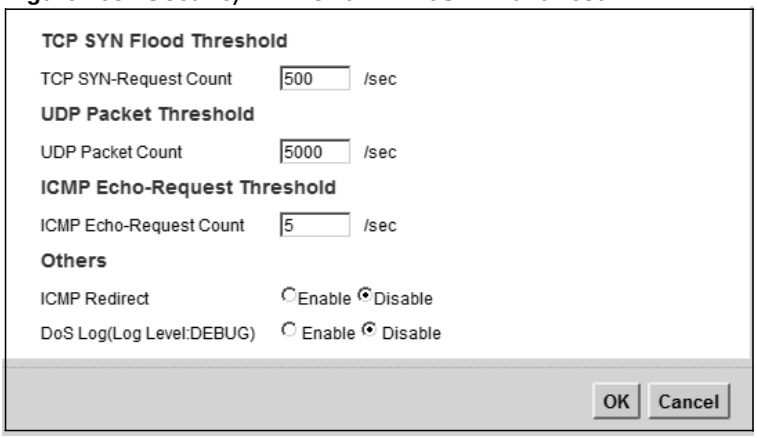
Reduce the threshold values if your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy).

- 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 Device may classify them as DoS attacks.

13.5.2 Configuring Firewall Thresholds

Click **Security > Firewall > DoS > Advanced** to display the following screen.

Figure 108 Security > Firewall > DoS > Advanced



The following table describes the labels in this screen.

Table 62 Security > Firewall > DoS > Advanced

LABEL	DESCRIPTION
TCP SYN-Request Count	This is the rate of new TCP half-open sessions per second that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the Device deletes half-open sessions as required to accommodate new connection attempts.
UDP Packet Count	This is the rate of new UDP half-open sessions per second that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the Device deletes half-open sessions as required to accommodate new connection attempts.
ICMP Echo-Request Count	This is the rate of new ICMP Echo-Request half-open sessions per second that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the Device deletes half-open sessions as required to accommodate new connection attempts.
ICMP Redirect	Select **Enable** to monitor for and block ICMP redirect attacks. An ICMP redirect attack is one where forged ICMP redirect messages can force the client device to route packets for certain connections through an attacker's host.
DoS Log(Log Level: DEBUG)	Select **Enable** to log DoS attacks. See Chapter 16 on page 173 for information on viewing logs.
Back	Click this button to return to the previous screen.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

13.6 Firewall Technical Reference

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

13.6.1 Firewall Rules Overview

Your customized rules take precedence and override the Device's default settings. The Device 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 Device 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 Router
- LAN to WAN
- WAN to LAN
- WAN to Router

Note: The LAN includes both the LAN port and the WLAN.

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

- LAN to Router

  These rules specify which computers on the LAN can manage the Device (remote management).

Note: You can also configure the remote management settings to allow only a specific computer to manage the Device.

- LAN to WAN

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

By default, the Device'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 Router

  By default the Device stops computers on the WAN from managing the Device. You could configure one of these rules to allow a WAN computer to manage the Device.

Note: You also need to configure the remote management settings to allow a WAN computer to manage the Device.

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 Device's default rules.

13.6.2 Guidelines For Enhancing Security With Your Firewall

6 Change the default password via web configurator.

7 Think about access control before you connect to the network in any way.

8 Limit who can access your router.

9 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.

10 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.

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

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

13.6.3 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the Device 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.

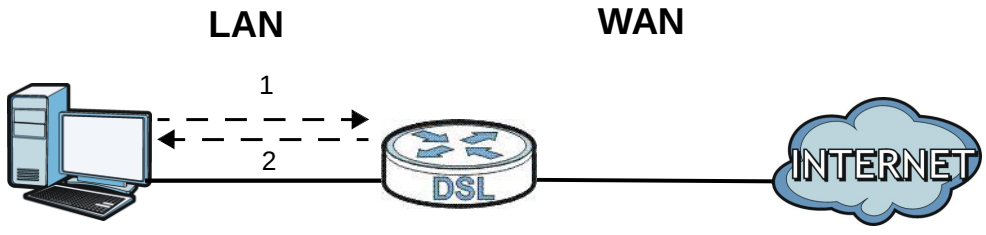
4 Does this rule conflict with any existing rules?

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.

13.6.4 Triangle Route

When the firewall is on, your Device acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the Device to protect your LAN against attacks.

Figure 109 Ideal Firewall Setup



13.6.4.1 The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. You may have more than one connection to the Internet (through one or more ISPs). If an alternate gateway is on the LAN (and its IP address is in the same subnet as the Device’s LAN IP address),

the "triangle route" (also called asymmetrical route) problem may occur. The steps below describe the "triangle route" problem.

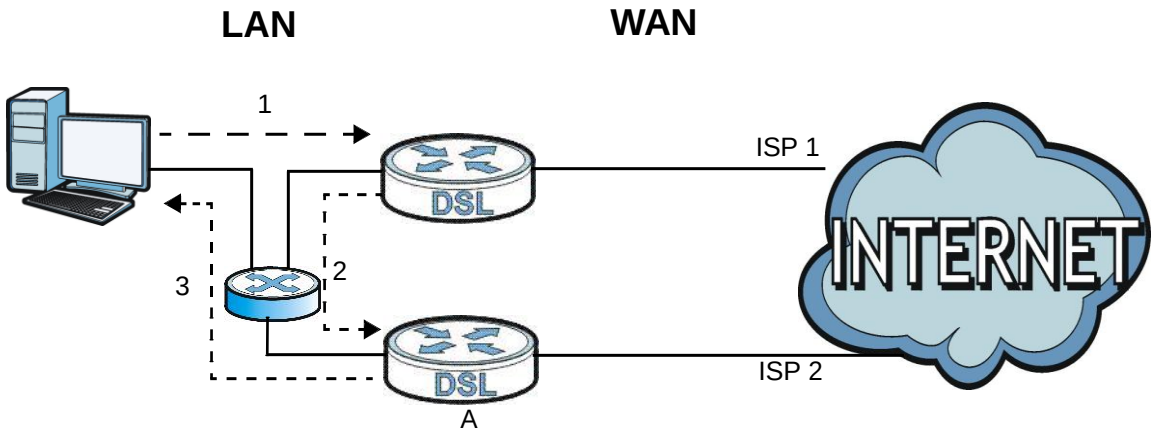
1 A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.

2 The Device reroutes the SYN packet through Gateway **A** on the LAN to the WAN.

3 The reply from the WAN goes directly to the computer on the LAN without going through the Device.

As a result, the Device resets the connection, as the connection has not been acknowledged.

Figure 110 "Triangle Route" Problem



13.6.4.2 Solving the "Triangle Route" Problem

If you have the Device allow triangle route sessions, traffic from the WAN can go directly to a LAN computer without passing through the Device and its firewall protection.

Another solution is to use IP alias. IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your Device supports up to three logical LAN interfaces with the Device being the gateway for each logical network.

It's like having multiple LAN networks that actually use the same physical cables and ports. By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the Device to your LAN. The following steps describe such a scenario.

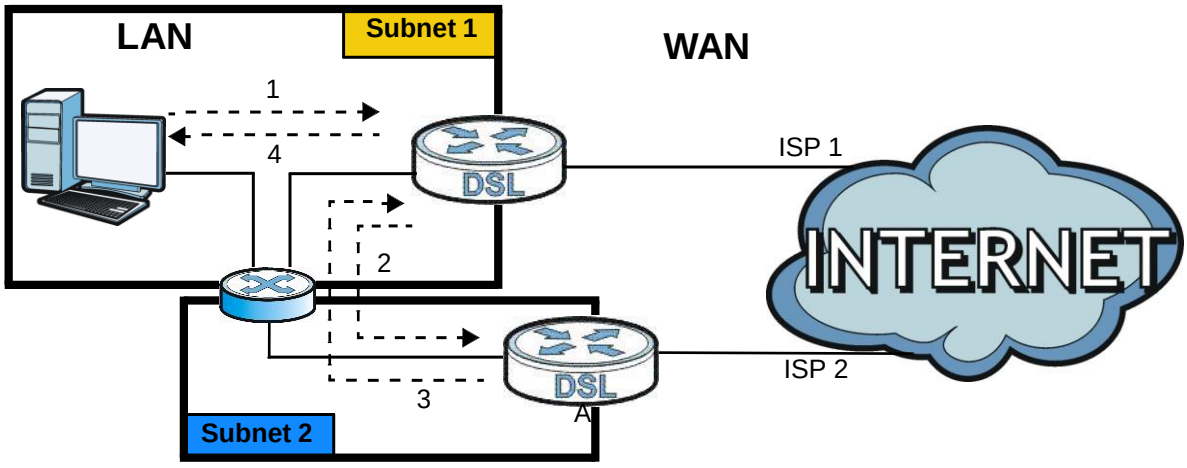
1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.

2 The Device reroutes the packet to Gateway A, which is in Subnet 2.

3 The reply from the WAN goes to the Device.

4 The Device then sends it to the computer on the LAN in Subnet 1.

Figure 111 IP Alias



14

Parental Control

14.1 Overview

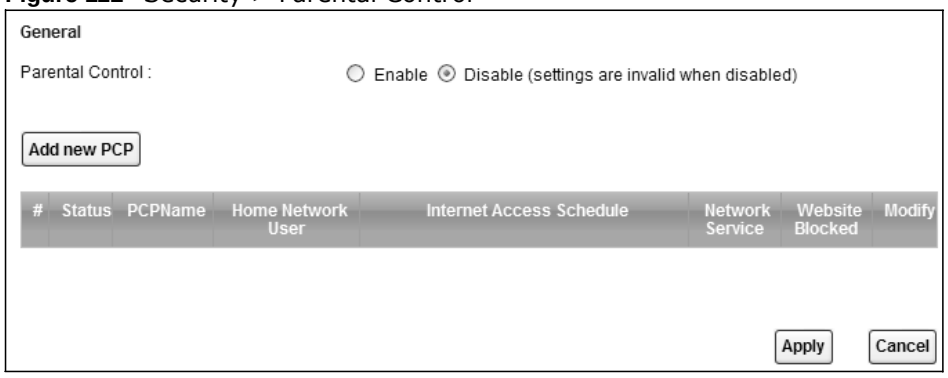
Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the Device performs parental control on a specific user.

14.2 The Parental Control Screen

Use this screen to enable parental control, view the parental control rules and schedules.

Click **Security > Parental Control** to open the following screen.

Figure 112 Security > Parental Control



The following table describes the fields in this screen.

Table 63 Security > Parental Control

LABEL	DESCRIPTION
Parental Control	Use this field to activate or deactivate parental control.
Add new PCP	Click this to create a new parental control rule.
#	This is the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
PCP Name	This shows the name of the rule.
Home Network User	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, **None** will be shown.

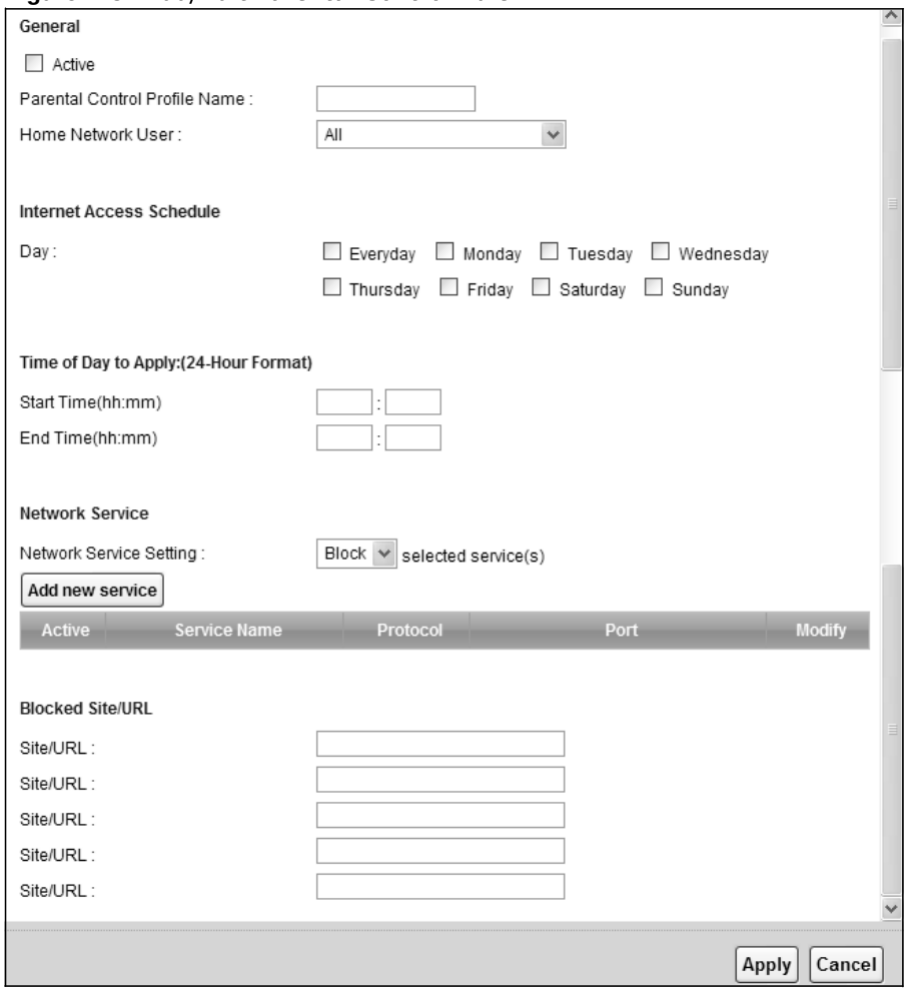
Table 63 Security > Parental Control (continued)

LABEL	DESCRIPTION
Website Blocked	This shows whether the website block is configured. If not, **None** will be shown.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

14.2.1 Add/Edit Parental Control Rule

Click **Add new PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 113 Add/Edit Parental Control Rule



The following table describes the fields in this screen.

Table 64 Parental Control: Add/Edit

LABEL	DESCRIPTION
General	
Active	Select the checkbox to activate this parental control rule.
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select **Custom**, enter the LAN user's MAC address. If you select **All**, the rule applies to all LAN users.
Internet Access Schedule	
Day	Select check boxes for the days that you want the Device to perform parental control.
Time of Day to Apply	Enter the starting and ending time that the LAN user is allowed access.
Network Service	
Network Service Setting	If you select **Block**, the Device prohibits the users from viewing the Web sites with the URLs listed below. If you select **Access**, the Device blocks access to all URLs except ones listed below.
Add new service	Click this to show a screen in which you can add a new service rule. You can configure the **Service Name**, **Protocol**, and **Name** of the new rule.
Active	This shows whether a configured service is activated or not.
Service Name	This shows the name of the rule.
Protocol	This shows the protocol of the rule.
Port	This shows the port of the rule.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Blocked Site/URL	Enter the URL of web sites or URL keywords to which the Device blocks access.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

15

Certificates

15.1 Overview

The Device 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.

15.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the Device's CA-signed certificates (Section 15.3 on page 167).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the Device (Section 15.4 on page 169).

15.2 What You Need to Know

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

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. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

Certificate File Format

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

- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

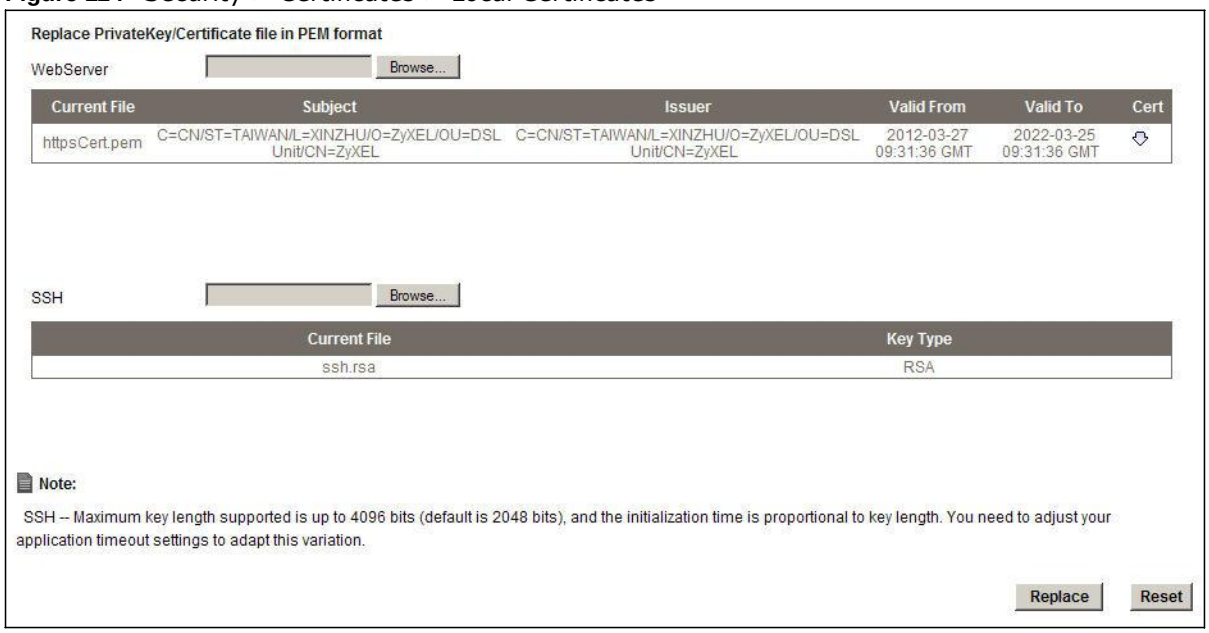
15.3 Local Certificates

Use this screen to view the Device's summary list of certificates and certification requests. You can import the following certificates to your Device:

- Web Server - This certificate secures HTTP connections.
- SSH - This certificate secures remote connections.

Click **Security > Certificates** to open the **Local Certificates** screen.

Figure 114 Security > Certificates > Local Certificates



The following table describes the labels in this screen.

Table 65 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
WebServer	Click **Browse...** to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
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.
Cert	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
SSH	Type in the location of the **SSH** certificate file you want to upload in this field or click **Browse** to find it.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.

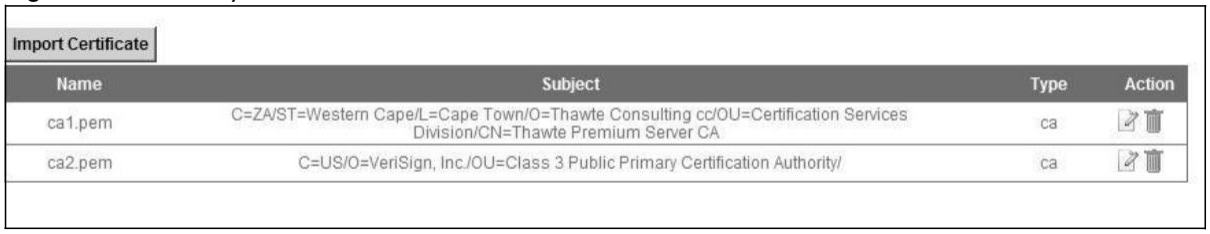
Table 65 Security > Certificates > Local Certificates (continued)

LABEL	DESCRIPTION
Key Type	This field applies to the **SSH** certificate. This shows the file format of the current certificate.
Replace	Click this to replace the certificate(s) and save your changes back to the Device.
Reset	Click this to clear your settings.

15.4 The Trusted CA Screen

Use this screen to view a summary list of certificates of the certification authorities that you have set the Device to accept as trusted. The Device 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 CA** to open the **Trusted CA** screen.

Figure 115 Security > Certificates > Trusted CA



The following table describes the fields in this screen.

Table 66 Security > Certificates > Trusted CA

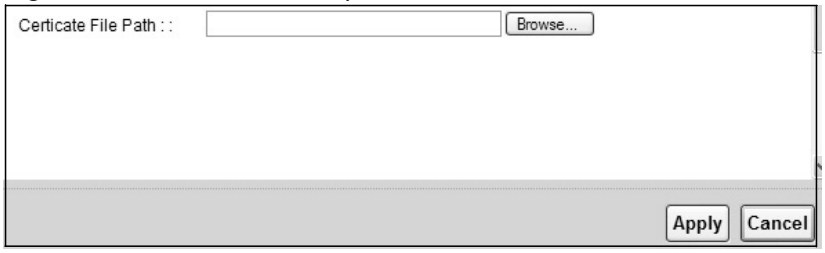
LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Device.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Action	Click **View** to open a screen with an in-depth list of information about the certificate. Click **Remove** to delete the certificate.

15.5 Trusted CA Import

Click **Import Certificate** in the **Trusted CA** screen to open the **Import Certificate** screen. You can save a trusted certification authority's certificate to the Device.

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

Figure 116 Trusted CA > Import



The following table describes the labels in this screen.

Table 67 Security > Certificates > Trusted CA > Import

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the Device.
Back	Click **Back** to return to the previous screen.

15.6 View Certificate

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 Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Click **Security** > **Certificates** > **Trusted CA** to open the **Trusted CA** screen. Click the **View** icon to open the **View Certificate** screen.

Figure 117 Trusted CA: View

The following table describes the labels in this screen.

Table 68 Trusted CA: View

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 Detail	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.

16 Log

16.1 Overview

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

16.1.1 What You Can Do in this Chapter

- Use the **Log** screen to see the system logs for the categories that you select (Section 16.2 on page 174).

16.1.2 What You Need To Know

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

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. 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.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 69 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.

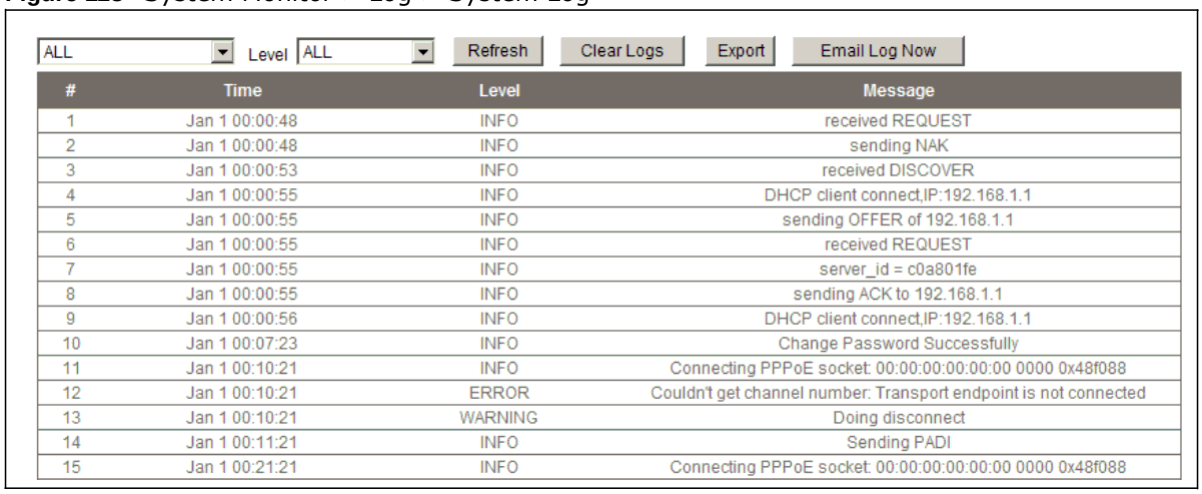
Table 69 Syslog Severity Levels

CODE	SEVERITY
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

16.2 The System Log Screen

Click **System Monitor > Log** to open the **System Log** screen. Use the **System Log** screen to see the system logs for the categories that you select in the upper left drop-down list box.

Figure 118 System Monitor > Log > System Log



The following table describes the fields in this screen.

Table 70 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Device searches through all logs of that severity or higher.
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.
Export	Click this to download logs to a file on your computer.
Email Log Now	Click this to send logs to a specified e-mail address.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Message	This field states the reason for the log.

17

Traffic Status

17.1 Overview

Use the **Traffic Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT.

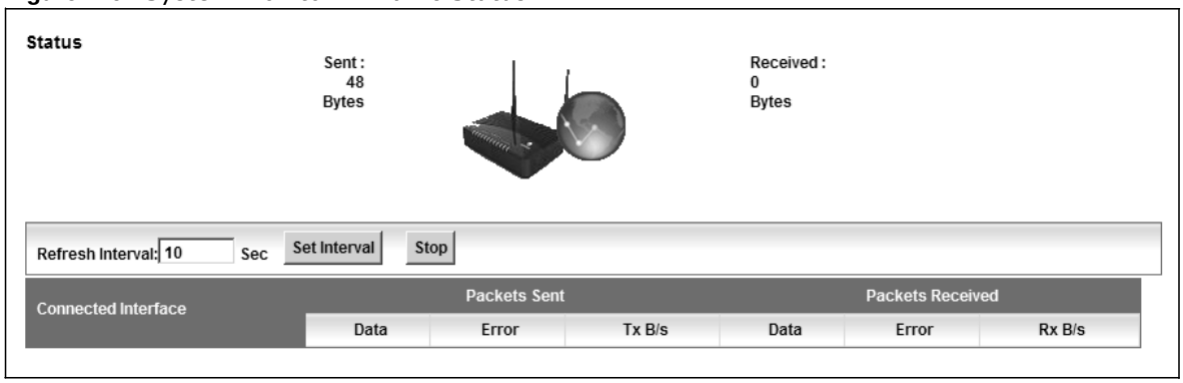
17.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 17.2 on page 175) .
- Use the **LAN** screen to view the LAN traffic statistics (Section 17.3 on page 176).
- Use the **NAT** screen to view the NAT status of the Device's client(s) (Section 17.4 on page 177).

17.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. You can view the WAN traffic statistics in this screen.

Figure 119 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 71 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Status	This shows the number of bytes received and sent through the WAN interface of the Device.
Refresh Interval	Enter how often you want the Device to update this screen from the drop-down list box.
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.
Connected Interface	This shows the name of the WAN interface that is currently connected.

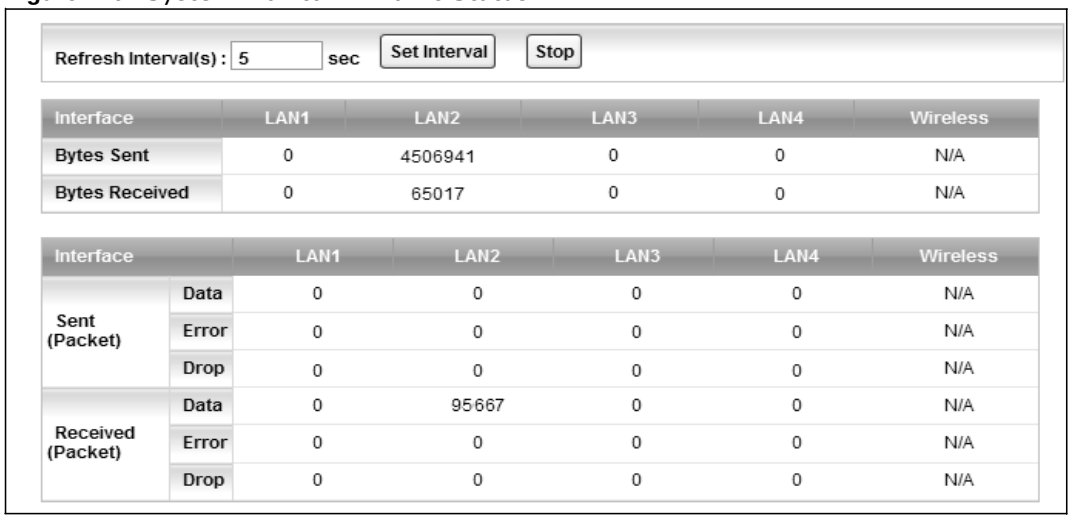
Table 71 System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

17.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. You can view the LAN traffic statistics in this screen.

Figure 120 System Monitor > Traffic Status > LAN



The following table describes the fields in this screen.

Table 72 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval(s)	Select how often you want the Device to update this screen from the drop-down list box.
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or WLAN interface.

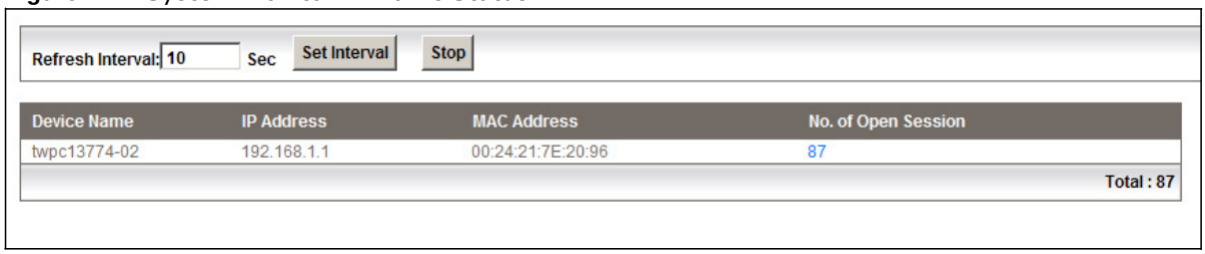
Table 72 System Monitor > Traffic Status > LAN (continued)

LABEL	DESCRIPTION
Sent (Packet)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packet)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

17.4 The NAT Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. You can view the NAT status of the Device's client(s) in this screen.

Figure 121 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

Table 73 System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.
Device Name	This shows the name of the client.
IP Address	This shows the IP address of the client.
MAC Address	This shows the MAC address of the client.
No. of Open Session	This shows the number of NAT sessions used by the client.

18

User Account

18.1 Overview

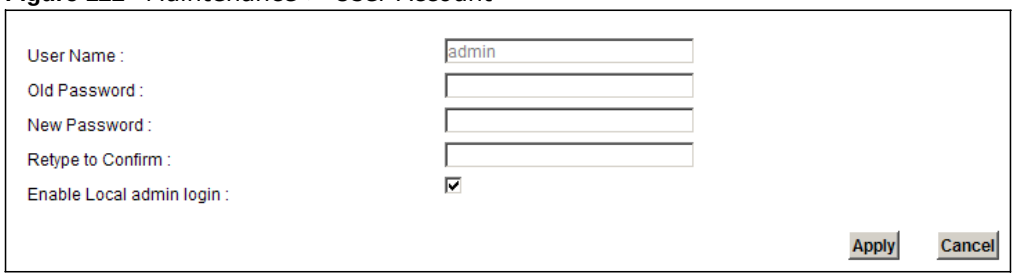
You can configure system password for different user accounts in the **User Account** screen.

18.2 The User Account Screen

Use the **User Account** screen to configure system password.

Click **Maintenance > User Account** to open the following screen.

Figure 122 Maintenance > User Account



The following table describes the labels in this screen.

Table 74 Maintenance > User Account

LABEL	DESCRIPTION
User Name	You can configure the password for the **Power User** and **Admin** accounts.
Old Password	Type the default password or the existing password you use to access the system in this field.
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 Device.
Retype to Confirm	Type the new password again for confirmation.
Enable Local admin login	Select this to enable local adminstrator login.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

19

System Setting

19.1 Overview

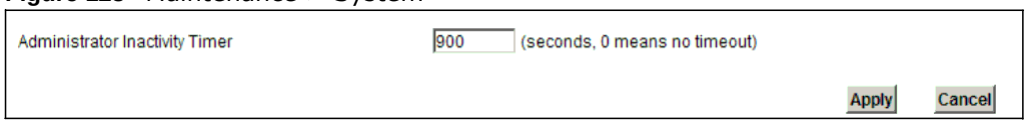
This chapter shows you how to configure the inactivity timeout interval.

19.2 The System Screen

Use this screen to configure system admin password.

Click **Maintenance > System** to open the screen as shown.

Figure 123 Maintenance > System



The following table describes the labels in this screen.

Table 75 Maintenance > System

LABEL	DESCRIPTION
Administrator Inactivity Timer	Type how many seconds a management session (either via the web configurator) can be left idle before the session times out and you have to log in again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

20

Time Setting

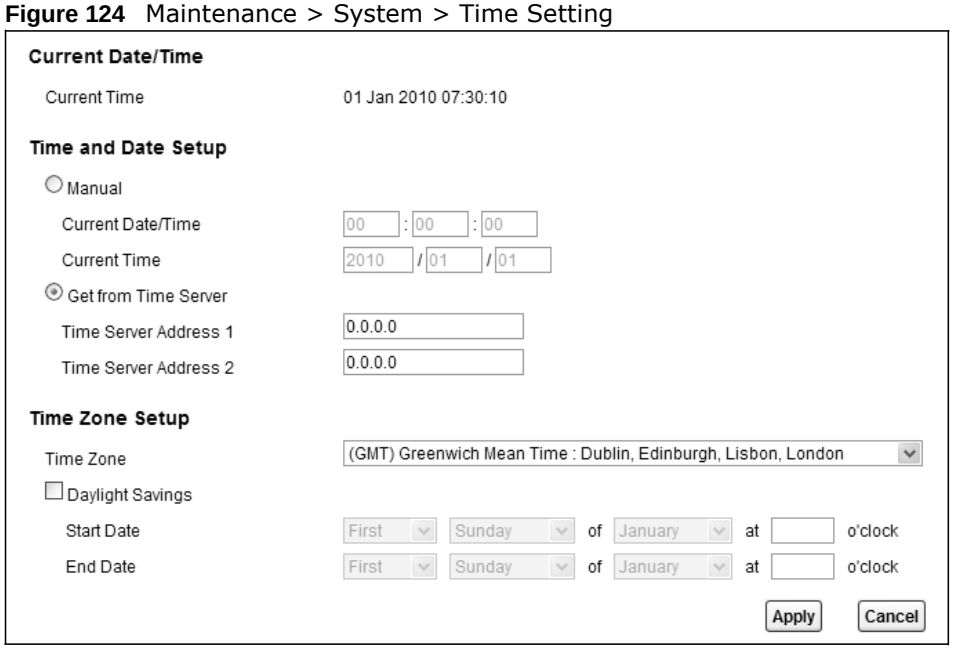
20.1 Overview

This chapter shows you how to configure the system time.

20.2 The Time Setting Screen

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

Figure 124 Maintenance > System > Time Setting



The following table describes the fields in this screen.

Table 76 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time and date of your Device. Each time you reload this page, the Device synchronizes the time and date with the time server.
Time and Date Setup	

Table 76 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
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.
Current Date/Time	This field displays the last updated time (in hh:mm:ss format) 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**.
Current Time	This field displays the last updated date (in yyyy/mm/dd format) 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 Device get the time and date from the time server you specified below.
Time Server Address 1/2	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).
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.

21

Log Setting

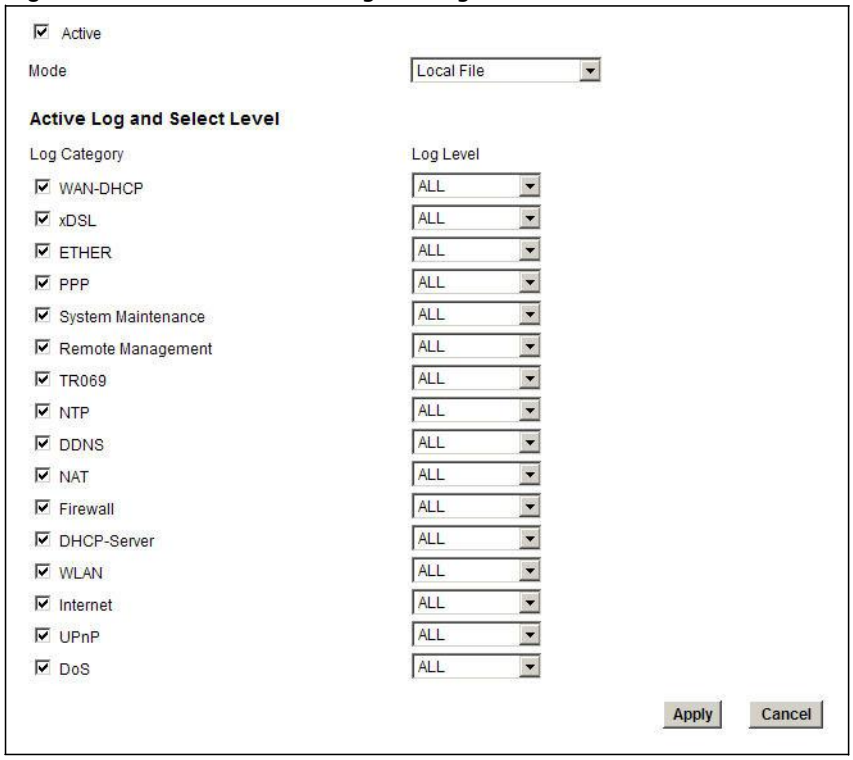
21.1 Overview

You can configure where the Device sends logs the Device records in the **Log Setting** screen.

21.2 The Log Setting Screen

To change your Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

Figure 125 Maintenance > Log Setting



The following table describes the fields in this screen.

Table 77 Maintenance > Log Setting

LABEL	DESCRIPTION
Active	Select the **Active** check box to enable logging.
Mode	Select the syslog destination from the drop-down list box. If you select **Local File**, the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select **Local File and Remote**.
E-mail Log Settings (The following fields will display if you select **Local File and Remote** in the **Mode** field.)	
SMTP Authentication	SMTP (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. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the E-mail logs.
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 system log e-mail message that the Device sends.
From	Specify where the logs are sent from.
To	The Device sends logs to the e-mail address specified in this field. If this field is left blank, the Device does not send logs via E-mail.
User Name	Enter the user name (up to 32 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Log Schedule	Specify the schedule for sending log. Specify days and times for sending logs in the following fields.
Day For Sending Log	Specify the day for sending log.
Time for Sending Log	Specify the time for sending log.
Clear log after sending mail	Select this to delete all the logs after the Device sends an E-mail of the logs.
Syslog Settings (The following fields will display if you select **Local File and Remote** in the **Mode** field.)	
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Syslog Server UDP Port	Enter the port number used by the syslog server.
Active Log and Alert	
Log Category	Select the categories of logs that you want to record.
Log Level	Select the log level. See Chapter 16 on page 173 for descriptions of log levels.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

22

Firmware Upgrade

22.1 Overview

This chapter explains how to upload new firmware to your Device. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

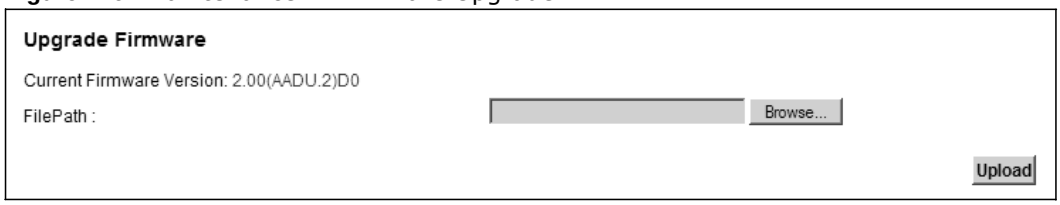
Only use firmware for your device's specific model. Refer to the label on the bottom of your Device.

22.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the Device while firmware upload is in progress!

Figure 126 Maintenance > Firmware Upgrade



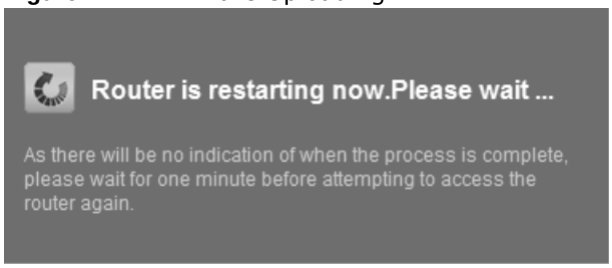
The following table describes the labels in this screen.

Table 78 Maintenance > Firmware Upgrade

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 **Browse ...** to find it.
Browse...	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 updating screen, wait two minutes before logging into the Device again.

Figure 127 Firmware Uploading



The Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 128 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 129 Error Message

23

Backup/Restore

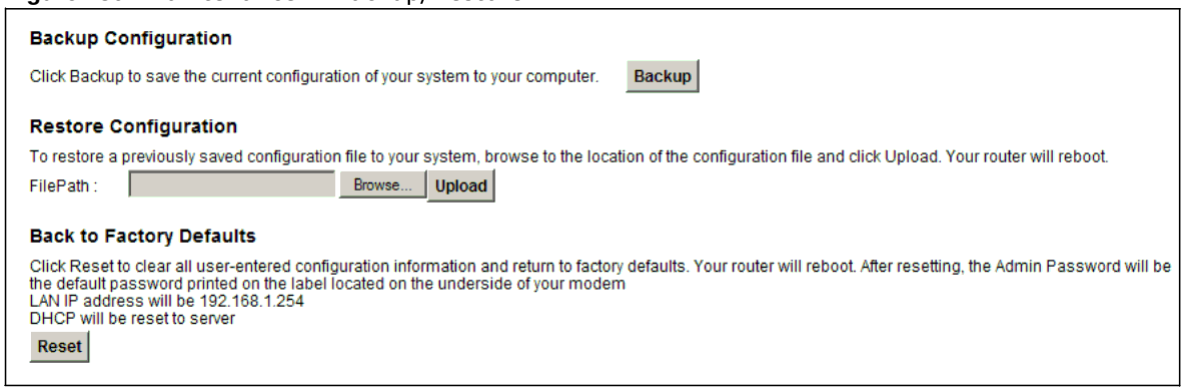
23.1 Overview

The **Backup/Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

23.2 The Backup/Restore Screen

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 130 Maintenance > Backup/Restore



Backup Configuration

Backup Configuration allows you to back up (save) the Device's current configuration to a file on your computer. Once your Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the Device's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your Device.

Table 79 Restore Configuration

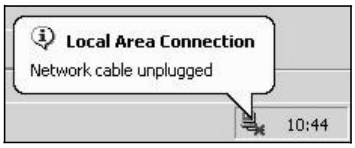
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.
Reset	Click this to reset your device settings back to the factory default.

Do not turn off the Device while configuration file upload is in progress.

After the Device configuration has been restored successfully, the login screen appears. Login again to restart the Device.

The Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 131 Network Temporarily Disconnected



If you restore the default configuration, 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 (192.168.1.254).

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Configuration** screen.

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the Device to its factory defaults. The following warning screen appears.

Figure 132 Reset Warning Message

Wait until the Device's login screen appears. You can also press the **RESET** button on the rear panel to reset the factory defaults of your Device. Refer to Section 1.5 on page 15 for more information on the **RESET** button.

23.3 The Reboot Screen

System restart allows you to reboot the Device remotely without turning the power off. You may need to do this if the Device hangs, for example.

Click **Maintenance > Reboot**. Click the **Reboot** button to have the Device reboot. This does not affect the Device's configuration.

24

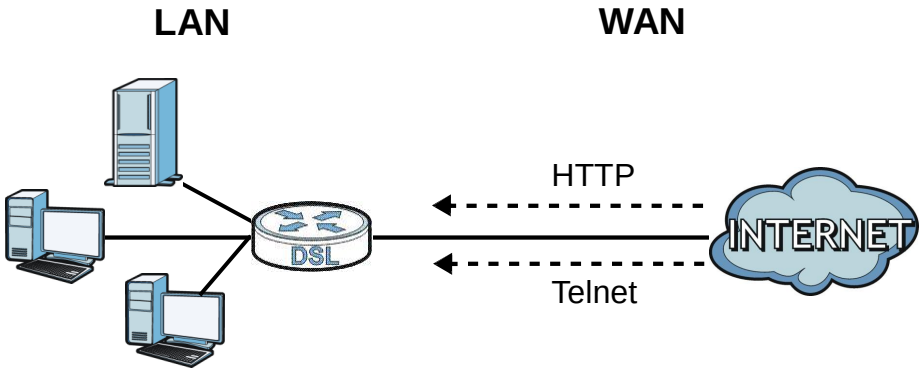
Remote Management

24.1 Overview

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

The following figure shows remote management of the Device coming in from the WAN.

Figure 133 Remote Management From the WAN



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

You may manage your Device from a remote location via:

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

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

24.1.1 What You Can Do in the Remote Management Screens

- Use the **WWW** screen (Section 24.2 on page 196) to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the Device.
- Use the **Telnet** screen (Section 24.3 on page 198) to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the Device.
- Use the **FTP** screen (Section 24.4 on page 199) to configure through which interface(s) and from which IP address(es) users can use FTP to access the Device.

- Your Device can act as an SNMP agent, which allows a manager station to manage and monitor the Device through the network. Use the **SNMP** screen (see Section 24.5 on page 199) to configure through which interface(s) and from which IP address(es) users can use SNMP to access the Device.
- Use the **DNS** screen (Section 24.6 on page 201) to configure through which interface(s) and from which IP address(es) users can send DNS queries to the Device.
- Use the **ICMP** screen (Section 24.7 on page 202) to set whether or not your Device will respond to pings and probes for services that you have not made available.
- Use the **SSH** screen (Section 24.8 on page 203) to configure through which interface(s) and from which IP address(es) users can use SSH to manage the Device.

24.1.2 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 Address** field does not match the client IP address. If it does not match, the Device will disconnect the session immediately.
- There is a firewall rule that blocks it.

Remote Management and NAT

When NAT is enabled:

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

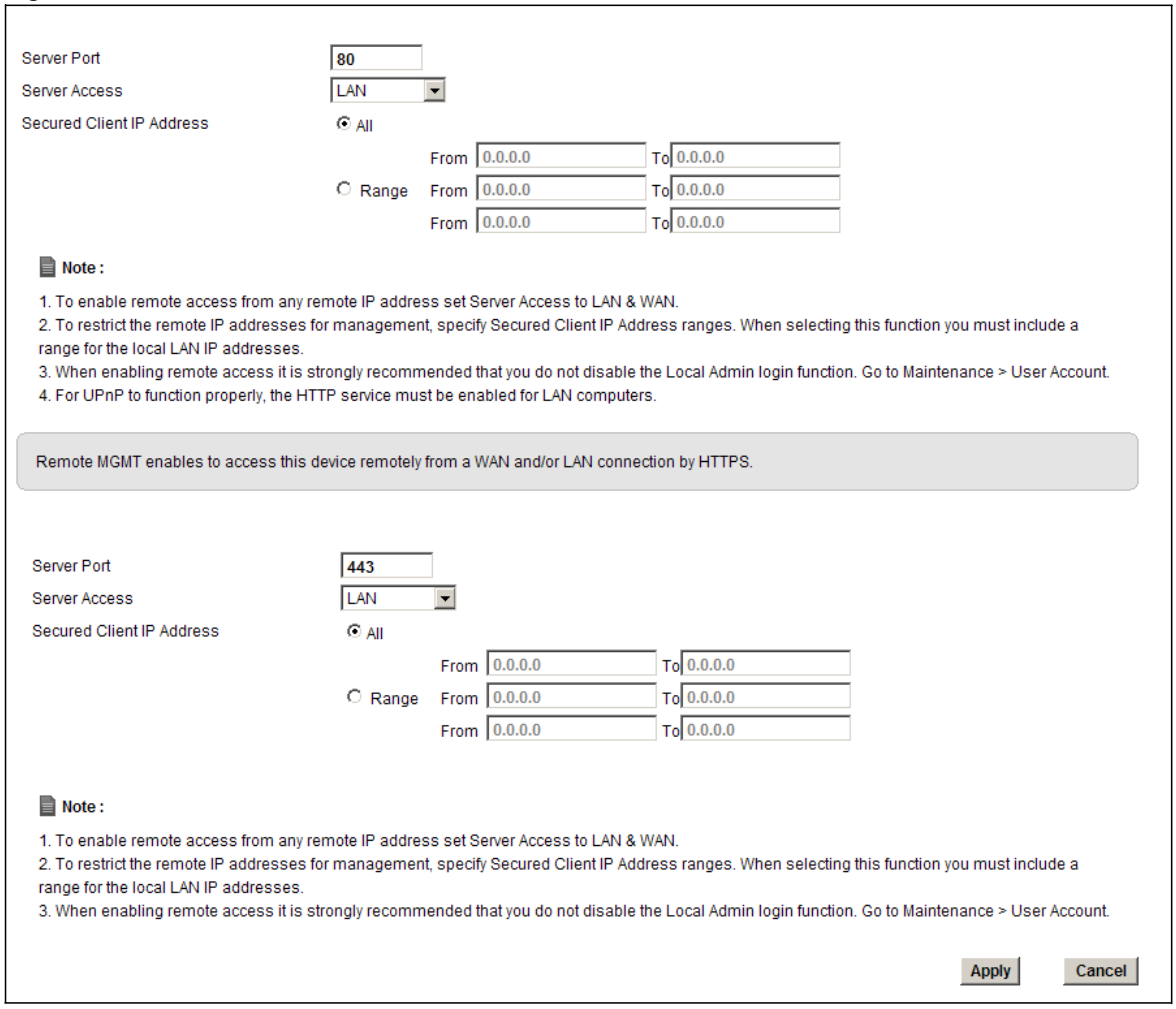
24.2 The WWW Screen

Use this screen to specify how to connect to the Device from a web browser, such as Internet Explorer.

24.2.1 Configuring the WWW Screen

Click **Maintenance > RemoteMGMT** to display the **WWW** screen.

Figure 134 Maintenance > RemoteMGMT > WWW



The following table describes the labels in this screen.

Table 80 Maintenance > RemoteMGMT > WWW

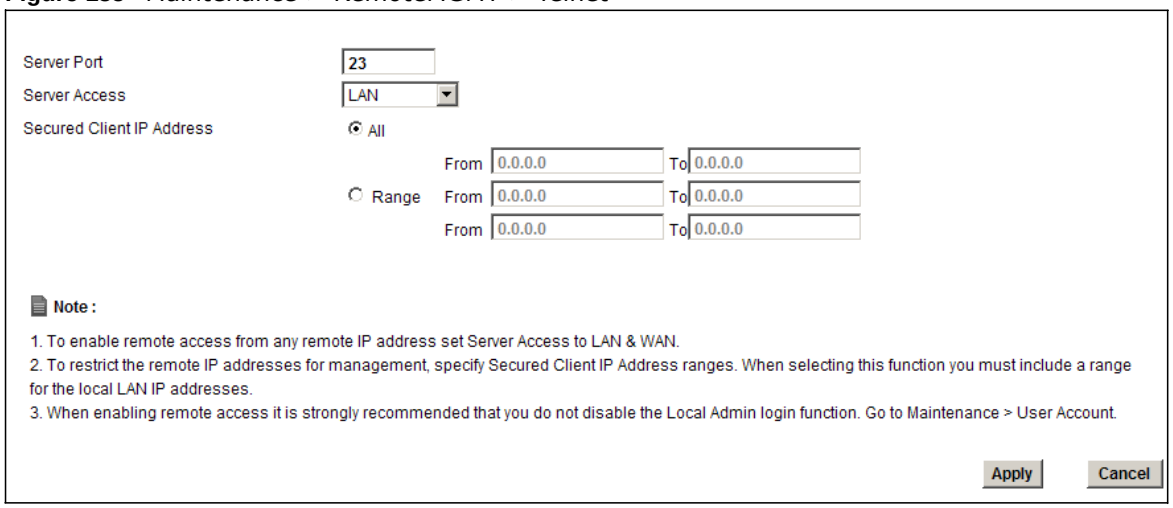
LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the Device using HTTP or HTTPS. If the number is grayed out, it is not editable.
Server Access	Select the interface(s) through which a computer may access the Device using this service. Note: It is recommended if you are allowing WAN access even temporarily to change the default password (in **Maintenance** > **User Account**). To allow access from the WAN, you will need to configure a WAN to Router firewall rule. See Section 3.7 on page 34 for information on configuring firewall rules.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the Device using this service. Select **All** to allow any computer to access the Device using this service. Choose **Range** to just allow the computer(s) with an IP address in the range that you specify to access the Device using this service.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

24.3 The Telnet Screen

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

Click **Maintenance > RemoteMGMT** > **Telnet** tab to display the screen as shown.

Figure 135 Maintenance > RemoteMGMT > Telnet



The following table describes the labels in this screen.

Table 81 Maintenance > RemoteMGMT > Telnet

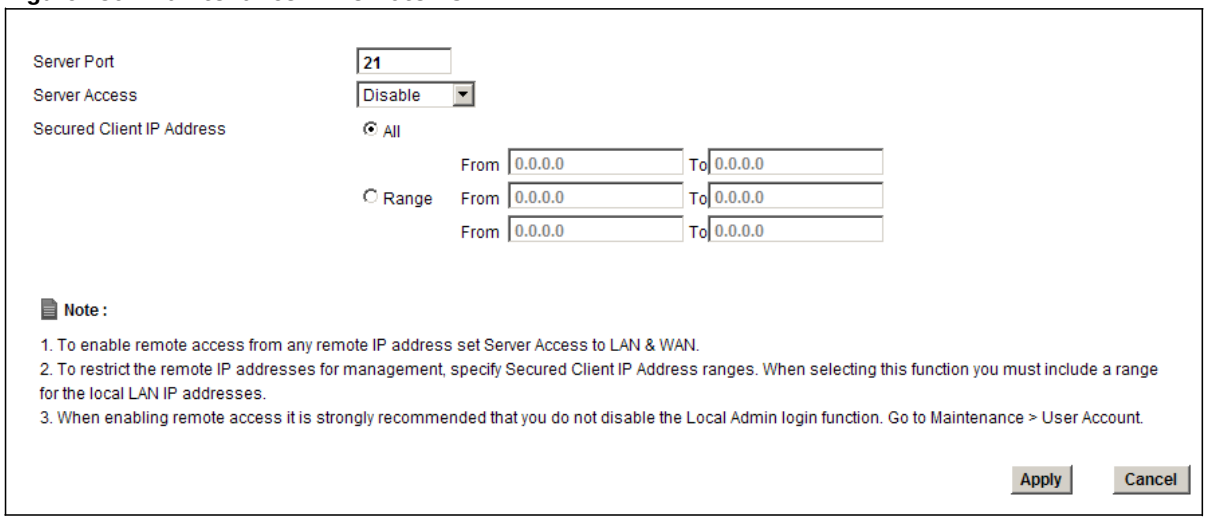
LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the Device. If the number is grayed out, it is not editable.
Server Access	Select the interface(s) through which a computer may access the Device using this service. Note: It is recommended if you are allowing WAN access even temporarily to change the default password (in **Maintenance** > **User Account**). To allow access from the WAN, you will need to configure a WAN to Router firewall rule. See Section 3.7 on page 34 for information on configuring firewall rules.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the Device using this service. Select **All** to allow any computer to access the Device using this service. Choose **Range** to just allow the computer(s) with an IP address in the range that you specify to access the Device using this service.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

24.4 The FTP Screen

You can use FTP (File Transfer Protocol) to upload and download the Device's firmware and configuration files. Please see the User's Guide chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

Use this screen to specify which interfaces allow FTP access and from which IP address the access can come. To change your Device's FTP settings, click **Maintenance > RemoteMGMT** > **FTP**. The screen appears as shown.

Figure 136 Maintenance > RemoteMGMT > FTP



The following table describes the labels in this screen.

Table 82 Maintenance > RemoteMGMT > FTP

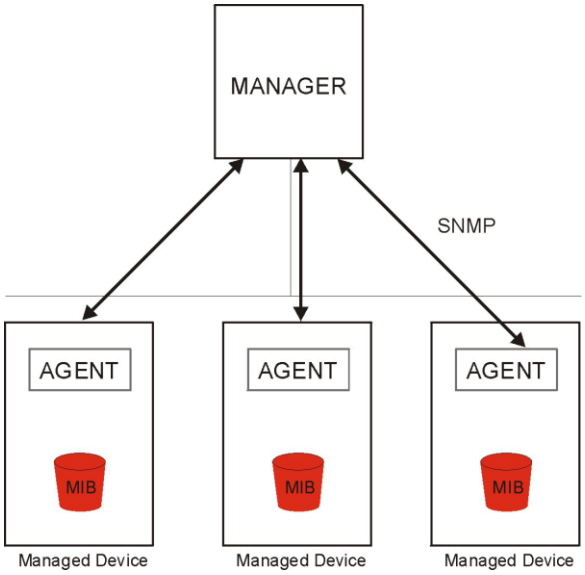
LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the Device. If the number is grayed out, it is not editable.
Server Access	Select the interface(s) through which a computer may access the Device using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the Device using this service. Select **All** to allow any computer to access the Device using this service. Choose **Range** to just allow the computer(s) with an IP address in the range that you specify to access the Device using this service.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

24.5 The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Device through the network. The Device supports SNMP version

one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 137 SNMP Management Model



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

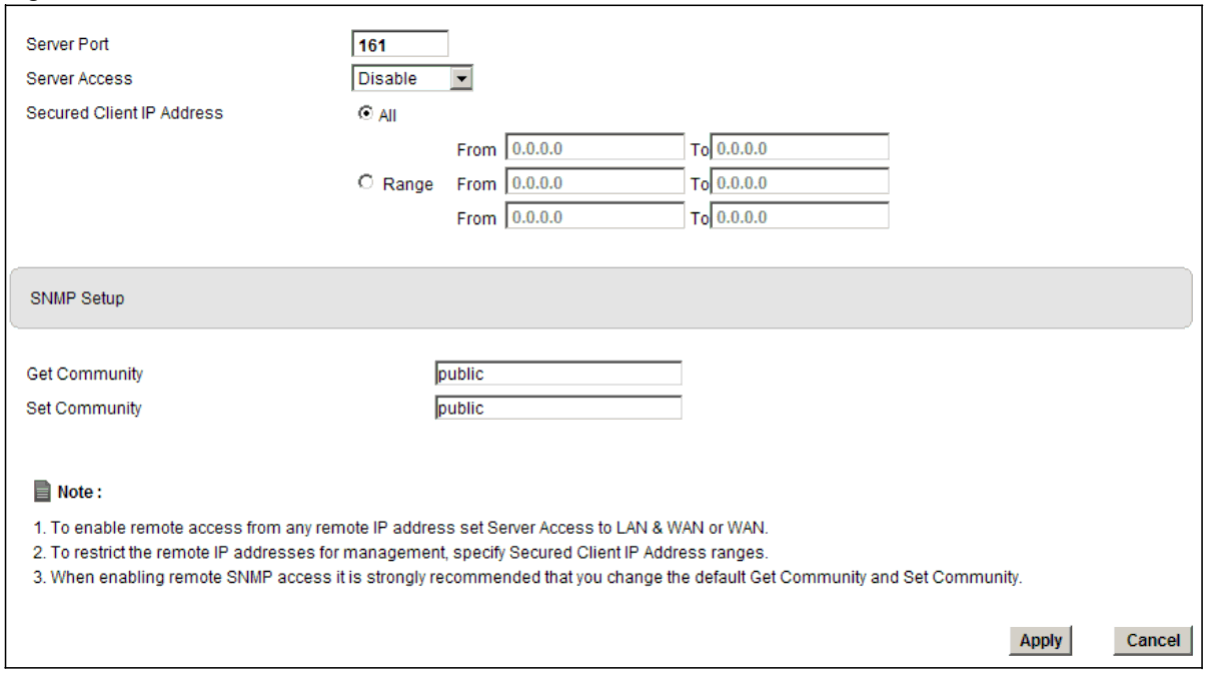
An agent is a management software module that resides in a managed device (the Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. 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.

24.5.1 Configuring SNMP

To change your Device's SNMP settings, click **Maintenance > RemoteMGMT** > **SNMP** tab. The screen appears as shown.

Figure 138 Maintenance > RemoteMGMT > SNMP



The following table describes the labels in this screen.

Table 83 Maintenance > RemoteMGMT > SNMP

LABEL	DESCRIPTION
Server Port	This displays the port the SNMP agent listens on. If the number is grayed out, it is not editable.
Server Access	Select the interface(s) through which a computer may access the Device using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to access the SNMP agent on the Device. Select **All** to allow any computer to access the SNMP agent. Choose **Range** to just allow the computer(s) with an IP address in the range that you specify to access the Device using this service.
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.
Apply	Click **Apply** to save your changes back to the Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

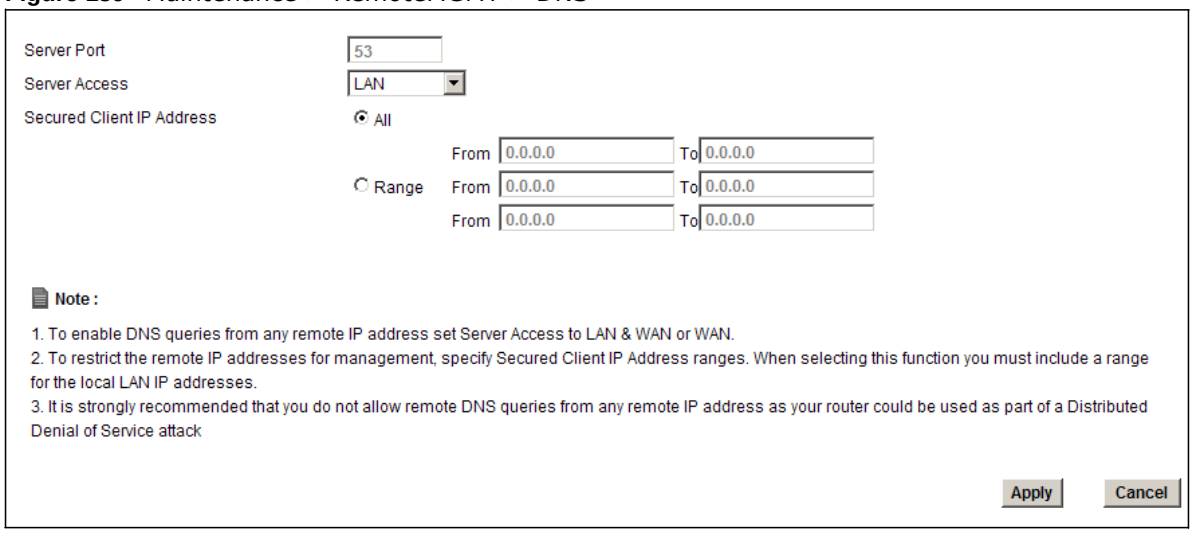
24.6 The DNS Screen

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa.

Use this screen to set from which IP address the Device will accept DNS queries and on which interface it can send them your Device's DNS settings. This feature is not available when the Device

is set to bridge mode. Click **Maintenance > RemoteMGMT** > **DNS** to change your Device's DNS settings.

Figure 139 Maintenance > RemoteMGMT > DNS



The following table describes the labels in this screen.

Table 84 Maintenance > RemoteMGMT > DNS

LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the Device. If the number is grayed out, it is not editable.
Access Status	Select the interface(s) through which a computer may send DNS queries to the Device.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to send DNS queries to the Device. Select **All** to allow any computer to send DNS queries to the Device. Choose **Range** to just allow the computer(s) with an IP address in the range that you specify to send DNS queries to the Device.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

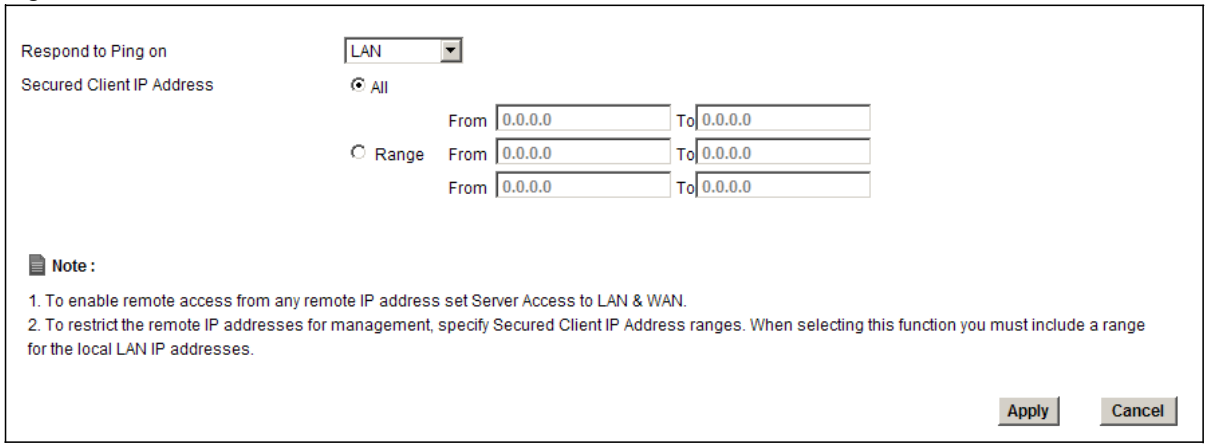
24.7 The ICMP Screen

To change your Device's security settings, click **Maintenance > RemoteMGMT** > **ICMP**. The screen appears as shown.

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

Note: If you want your device to respond to pings and requests for unauthorized services, you will also need to configure the firewall accordingly by disabling SPI.

Figure 140 Maintenance > RemoteMGMT > ICMP



The following table describes the labels in this screen.

Table 85 Maintenance > RemoteMGMT > ICMP

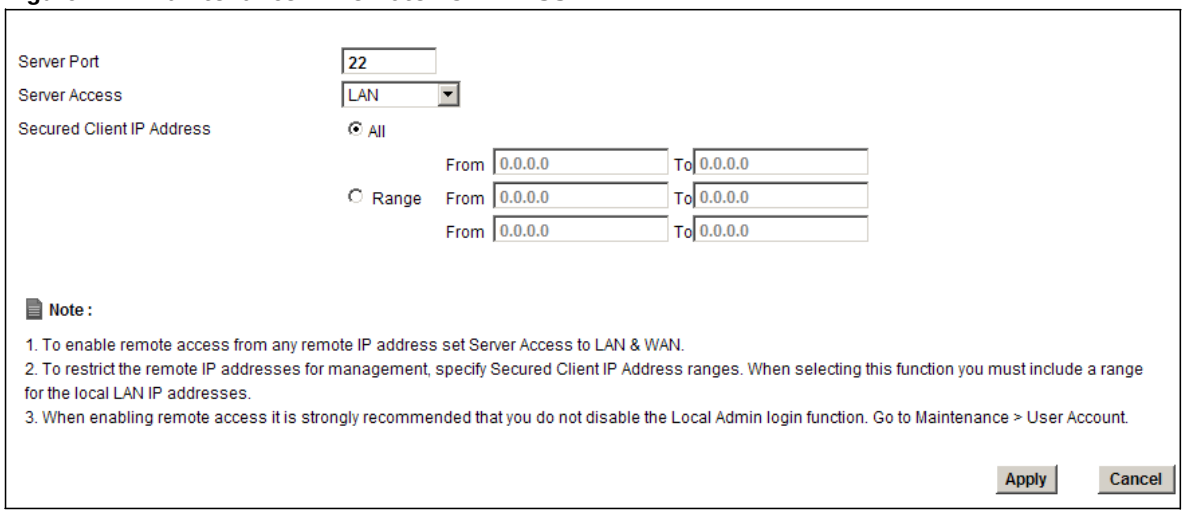
LABEL	DESCRIPTION
Respond to Ping on	The Device will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to send Ping requests to the Device. Select **All** to allow any computer to send Ping requests to the Device. Choose **Range** to just allow the computer(s) with an IP address in the range that you specify to send Ping requests to the Device.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

24.8 The SSH Screen

You can use Secure SHell (SSH) to securely access the Device's command line interface. Specify which interfaces allow SSH access and from which IP address the access can come. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Click **Maintenance > RemoteMGMT** > **SSH** tab to display the screen as shown.

Figure 141 Maintenance > RemoteMGMT > SSH



The following table describes the labels in this screen.

Table 86 Maintenance > RemoteMGMT > SSH

LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the Device. If the number is grayed out, it is not editable.
Server Access	Select the interface(s) through which a computer may access the Device using this service. Note: It is recommended if you are allowing WAN access even temporarily to change the default password (in **Maintenance** > **User Account**). To allow access from the WAN, you will need to configure a WAN to Router firewall rule. See Section 3.7 on page 34 for information on configuring firewall rules.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the Device using this service. Select **All** to allow any computer to access the Device using this service. Choose **Range** to just allow the computer(s) with an IP address in the range that you specify to access the Device using this service.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

25

Diagnostic

25.1 Overview

These read-only screens display information to help you identify problems with the Device.

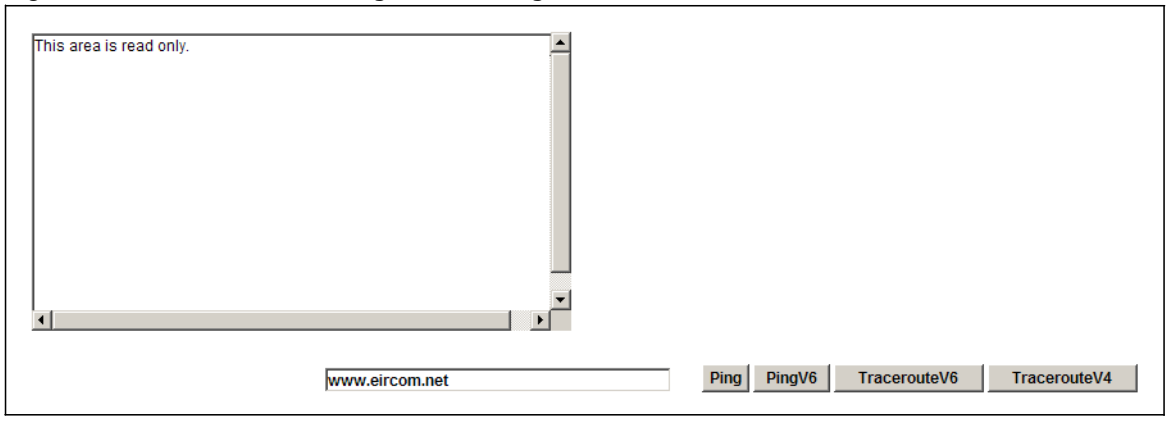
25.1.1 What You Can Do in the Diagnostic Screens

- Use the **Ping** screen (Section 25.2 on page 205) to ping an IP address.
- Use the **DSL Line** screen (Section 25.3 on page 206) to view the DSL line statistics and reset the ADSL line.

25.2 The General Screen

Use this screen to ping an IP address. Click **Maintenance > Diagnostic > Ping** to open the screen shown next.

Figure 142 Maintenance > Diagnostic > Ping



The following table describes the fields in this screen.

Table 87 Maintenance > Diagnostic > Ping

LABEL	DESCRIPTION
	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this to ping the IP address that you entered.
PingV6	Click this to ping the IPv6 address that you entered.

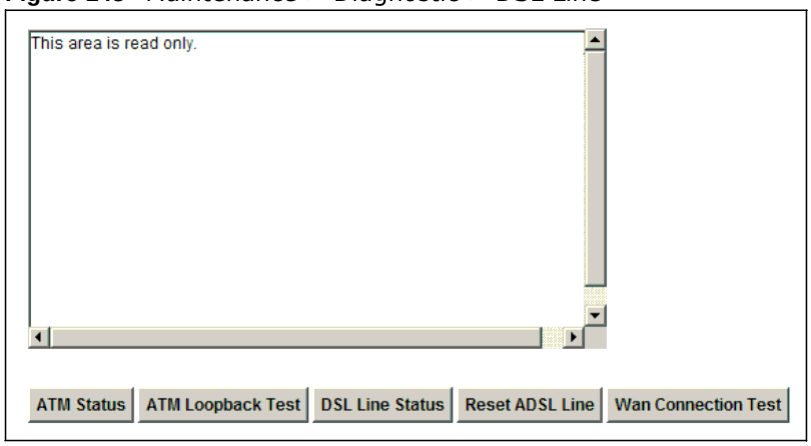
Table 87 Maintenance > Diagnostic > Ping (continued)

LABEL	DESCRIPTION
TracerouteV6	Click this to display the route path and transmission delays between the Device to the IPv6 address that you entered.
TracerouteV4	Click this to display the route path and transmission delays between the Device to the IPv4 address that you entered.

25.3 The DSL Line 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 143 Maintenance > Diagnostic > DSL Line



The following table describes the fields in this screen.

Table 88 Maintenance > Diagnostic > DSL Line

LABEL	DESCRIPTION
ATM Status	Click this to view your DSL connection's Asynchronous Transfer Mode (ATM) statistics. ATM is a 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. The (Segmentation and Reassembly) SAR driver translates packets into ATM cells. It also receives ATM cells and reassembles them into packets. These counters are set back to zero whenever the device starts up. **inPkts** is the number of good ATM cells that have been received. **inDiscards** is the number of received ATM cells that were rejected. **inF4Pkts** is the number of ATM Operations, Administration, and Management (OAM) F4 cells that have been received. See ITU recommendation I.610 for more on OAM for ATM. **inF5Pkts** is the number of ATM OAM F5 cells that have been received. **outPkts** is the number of ATM cells that have been sent. **outDiscards** is the number of ATM cells sent that were rejected. **outF4Pkts** is the number of ATM OAM F4 cells that have been sent. **outF5Pkts** is the number of ATM OAM F5 cells that have been sent.
ATM Loopback Test	Click this to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.
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 Device 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 Device is using to transmit to the ISP. **attenuation downstream** is the reduction in amplitude (in decibels) of the DSL signal coming into the Device 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.
Reset ADSL Line	Click this to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
WAN Connection Test	Click this to check your WAN connection status of DSL, ATM, Ethernet PPPoE, IP, and Pinging.

26

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
- Device Access and Login
- Internet Access

26.1 Power, Hardware Connections, and LEDs

The Device does not turn on. None of the LEDs turn on.

1. Make sure the Device is turned on.
2. Make sure you are using the power adaptor or cord included with the Device.
3. Make sure the power adaptor or cord is connected to the Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the Device 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 27.1 on page 213.
2. Check the hardware connections.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the Device off and on.
5. If the problem continues, contact the vendor.

26.2 Device Access and Login

I forgot the IP address for the Device.

1. The default IP address is **192.168.1.254**.
2. If you changed the IP address and have forgotten it, you might get the IP address of the Device 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 Device (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 15.

I forgot the password.

1. The default admin user name and password can be found on the cover of this User's Guide.
2. If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 15.

I cannot see or access the **Login** screen for the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.254.
   - If you changed the IP address (Section 6.2 on page 79), 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 Device.
2. Check the hardware connections, and make sure the LEDs are behaving as expected.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
4. Reset the device to its factory defaults, and try to access the Device with the default IP address. See Section 1.5 on page 15.
5. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

   Advanced Suggestions

- Try to access the Device using another service, such as Telnet. If you can access the Device, check the remote management settings and firewall rules to find out why the Device does not respond to HTTP.
- If your computer is connected to the **DSL** port or is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the Device.

1. Make sure you have entered the password correctly. The default user and default admin password can be found on the cover page of this User's Guide. 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 Device. Log out of the Device in the other session, or ask the person who is logged in to log out.
3. Turn the Device 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 15.

I cannot Telnet to the Device.

See the troubleshooting suggestions for I cannot see or access the Login screen for 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 for the web configurator. Ignore the suggestions about your browser.

26.3 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 27.1 on page 213.
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 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

4 If you are trying to access the Internet wirelessly, make sure you enabled the wireless LAN and have selected the correct country and channel in which your Device operates in the **Wireless LAN > AP** screen.

5 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the Device), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected.

2 Turn the Device 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 27.1 on page 213. If the Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Check the signal strength. If the signal strength is low, try moving your computer closer to the Device if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 Turn the Device off and on.

4 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.

27

LED Descriptions

27.1 LED Descriptions

Table 89 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
USB	Green	On	The Device recognizes a USB connection through the USB slot.
		Blinking	The Device is sending/receiving data to /from the USB device connected to it.
POWER	Green	On	The Device is receiving power and ready for use.
		Blinking	The Device is self-testing.
	Red	On	The Device detected an error while self-testing, or there is a device malfunction.
		Off	The Device is not receiving power.
ETHERNET 1-4	Green	On	The Device has an Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The Device is sending/receiving data to /from the LAN.
		Off	The Device does not have an Ethernet connection with the LAN.
WiFi	Green	On	The wireless network is activated.
		Blinking	The Device is communicating with other wireless clients.
	Orange	Blinking	The Device is setting up a WPS connection.
		Off	The wireless network is not activated.
DSL	Green	On	The DSL line is up.
		Blinking	The Device is initializing the DSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The Device is sending or receiving IP traffic.
	Red	On	The Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The Device does not have an IP connection.

A

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.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

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.

Regulatory Information

European Union

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.

[German]	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.

CE

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2, 4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries inwhich additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "*Overview of Regulatory Requirements for Wireless LANs*":.

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP)[1] (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		V
5150-5350	200	V	
5470-5725	1000		V

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

France

For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483.5 MHz. There are no restrictions when used indoors or in other parts of the 2.4 GHz band. Check http://www.arcep.fr/ for more details.

Pour la bande 2.4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483.5 MHz. Il n'y a pas de restrictions pour des utilisations en intérieur ou dans d'autres parties de la bande 2.4 GHz. Consultez http://www.arcep.fr/ pour de plus amples détails.

R&TTE 1999/5/EC		
WLAN 2.4 – 2.4835 GHz		
IEEE 802.11 b/g/n		
Location	Frequency Range (GHz)	Power (EIRP)
Indoor (No restrictions)	2.4 – 2.4835	100mW (20dBm)
Outdoor	2.4 – 2.454	100mW (20dBm)
	2.454 – 2.4835	10mW (10dBm)

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

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.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- 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.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. 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.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- This product is for indoor use only (utilisation intérieure exclusivement).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index

Numbers

A

B

C

D

E

F

H

I

L

M

N

P

Q

R

S

T

U

V

W