# eircom F1000 modem

Wireless N VDSL2 VoIP Combo WAN Gigabit IAD

Version 1.00
Edition 1, 6/2013

# User's Guide

| Default Login Details | |
|---|---|
| LAN IP Address | http://192.168.1.254 |
| Login | admin |
| Password | Default password is the wireless key printed on the back of the Device. |

**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.

# Contents Overview

# Table of Contents

# PART I
# User's Guide

# 1

# Introducing the Device

## 1.1 Overview

The Device is a wireless VDSL router and Gigabit Ethernet gateway. It has a DSL port and a Gigabit Ethernet port for super-fast Internet access. The Device supports both Packet Transfer Mode (PTM) and Asynchronous Transfer Mode (ATM). It is backward compatible with ADSL, ADSL2 and ADSL2+ in case VDSL is not available.

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

The Device has two USB ports for sharing files via a USB storage device, sharing a USB printer, or connecting a 3G dongle for a WAN backup connection.

The Device works over the analog telephone system, POTS (Plain Old Telephone Service).

## 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.
- 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.

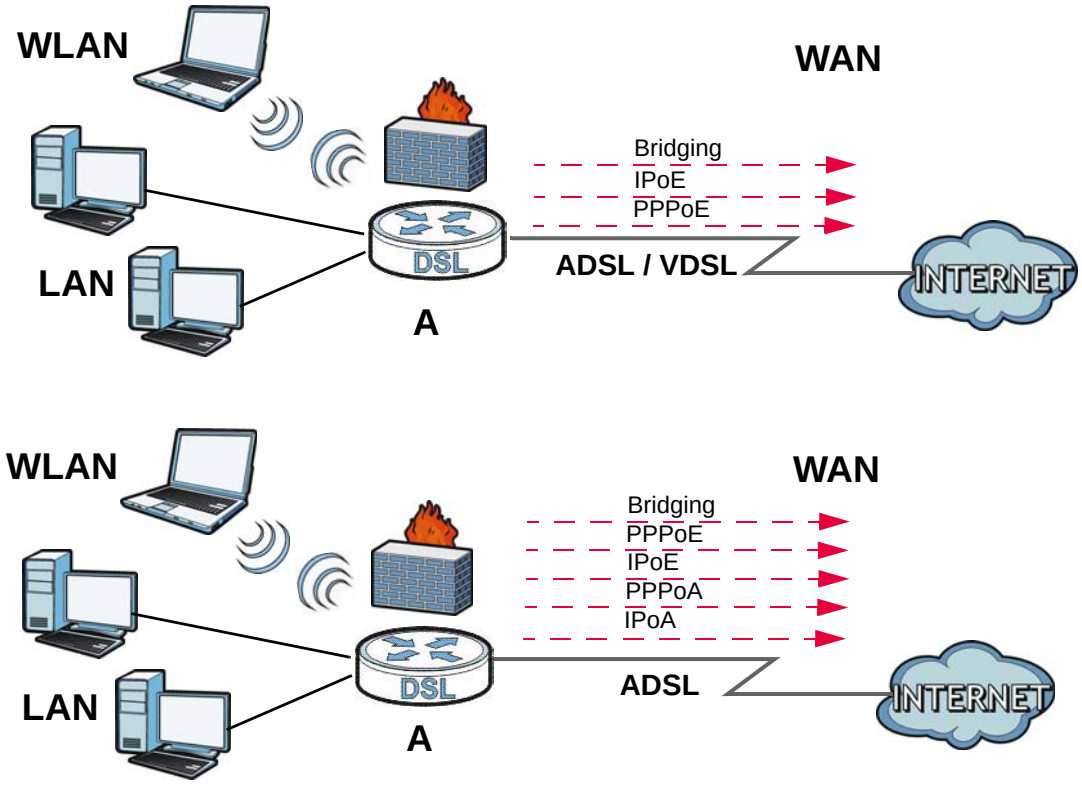
## 1.4.1 Internet Access

Your Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. You can have multiple WAN services over one ADSL or VDSL. The Device cannot work in ADSL and VDSL mode at the same time.

Note: The ADSL and VDSL lines share the same WAN (layer-2) interfaces that you configure in the Device. Refer to Section 4.2 on page 45 for the **Network Setting > Broadband** screen.

Computers can connect to the Device's LAN ports (or wirelessly).

**Figure 1** Device's Internet Access Application




You can also configure IP filtering on the Device for secure Internet access. When the IP filter is on, all incoming traffic from the Internet to your network is blocked by default 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.

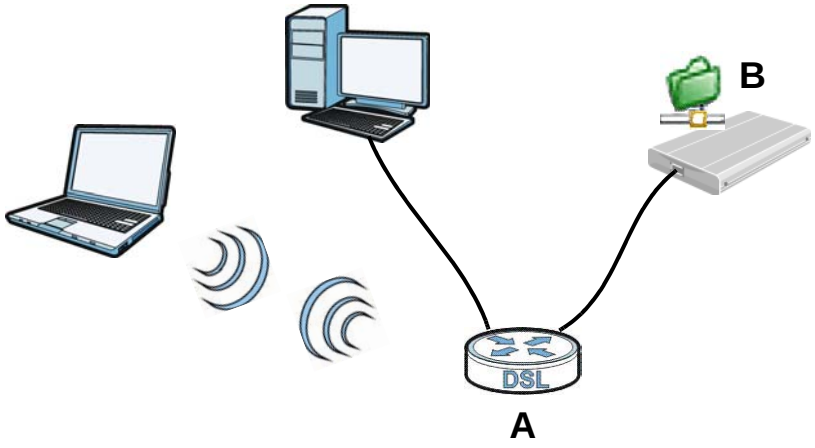
## 1.4.2 Device's USB Support

The USB port of the Device is used for file-sharing, media server and printer-sharing.

### File Sharing

Use the built-in USB 2.0 port to share files on a USB memory stick or a USB hard drive (**B**). You can connect one USB hard drive to the Device at a time. Use FTP to access the files on the USB device.

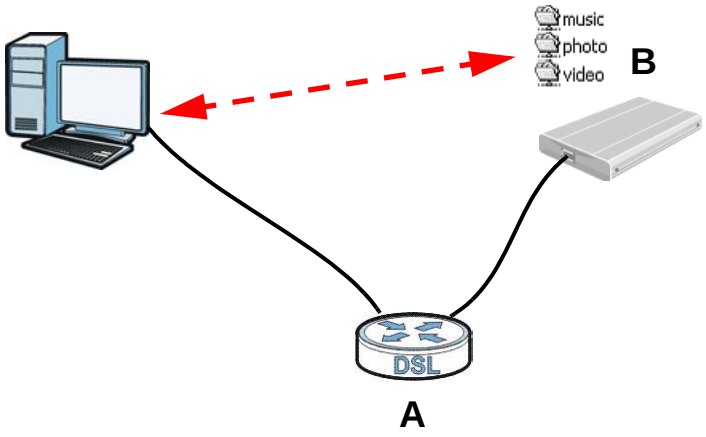
**Figure 2** USB File Sharing Application




### Media Server

You can also use the Device as a media server. This lets anyone on your network play video, music, and photos from a USB device (**B**) connected to the Device's USB port (without having to copy them to another computer).

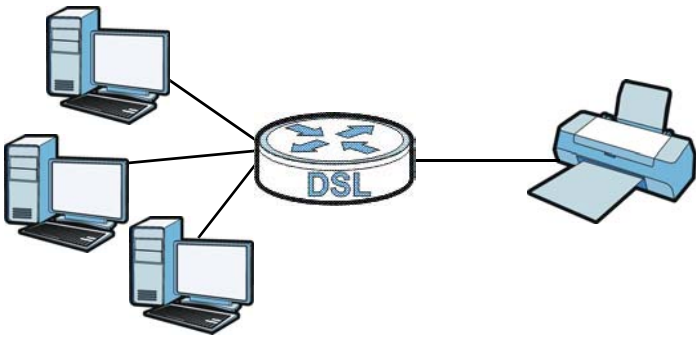
**Figure 3** USB Media Server Application



### Printer 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 configuring a TCP/IP port on the computers connected to your network.

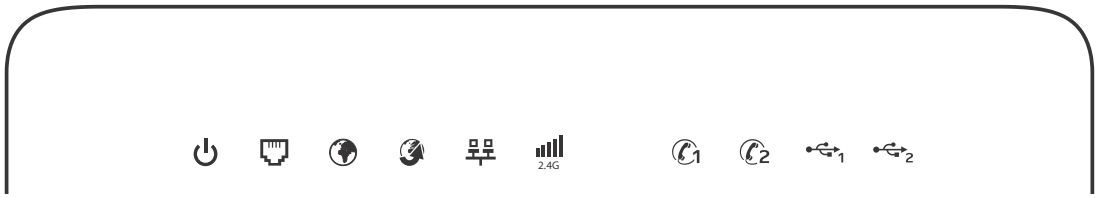
**Figure 4** Sharing a USB Printer




# 1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

**Figure 5** LEDs on the Device




None of the LEDs are on if the Device is not receiving power.

**Table 1** LED Descriptions

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| PWR/SYS | 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. |
| DSL | Green | On | The ADSL or VDSL line is up. |
| | | Blinking | The Device is initializing the ADSL or VDSL line. |
| | | Off | The DSL line is down. |

**Table 1** LED Descriptions (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| INTERNET | Green | On | The Device has an IP connection but no traffic.<br>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. |
| | | Off | There is no Internet connection or the gateway is in bridged mode. |
| | 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. |
| WAN | Green | On | The Device has a successful 1000 Mbps Ethernet connection on the WAN. |
| | | Blinking | The Device is sending or receiving data to/from the WAN at 1000 Mbps. |
| | Orange | On | The Device has a successful 10/100 Mbps Ethernet connection on the WAN. |
| | | Blinking | The Device is sending or receiving data to/from the WAN at 10/100 Mbps. |
| | | Off | There is no Ethernet connection on the WAN. |
| LAN | Green | On | The Device has a successful 1000 Mbps Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The Device is sending or receiving data to/from the LAN at 1000 Mbps. |
| | | Off | The Device does not have an Ethernet connection with the LAN. |
| WiFi 2.4G | Green | On | The 2.4 GHz 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 2.4 GHz wireless network is not activated. |
| Phone1, Phone2 | Green | On | A SIP account is registered for the phone port. |
| | | Blinking | A telephone connected to the phone port has its receiver off of the hook or there is an incoming call. |
| | Orange | On | A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account. |
| | | Blinking | A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account. |
| | | Off | The phone port does not have a SIP account registered. |
| USB1 | Green | On | The Device recognizes a USB connection through the USB1 slot. |
| | | Blinking | The Device is sending/receiving data to /from the USB device connected to it. |
| | | Off | The Device does not detect a USB connection through the USB1 slot. |
| USB2 | Green | On | The Device recognizes a USB connection through the USB2 slot. |
| | | Blinking | The Device is sending/receiving data to /from the USB device connected to it. |
| | | Off | The Device does not detect a USB connection through the USB2 slot. |

# 1.6 The RESET Button

If you forget your password or cannot access the Web Configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to the default password printed on the back of the Device.

1 Make sure the **PWR/SYS** LED is on (not blinking).

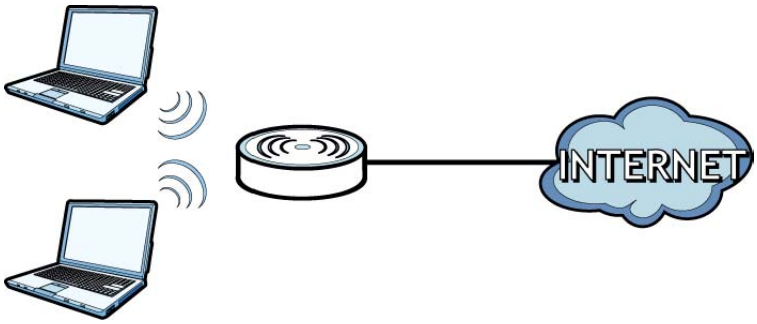
2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **PWR/SYS** LED begins to blink and then release it. When the **PWR/SYS** LED begins to blink, the defaults have been restored and the device restarts.

# 1.7 Wireless Access

The Device is a wireless Access Point (AP) for wireless 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 configure your wireless network in either the built-in Web Configurator, or using the WPS button.

**Figure 6** Wireless Access Example




## 1.7.1 Using the Wi-Fi and WPS Buttons

If the wireless network is turned off, press the **Wi-Fi** button for one second. Once the **WiFi 2.4G** LED turns green, the wireless network is active.

You can also use the **WPS** 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 **PWR/SYS** LED is on and not blinking.

2 Press the **WPS** button for five seconds and release it.

3 Press the WPS button on another WPS-enabled device within range of the Device. The **WiFi 2.4G** LED flashes orange while the Device sets up a WPS connection with the other wireless device.

4 Once the connection is successfully made, the **WiFi 2.4G** LED shines green.

To turn off the wireless network, press the **Wi-Fi** button for one to five seconds. The **WiFi 2.4G** LED turns off when the wireless network is off.

# 1.8 Wall-mounting Instructions

Do the following to hang your Device on a wall.

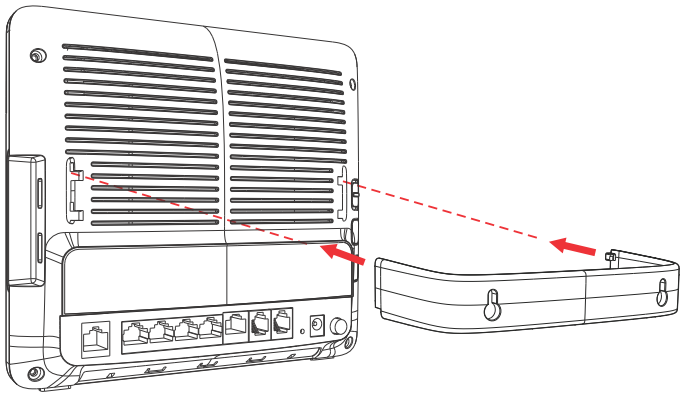
1 Locate a high position on a wall that is free of obstructions. Use a sturdy wall.

2 Hold the bracket against the wall and mark where to drill the holes.

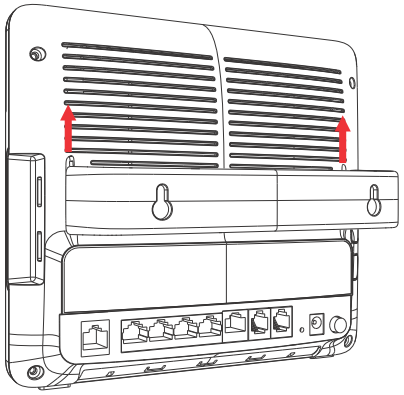
3 Drill the two screw holes in the wall.

**Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.**

4 Align and insert the bracket to the wall-mounting notches on the rear panel of the Device.



**5** Push the bracket up to tightly attach it to the Device.



**6** Mount the Device on the screws which are already installed on the wall. Make sure that the Device is firmly attached to the screws so it does not fall off.

# 2

# 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 or 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).

See Appendix C on page 315 if you need to make sure these functions are allowed in Internet Explorer.

### 2.1.1 Accessing the Web Configurator

1 Make sure your Device hardware is properly connected (refer to the Quick Start Guide).

2 Launch your web browser.

3 Type "192.168.1.254" as the URL.

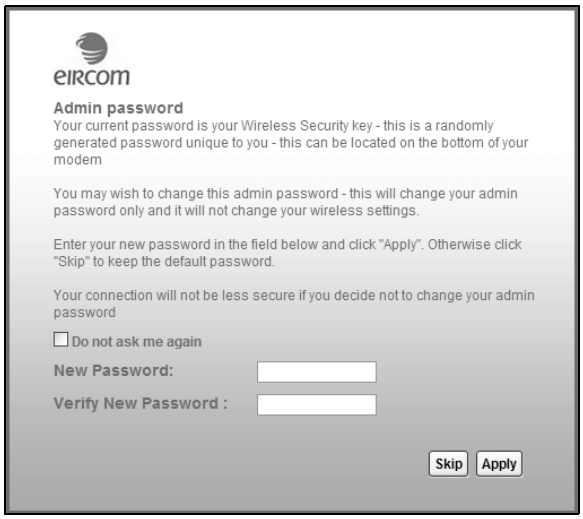
4 A password screen displays. Type “admin” (default) as the username and enter the default password (which is the same as the wireless key on the Device’s back label), then click **Login**. If you have changed the password, enter your new password and click **Login**.

**Figure 7** Login 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.

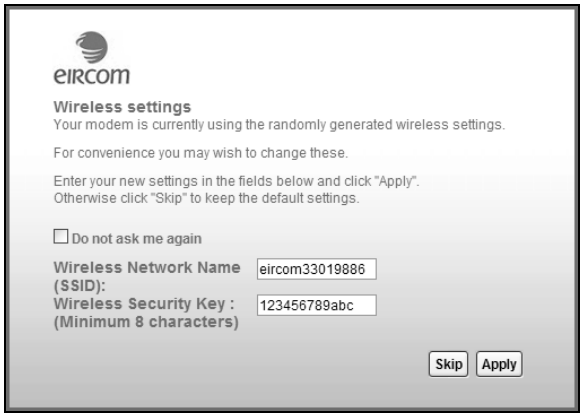
5 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Skip** to proceed to the main menu if you do not want to change the password now.

**Figure 8** Change Password Screen



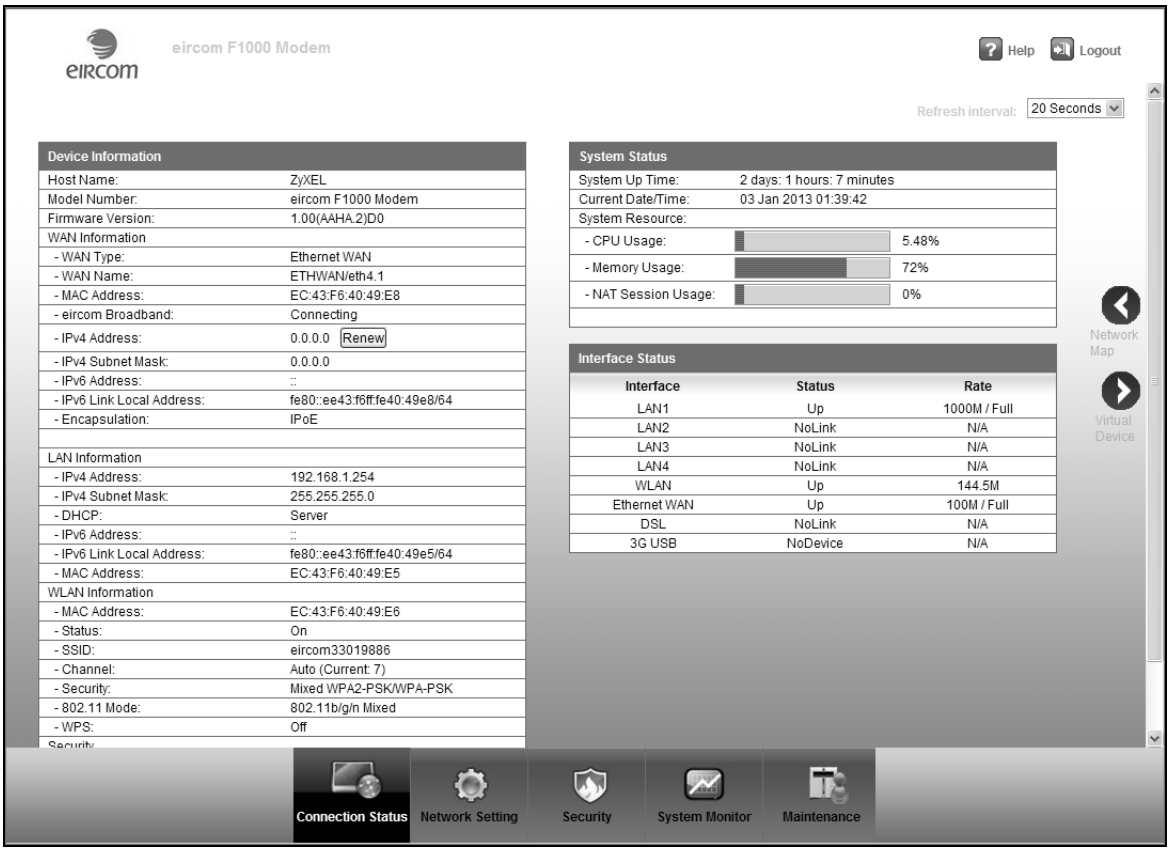

The following screen displays and asks if you want to change your wireless settings, including SSID and wireless security key. If you have changed the settings, click **Apply**. Otherwise, click **Skip** to proceed to the **Connection Status** screen if you do not want to change them now.

**Figure 9** Change Wireless Settings Screen



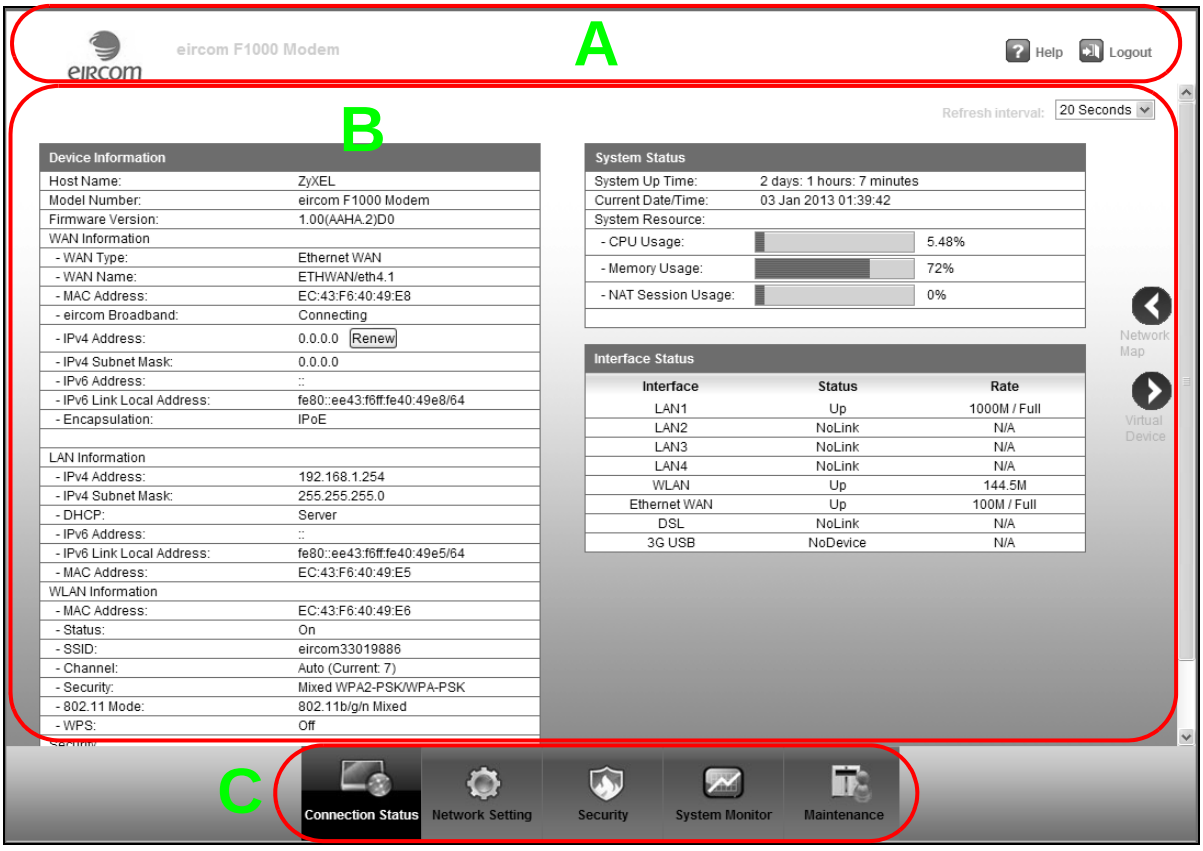

6 The **Connection Status** screen appears. You can view the Device's interface and system information.

**Figure 10** Connection Status



# 2.2 Web Configurator Layout

**Figure 11** 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 icons in the upper right corner.


Click the **Help** icon to get support on eircom's 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.

After you click **Connection Status**, the **Connection Status** screen is displayed. See Chapter 3 on page 40 for more information.

If you click **Virtual Device** on the **Connection Status** screen, a visual graphic appears, showing the connection status of the Device's ports. The connected ports are in color and disconnected ports are gray.

**Figure 12** Virtual Device


## 2.2.3 Navigation Panel

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

**Table 2** Navigation Panel Summary

| LINK | TAB | FUNCTION |
|---|---|---|
| Connection Status | | This screen shows the Device's interface and system information. |
| Network Setting | | |
| Broadband | Broadband | Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections. |
| | 3G Backup | Use this screen to configure 3G WAN connection. |
| | Advanced | Use this screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions. |
| | 802.1x | Use this screen to view and configure the IEEE 802.1x settings on the Device. |

**Table 2** Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| Wireless | General | Use this screen to 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 configure and view your WPS (Wi-Fi Protected Setup) settings. |
| | WMM | Use this screen to enable or disable Wi-Fi MultiMedia (WMM). |
| | WDS | Use this screen to set up Wireless Distribution System (WDS) links to other access points. |
| | Others | Use this screen to configure advanced wireless settings. |
| | Channel Status | Use this screen to scan wireless LAN channel noises and view the results. |
| 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. |
| | UPnP | Use this screen to turn UPnP and UPnP NAT-T on or off. |
| | Additional Subnet | Use this screen to configure IP alias and public static IP. |
| | STB Vendor ID | Use this screen to have the Device automatically create static DHCP entries for Set Top Box (STB) devices when they request IP addresses. |
| | 5th Ethernet port | Use this screen to configure the role of the **WAN** port. It can be either the Ethernet WAN or a LAN port. |
| | LAN VLAN | Use this screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent out through individual LAN ports. |
| | Wake on Lan | Use this screen to remotely turn on a device on the network. |
| Routing | Static Route | Use this screen to view and set up static routes on the Device. |
| | DNS Route | Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). |
| | Policy Forwarding | Use this screen to configure policy routing on the Device. |
| | RIP | Use this screen to configure Routing Information Protocol to exchange routing information with other routers. |
| QoS | General | Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions. |
| | Queue Setup | Use this screen to configure QoS queues. |
| | Class Setup | Use this screen to define a classifier. |
| | Policer Setup | Use these screens to configure QoS policers. |

**Table 2** Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| NAT | Port Forwarding | Use this screen to make your local servers visible to the outside world. |
| | Applications | Use this screen to configure servers behind the Device. |
| | Port Triggering | Use this screen to change your Device's port triggering settings. |
| | 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 enable or disable SIP ALG. |
| | Address Mapping | Use this screen to change your Device's address mapping settings. |
| | Sessions | Use this screen to configure the maximum number of NAT sessions each client host is allowed to have through the Device. |
| DNS | DNS Entry | Use this screen to view and configure DNS routes. |
| | Dynamic DNS | Use this screen to allow a static hostname alias for a dynamic IP address. |
| Interface Group | | Use this screen to map a port to a PVC or bridge group. |
| USB Service | File Sharing | Use this screen to enable file sharing via the Device. |
| | Media Server | Use this screen to use the Device as a media server. |
| | Printer Server | Use this screen to enable the print server on the Device and get the model name of the associated printer. |
| Security Settings | | |
| Firewall | General | Use this screen to configure the security level of your firewall. |
| | Protocol | Use this screen to add Internet services and configure firewall rules. |
| | Access Control | Use this screen to enable specific traffic directions for network services. |
| | DoS | Use this screen to activate protection against Denial of Service (DoS) attacks. |
| MAC Filter | | Use this screen to block or allow traffic from devices of certain MAC addresses to the Device. |
| Parental Control | | Use this screen to block web sites with the specific URL. |
| Scheduler Rules | | Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced. |
| Certificates | Local Certificates | Use this screen to view a summary list of certificates and manage certificates and certification requests. |
| | Trusted CA | Use this screen to view and manage the list of the trusted CAs. |
| IPSec VPN | Setup | Use this screen to add or edit VPN policies. |
| | Monitor | Use this screen to view the status of all IPSec VPN tunnels. You can also manually initiate a tunnel in this screen. |
| System Monitor | | |
| Log | System Log | Use this screen to view the status of events that occurred to the Device. You can export or e-mail the logs. |
| | Security Log | Use this screen to view the login record of the Device. You can export or e-mail the logs. |

**Table 2** Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| 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 NAT statistics for connected hosts. |
| VoIP Status | | Use this screen to view VoIP registration, current call statust and phone numbers for the phone ports. |
| ARP Table | | Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection. |
| Routing Table | | Use this screen to view the routing table on the Device. |
| IGMP/MLD Group Status | | Use this screen to view the status of all IGMP settings on the Device. |
| xDSL Statistics | | Use this screen to view the Device's xDSL traffic statistics. |
| 3G Statistics | | Use this screen to look at 3G Internet connection status. |
| Maintenance | | |
| User Account | | Use this screen to change user password on the Device. |
| Remote MGMT | | Use this screen to enable specific traffic directions for network services. |
| TR-064 | | Use this screen to enable management via TR-064 on the LAN. |
| SNMP | | Use this screen to configure SNMP (Simple Network Management Protocol) settings. |
| Time | | Use this screen to change your Device's time and date. |
| Email Notification | | Use this screen to configure up to two mail servers and sender addresses on the Device. |
| Log Setting | | Use this screen to change your Device's log settings. |
| Firmware Upgrade | | Use this screen to upload firmware to your device. |
| Configuration | | Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings. |
| Reboot | | Use this screen to reboot the Device without turning the power off. |
| Diagnostic | Ping & Traceroute & Nslookup | Use this screen to identify problems with the DSL connection. You can use Ping, TraceRoute, or Nslookup to help you identify problems. |
| | 802.1ag | Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports. |
| | OAM Ping | Use this screen to view information to help you identify problems with the DSL connection. |
| | WAN Diagnostics Tests | Use this screen to perform a test on the current WAN connection and view the result on the screen. |

# PART II
# Technical Reference

# 3

# Status and Network Map Screens

## 3.1 Overview

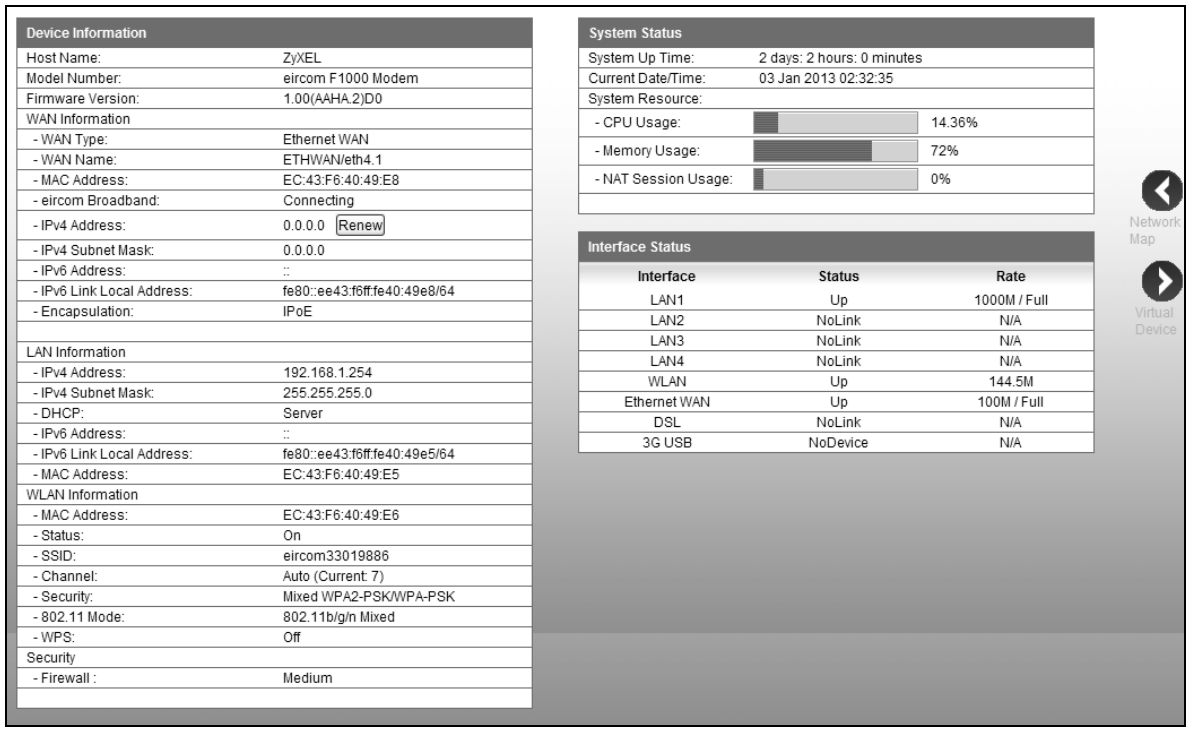
After you log into the Web Configurator, the **Connection Status** screen appears. Use the screen to look at the current status of the Device, system resources, and interfaces (LAN, WAN, and WLAN).

Use the **Network Map** screen to view the network connection status of the Device and clients connected to it.

## 3.2 The Connection Status Screen

Use this screen to view the status of the Device. Click **Connection Status** to open this screen.

**Figure 13** Connection Status Screen



Each field is described in the following table.

**Table 3** Connection Status Screen

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select how often you want the Device to update this screen. |
| Device Information | |
| Host Name | This field displays the Device system name. It is used for identification. |
| Model Number | This shows the model number of your Device. |
| Firmware Version | This is the current version of the firmware inside the Device. |
| WAN Information (These fields display when you have a WAN connection.) | |
| WAN Type | This field displays the current WAN connection type. |
| WAN Name | This field displays the name of the current WAN interface. |
| MAC Address | This shows the WAN Ethernet adapter MAC (Media Access Control) Address of your Device. |
| eircom Broadband | This shows the status of the WAN connection to the eircom network. |
| IPv4 Address | This field displays the current IP address of the Device in the WAN. Click **Release** or **Disconnect** to release your IP address to 0.0.0.0. If you want to renew your IP address, click **Renew**. |
| IPv4 Subnet Mask | This field displays the current subnet mask in the WAN. |
| IPv6 Address | This is the main IPv6 address of the Device's WAN interface, assigned through DHCPv6 or router advertisements. |
| IPv6 Link Local Address | This is the link-local address the Device generated itself for the WAN interface. |
| Encapsulation | This field displays the current encapsulation method. |
| LAN Information | |
| IPv4 Address | This is the current IPv4 IP address of the Device in the LAN. |
| IPv4 Subnet Mask | This is the current subnet mask in the LAN. |
| DHCP | This field displays what DHCP services the Device is providing to the LAN. Choices are:<br>**Server** - The Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.<br>**Relay** - The Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.<br>**None** - The Device is not providing any DHCP services to the LAN. |
| IPv6 Address | This is the main IPv6 address of the Device's LAN interface, assigned through DHCPv6 or router advertisements. |
| IPv6 Link Local Address | This is the link-local address the Device generated itself for the LAN interface. |
| MAC Address | This shows the LAN Ethernet adapter MAC (Media Access Control) Address of your Device. |
| WLAN Information | |
| MAC Address | This shows the wireless adapter MAC (Media Access Control) Address of your Device. |
| Status | This displays whether WLAN is activated. |
| SSID | This is the descriptive name used to identify the Device in a wireless LAN. |
| Channel | This is the channel number used by the Device now. |
| Security | This displays the type of security mode the Device is using in the wireless LAN. |

**Table 3** Connection Status Screen (continued)

| LABEL | DESCRIPTION |
|---|---|
| 802.11 Mode | This displays the type of 802.11 mode the Device is using in the wireless LAN. |
| WPS | This displays whether WPS is activated. |
| Security | |
| Firewall | This displays the firewall's current security level. |
| System Status | |
| System Up Time | 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. |
| Current Date/Time | This field displays the current date and time in the Device. You can change this in **Maintenance> Time Setting**. |
| System Resource | |
| 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 (for example, using QoS; see Chapter 8 on page 135). |
| 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%, the Device is probably becoming unstable, and you should restart the device. See Section 35.2 on page 269, or turn off the device (unplug the power) for a few seconds. |
| NAT Session Usage | This field displays what percentage of the Device supported NAT sessions are currently being used. |
| Interface Status | |
| Interface | This column displays each interface the Device has. |
| Status | This field indicates the interface's use status.<br>For the DSL interface, this field displays **Down** (line down), **Up** (line up or connected) and **Drop** (dropping a call) if you're using PPPoE encapsulation.<br>For the Ethernet WAN and LAN interface, this field displays **Up** when using the interface and **NoLink** when not using the interface.<br>For the WLAN interface, this field displays the enabled (**Active**) or disabled (**InActive**) state of the interface.<br>For the 3G USB interface, this field displays **Up** when using the interface and **NoDevice** when no device is detected in any USB slot. |
| Rate | For the Ethernet WAN and LAN interface, this displays the port speed and duplex setting.<br>For the DSL interface, it displays the downstream and upstream transmission rate.<br>For the WLAN interface, it displays the maximum transmission rate or **N/A** with WLAN disabled.<br>For the 3G USB interface, this field displays **Up** when a 3G USB device is installed in a USB slot and **NoDevice** when no device is detected in any USB slot. |

# 3.3 The Network Map Screen

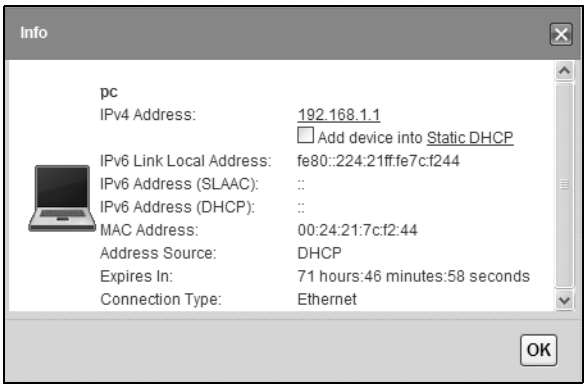
Use this screen to view the network connection status of the device and its clients. A warning message appears if there is a connection problem. You can click the link from the warning message

to open the diagnostic screens for troubleshooting, see Section 3.3.1 on page 39 for more information.

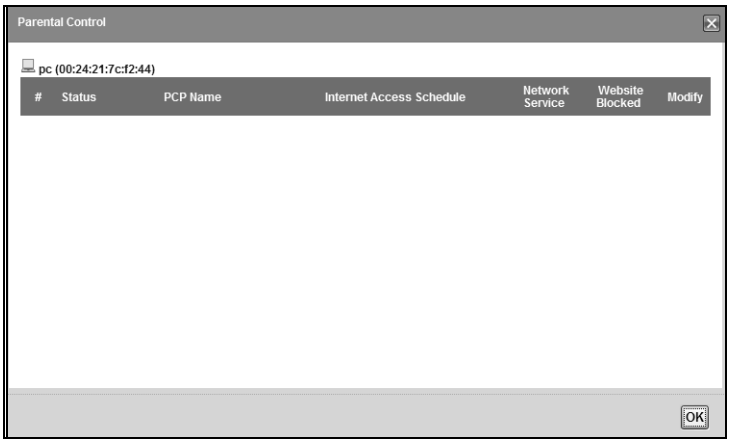
**Figure 14** Network Map: Icon View Mode


By clicking a client's name, you can do the following:


- Click **Info** to view information about the client. Select **Add device into Static DHCP** and click the **Static DHCP** link to configure a static DHCP client list. See Section 6.3 on page 109 for more information.



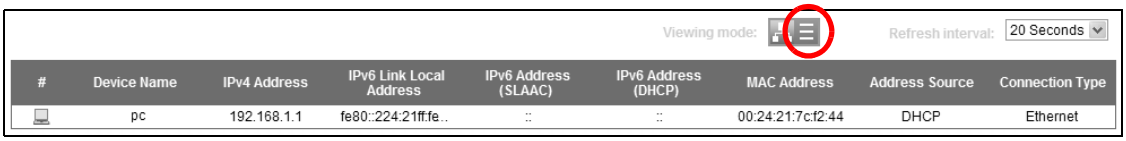
- Click **Parental Control** to open the following screen where you can block web sites with specific URLs.




- Click **Change name/icon** if you want to change the name or icon of the client.


If you prefer to view the status in a list, click **List View** in the **Viewing mode** selection box. You can configure how often you want the Device to update this screen in **Refresh interval**.

**Figure 15** Network Map: List View Mode

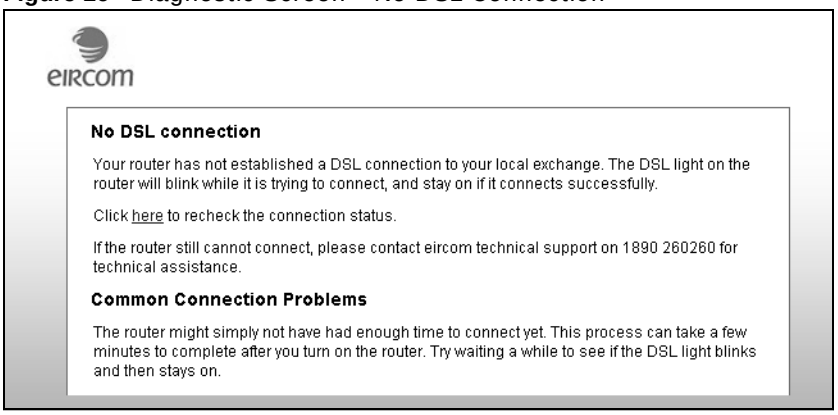



## 3.3.1 The Diagnostic Screens

Depending on your WAN connection problem, a different screen appears. Follow the on-screen instructions to troubleshoot the problem.

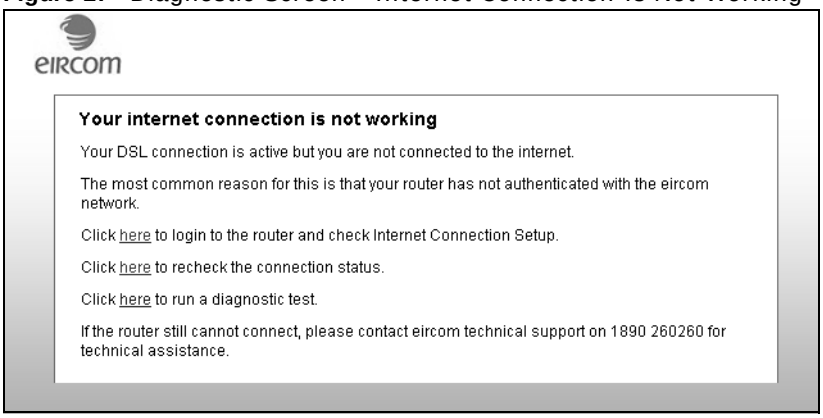
- This screen appears when there is no WAN connection.

**Figure 16** Diagnostic Screen - No DSL Connection



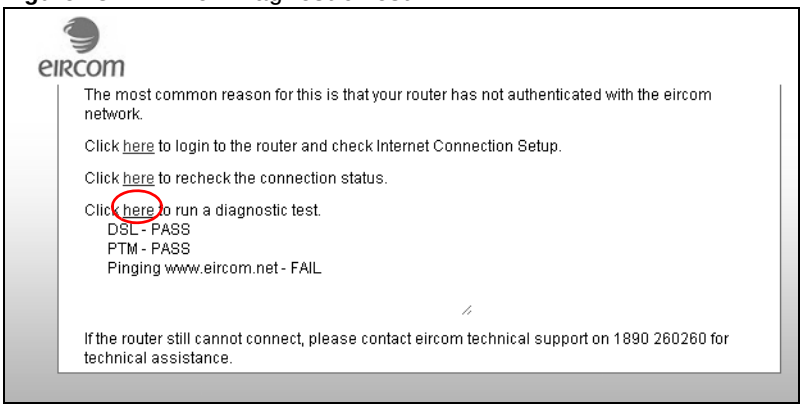

- This screen appears when your WAN connection is up but the Device fails to connect to the Internet.

**Figure 17** Diagnostic Screen - Internet Connection Is Not Working




- Click the following link to start a diagnostic test and view the result on the screen.

**Figure 18** Link for Diagnostic Test



# 4

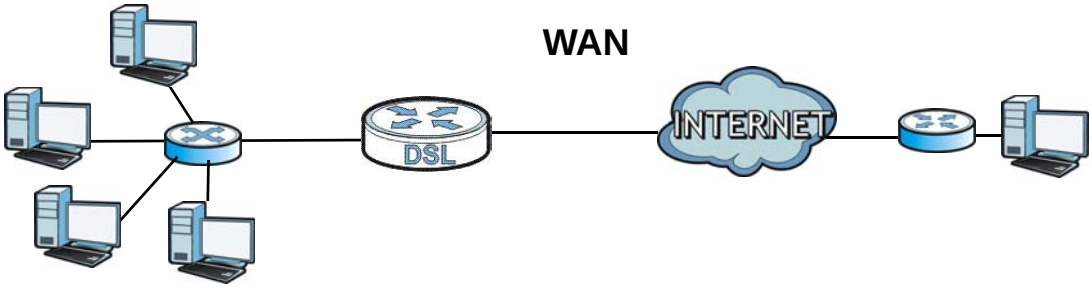
# Broadband

## 4.1 Overview

This chapter discusses 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 19** LAN and WAN




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

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

**Figure 20** 3G WAN Connection


### 4.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the Device for Internet access (Section 4.2 on page 45).
- Use the **3G Backup** screen to configure 3G WAN connection (Section 4.3 on page 55).

- Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions (Section 4.4 on page 59).
- Use the **802.1x** screen to view and configure the IEEE 802.1X settings on the Device (Section 4.5 on page 60).

**Table 4** WAN Setup Overview

| LAYER-2 INTERFACE | | INTERNET CONNECTION | | |
|---|---|---|---|---|
| **CONNECTION** | **DSL LINK TYPE** | **MODE** | **ENCAPSULATION** | **CONNECTION SETTINGS** |
| ADSL/VDSL over PTM | N/A | Routing | PPPoE | PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU |
| | | | IPoE | IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU |
| | | Bridge | N/A | VLAN and QoS |
| ADSL over ATM | EoA | Routing | PPPoE/PPP0A | ATM PVC configuration, PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU |
| | | | IPoE/IPoA | ATM PVC configuration, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU |
| | | Bridge | N/A | ATM PVC configuration, and QoS |
| EtherWAN | N/A | Routing | PPPoE | PPP user name and password, WAN IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU |
| | | | IPoE | WAN IPv4/IPv6 IP address, NAT, DNS server and routing feature |
| | | Bridge | N/A | VLAN and QoS |

## 4.1.2 What You Need to Know

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

### Encapsulation Method

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

### WAN IP Address

The WAN IP address is an IP address for the 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 ISPeircom each time the Device tries to access the Internet.

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

### ATM

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

### PTM

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

### 3G

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

## IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x $10^{38}$ IP addresses. The Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).

## IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So 2001:0db8:1a2b:0015:0000:0000:1a2f:0000 can be written as 2001:db8:1a2b:15:0:0:1a2f:0.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So 2001:0db8:0000:0000:1a2f:0000:0000:0015 can be written as 2001:0db8::1a2f:0000:0000:0015, 2001:0db8:0000:0000:1a2f::0015, 2001:db8::1a2f:0:0:15 or 2001:db8:0:0:1a2f::15.

## IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address

compose the network address. The prefix length is written as “/x” where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (2001:db8) is the subnet prefix.

## IPv6 Subnet Masking

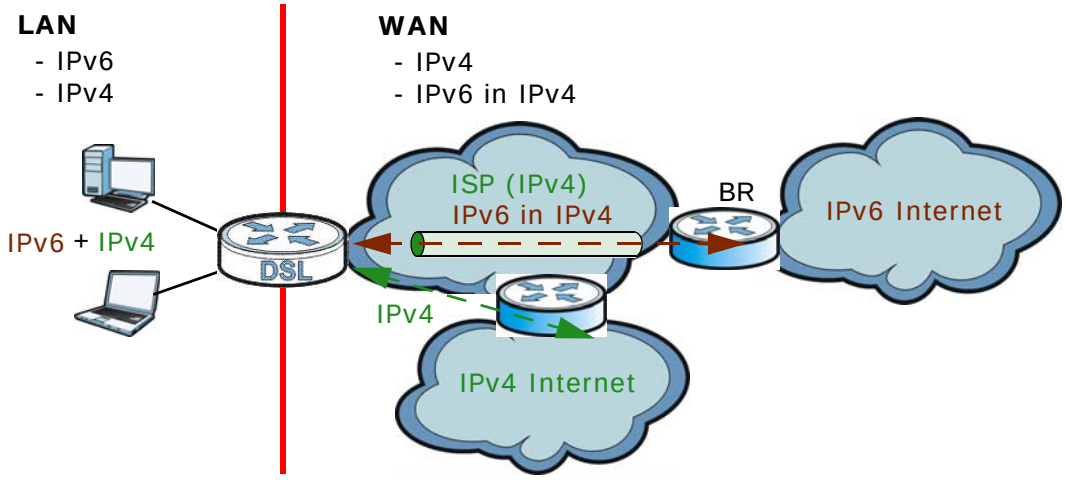
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block’s 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

## IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6rd) when the local network uses IPv6 and eircom has an IPv4 network. When the Device has an IPv4 WAN address and you set **IPv6/IPv4 Mode** to **IPv4 Only**, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross eircom’s IPv4 network.

The Device generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to eircom’s Border Relay router (BR in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The Device uses it’s configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

**Figure 21** IPv6 Rapid Deployment

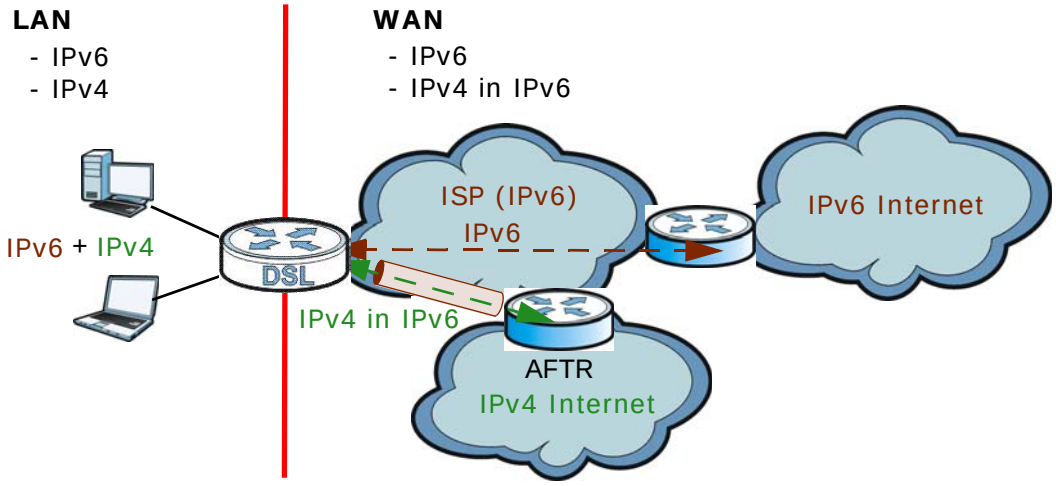



## Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the Device has an IPv6 WAN address and you set **IPv6/IPv4 Mode** to **IPv6 Only**, you can enable Dual Stack Lite to use IPv4 computers and services.

The Device tunnels IPv4 packets inside IPv6 encapsulation packets to the ISP’s Address Family Transition Router (AFTR in the graphic) to connect to the IPv4 Internet. The local network can also use IPv6 services. The Device uses it’s configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

**Figure 22** Dual Stack Lite



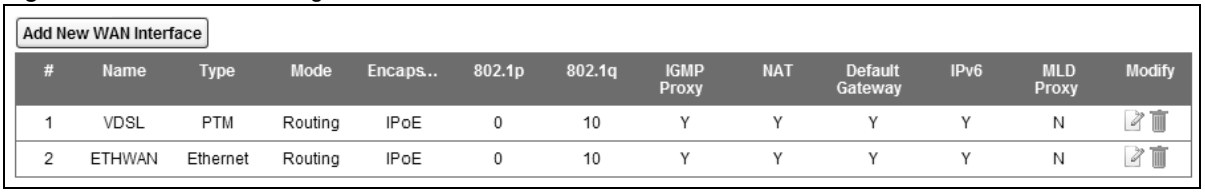

### 4.1.3 Before You Begin

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

## 4.2 The Broadband Screen

Use this screen to change your Device's Internet access settings. Click **Network Setting > Broadband** from the menu. The summary table shows you the configured WAN services (connections) on the Device.

**Figure 23** Network Setting > Broadband




The following table describes the labels in this screen.

**Table 5** Network Setting > Broadband

| LABEL | DESCRIPTION |
|---|---|
| Add New WAN Interface | Click this button to create a new connection. |
| # | This is the index number of the entry. |
| Name | This is the service name of the connection. |
| Type | This shows whether it is an ATM, Ethernet or a PTM connection. |
| Mode | This shows whether the connection is in routing or bridge mode. |
| Encapsulation | This is the method of encapsulation used by this connection. |

**Table 5** Network Setting > Broadband (continued)

| LABEL | DESCRIPTION |
|---|---|
| 802.1p | This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned. |
| 802.1q | This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned. |
| IGMP Proxy | This shows whether the Device act as an IGMP proxy on this connection. |
| NAT | This shows whether NAT is activated or not for this connection. |
| Default Gateway | This shows whether the Device use the WAN interface of this connection as the system default gateway. |
| IPv6 | This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service. |
| MLD Proxy | This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service. |
| Modify | Click the **Edit** icon to configure the WAN connection.<br>Click the **Delete** icon to remove the WAN connection. |

## 4.2.1 Add/Edit Internet Connection

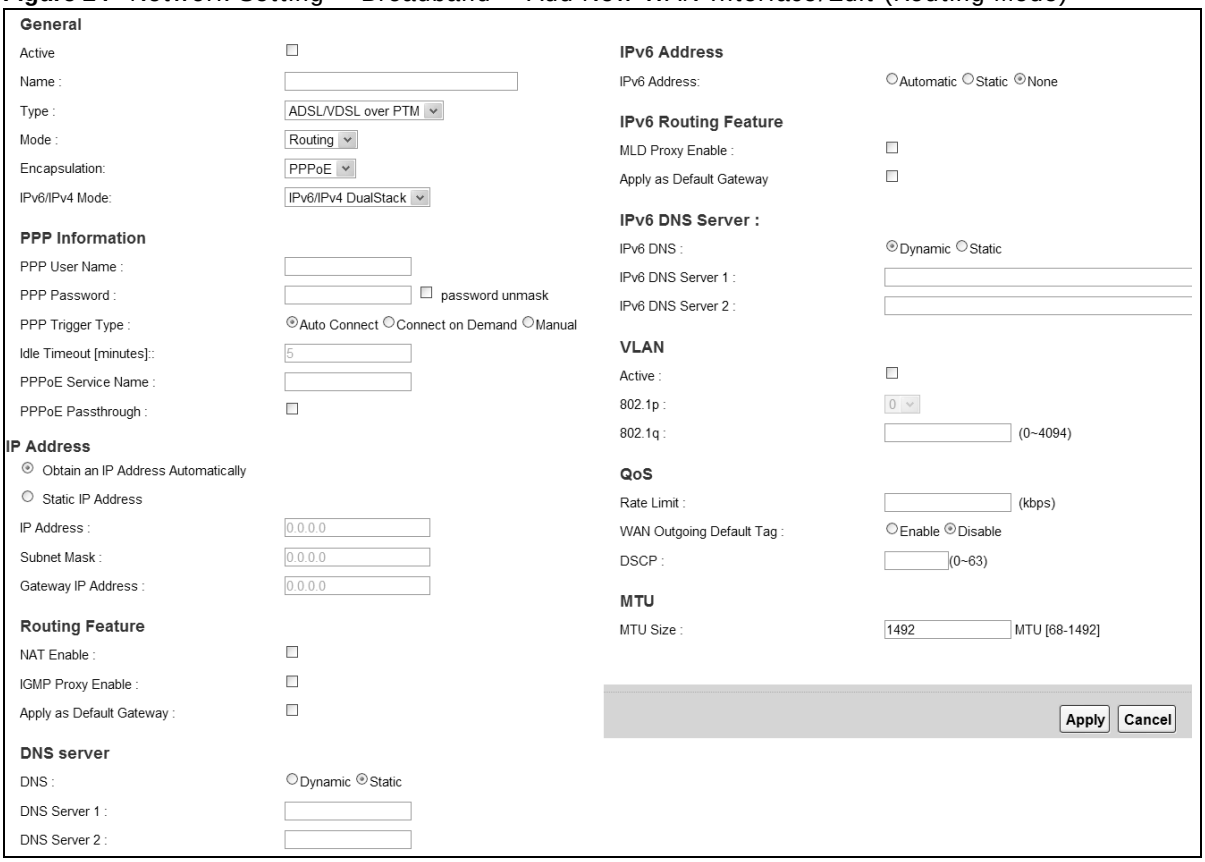
Click **Add New WAN Interface** in the **Broadband** screen or the **Edit** icon next to an existing WAN interface to configure a WAN connection. The screen varies depending on the interface type, mode, encapsulation, and IPv6/IPv4 mode you select.

### 4.2.1.1 Routing Mode

Use **Routing** mode if eircom give you one IP address only and you want multiple computers to share an Internet account.

The following example screen displays when you select the **ADSL/VDSL over ATM** connection type, **Routing** mode, and **PPPoE** encapsulation. The screen varies when you select other interface type, encapsulation, and IPv6/IPv4 mode.

**Figure 24** Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)




The following table describes the labels in this screen.

**Table 6** Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)

| LABEL | DESCRIPTION |
|---|---|
| General | |
| Active | Select this to activate the WAN configuration settings. |
| Name | Specify a descriptive name for this connection. |
| Type | Select whether it is an ADSL/VDSL over PTM, ADSL over ATM connection or Ethernet. |

**Table 6** Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Mode | Select **Routing** if your ISP give you one IP address only and you want multiple computers to share an Internet account. |
| Encapsulation | Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select **Routing** in the **Mode** field.<br><br>The choices depend on the connection type you selected. If your connection type is **ADSL/VDSL over PTM**, the choices are **PPPoE** and **IPoE**. If your connection type is **ADSL over ATM**, the choices are **PPPoE**, **PPPoA**, **IPoE** and **IPoA**. |
| IPv6/IPv4 Mode | Select **IPv4 Only** if you want the Device to run IPv4 only.<br><br>Select **IPv6/IPv4 DualStack** to allow the Device to run IPv4 and IPv6 at the same time.<br><br>Select **IPv6 Only** if you want the Device to run IPv6 only. |
| ATM PVC Configuration (These fields appear when the **Type** is set to **ADSL over ATM**.) | |
| 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. |
| DSL Link Type | This field is not editable. The selection depends on the setting in the **Encapsulation** field.<br><br>**EoA** (Ethernet over ATM) uses an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. EoA supports ENET ENCAP (IPoE), PPPoE and RFC1483/2684 bridging encapsulation methods.<br><br>**PPPoA** (PPP over ATM) allows just one PPPoA connection over a PVC.<br><br>**IPoA** (IP over ATM) allows just one RFC 1483 routing connection over a PVC. |
| Encapsulation Mode | Select the method of multiplexing used by your ISP from the drop-down list box. Choices are:<br><br>• **LLC/SNAP-BRIDGING:** In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select **IPoE** or **PPPoE** in the **Select DSL Link Type** field.<br>• **VC/MUX:** In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.<br>• **LLC/ENCAPSULATION:** More than one protocol can be carried over the same VC. This is available only when you select **PPPoA** in the **Encapsulation** field.<br>• **LLC/SNAP-ROUTING:** In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LCC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select **IPoA** in the **Encapsulation** field. |
| Service Category | Select **UBR Without PCR** or **UBR With PCR** for applications that are non-time sensitive, such as e-mail.<br><br>Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.<br><br>Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.<br><br>Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that 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.This field is not available when you select **UBR Without PCR**. |

**Table 6** Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Sustainable Cell Rate | The Sustainable 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.<br><br>This field is available only when you select **Non Realtime VBR** or **Realtime VBR**. |
| 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.<br><br>This field is available only when you select **Non Realtime VBR** or **Realtime VBR**. |
| PPP Information (This is available only when you select **PPPoE** or **PPPoA** in the **Mode** field.) | |
| PPP User Name | Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given. |
| PPP Password | Enter the password associated with the user name above. Select **password unmask** to show your entered password in plain text. |
| PPP Triger Type | Select when to have the Device establish the PPP connection.<br><br>**Auto Connect** - select this to not let the connection time out.<br><br>**Connect on Demand** - select this to automatically bring up the connection when the Device receives packets destined for the Internet.<br><br>**Manual** - select this if you want to manually trigger the connection up. You can manually connect and disconnect the connection on the **Connection Status** screen. |
| Idle Timeout | This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.<br><br>This field is not configurable if you select **Auto Connect** in the **PPP Triger Type** field. |
| PPPoE Service Name | Enter the name of your PPPoE service here. |
| PPPoE Passthrough | This field is available when you select **PPPoE** encapsulation.<br><br>In addition to the Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten 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.<br><br>PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.<br><br>Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP. |
| IP Address (This is available only when you select **IPv4 Only** or **IPv6/IPv4 DualStack** in the **IPv6/IPv4 Mode** field.) | |
| Obtain an IP Address Automatically | A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address. |
| DHCP option 60/ Vendor ID | This field displays when editing an existing WAN interface. Type the class vender ID you want the Device to add in the DHCP Discovery packets that go to the DHCP server. |
| DHCP option 43 Enable | This field displays when editing an existing WAN interface. Type the vender specific information you want the Device to add in the DHCP Offer packets. The information is used, for example, for configuring an ACS's (Auto Configuration Server) URL. |
| Static IP Address | Select this option If the ISP assigned a fixed IP address. |
| IP Address | Enter the static IP address provided by your ISP. |
| Subnet Mask | Enter the subnet mask provided by your ISP. |

**Table 6** Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Gateway IP Address | Enter the gateway IP address provided by your ISP. |
| Routing Feature (This is available only when you select **IPv4 Only** or **IPv6/IPv4 DualStack** in the **IPv6/IPv4 Mode** field.) | |
| NAT Enable | Select this option to activate NAT on this connection. |
| IGMP Proxy Enable | Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.<br>Select this option to have the Device act as an IGMP proxy on this connection. This allows the Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly. |
| Apply as Default Gateway | Select this option to have the Device use the WAN interface of this connection as the system default gateway. |
| DNS Server (This is available only when you select **IPv4 Only** or **IPv6/IPv4 DualStack** in the **IPv6/IPv4 Mode** field.) | |
| DNS | Select **Dynamic** if you want the Device use the DNS server addresses assigned by your ISP.<br>Select **Static** if you want the Device use the DNS server addresses you configure manually. |
| DNS Server 1 | Enter the first DNS server address assigned by the ISP. |
| DNS Server 2 | Enter the second DNS server address assigned by the ISP. |
| WAN MAC Address | |
| Factory Default | Select **Factory Default** to use the factory assigned default MAC address. |
| Clone the computer's MAC address - IP Address | Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication. |
| Set WAN MAC Address | Select this option and enter the MAC address you want to use. |
| Tunnel (This is available only when you select **IPv4 Only** or **IPv6 Only** in the **IPv6/IPv4 Mode** field.)<br>The DS-Lite (Dual Stack Lite) fields display when you set the **IPv6/IPv4 Mode** field to **IPv6 Only**.<br>Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 44 for more information.<br>The 6RD (IPv6 rapid deployment) fields display when you set the **IPv6/IPv4 Mode** field to **IPv4 Only**. See IPv6 Rapid Deployment on page 44 for more information. | |
| Enable DS-Lite | This is available only when you select **IPv6 Only** in the **IPv6/IPv4 Mode** field. Select **Enable** to let local computers use IPv4 through an ISP's IPv6 network. |
| DS-Lite Relay Server IP | Specify the transition router's IPv6 address. |
| Enable 6RD | This is available only when you select **IPv4 Only** in the **IPv6/IPv4 Mode** field. Select **Enable** to tunnel IPv6 traffic from the local network through the ISP's IPv4 network. |
| 6RD Type | Select **Static** if you have the IPv4 address of the relay server, otherwise select **DHCP** to have the Device detect it automatically through DHCP. |
| IPv4 Mask Length | Enter the subnet mask number (1~32) for the IPv4 network. |
| 6RD Border Relay Server IP | When you set the **6RD Type** to **Static**, specify the relay server's IPv4 address in this field. |
| 6RD IPv6 Prefix | Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet. |

**Table 6** Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| IPv6 Address (This is available only when you select **IPv6/IPv4 DualStack** or **IPv6 Only** in the **IPv6/IPv4 Mode** field.) | |
| IPv6 Address | Select **Automatic** if you want to have the Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.<br>• Select **Get IPv6 Address From DHCPv6 Server(IA_NA)** 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. This option is available only when you choose to get your IPv6 address automatically.<br>• Select **Prefix Delegation(IA_PD)** to use DHCP PD (Prefix Delegation) which enables the Device to pass the IPv6 prefix information to its LAN hosts. The hosts can then use the prefix to generate their IPv6 addresses.<br>Select **Static** if you have a fixed IPv6 address assigned by your ISP.<br>Select **None** to not assign any IPv6 address to this WAN connection. |
| WAN IPv6 Address | Enter the IPv6 address assigned by your ISP. |
| Prefix Length | Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address. |
| Next Hop | Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Device's interface(s). The gateway helps forward packets to their destinations. |
| IPv6 Routing Feature (This is available only when you select **IPv6/IPv4 DualStack** or **IPv6 Only** in the **IPv6/IPv4 Mode** field. You can enable IPv6 routing features in the following section.) | |
| MLD Proxy Enable | Select this checkbox to have the Device act as an MLD proxy on 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. |
| Apply as Default Gateway | Select this option to have the Device use the WAN interface of this connection as the system default gateway. |
| IPv6 DNS Server | Configure the IPv6 DNS server in the following section. |
| IPv6 DNS | Select **Dynamic** to have the Device get the IPv6 DNS server addresses from the ISP automatically.<br>Select **Static** to have the Device use the IPv6 DNS server addresses you configure manually. |
| IPv6 DNS Server 1 | Enter the first IPv6 DNS server address assigned by the ISP. |
| IPv6 DNS Server 2 | Enter the second IPv6 DNS server address assigned by the ISP. |
| VLAN (These fields appear when the **Type** is set to **ADSL/VDSL over PTM**.) | |
| Active | Select this option to add the VLAN tag (specified below) to the outgoing traffic through this connection. |
| 802.1p | IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.<br>Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. |
| 802.1q | Type the VLAN ID number (from 1 to 4094) for traffic through this connection. |
| QoS | |
| Rate Limit | Enter the rate limit for the connection. This is the maximum transmission rate allowed for traffic on this connection. |

**Table 6** Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

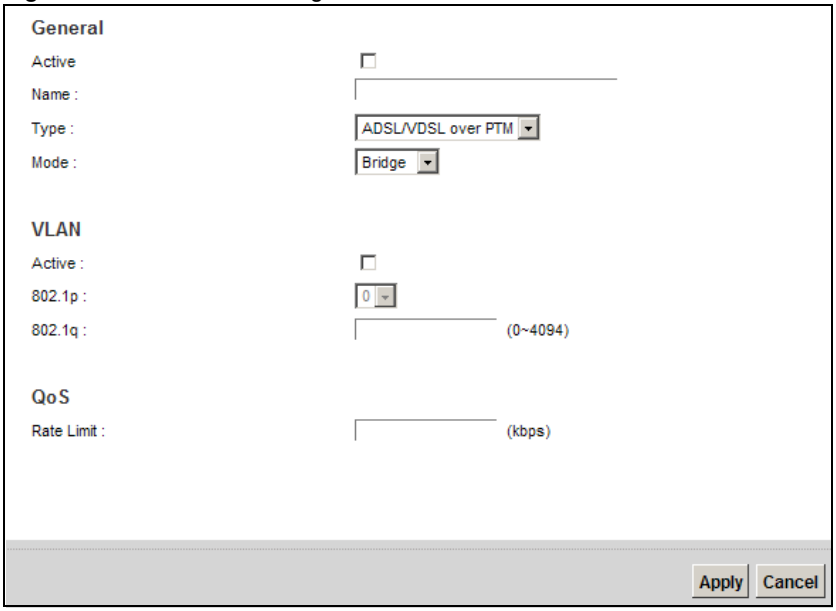
| LABEL | DESCRIPTION |
|---|---|
| WAN Outgoing Default Tag | Select **Enable** and enter a **DSCP** (DiffServ Code Point) value to have the Device add it in the packets sent by this WAN interface. |
| MTU | |
| MTU Size | Enter the MTU (Maximum Transfer Unit) size for this traffic. |
| Apply | Click **Apply** to save your changes back to the Device. |
| Cancel | Click **Cancel** to exit this screen without saving. |

### 4.2.1.2 Bridge Mode

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Bridge** as the encapsulation mode. The screen varies depending on the interface type you select.

If you select **ADSL / VDSL over PTM** as the interface type, the following screen appears.

**Figure 25** Network Setting > Broadband > Add New WAN Interface/Edit (Bridge Mode )




The following table describes the fields in this screen.

**Table 7** Network Setting > Broadband > Add New WAN Interface/Edit (Bridge Mode)

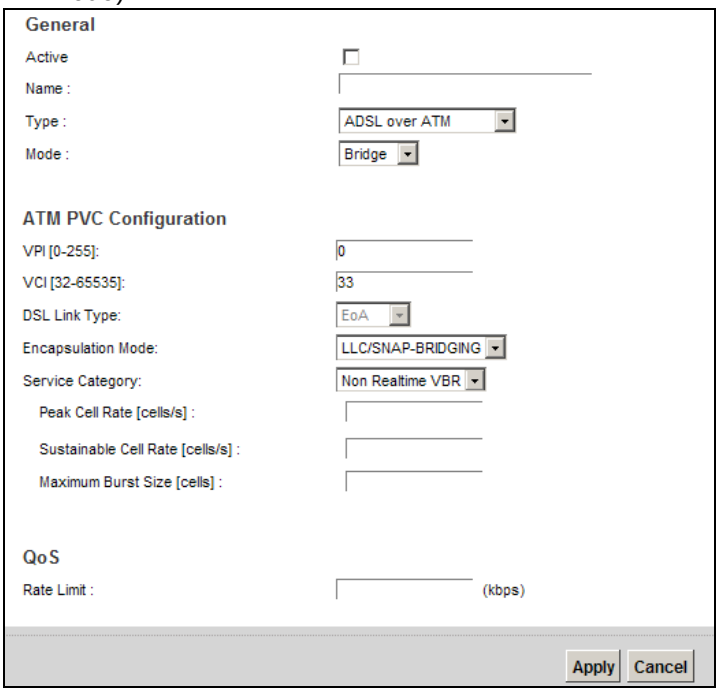
| LABEL | DESCRIPTION |
|---|---|
| General | |
| Active | Select this to activate the WAN configuration settings. |
| Name | Enter a service name of the connection. |
| Type | Select **ADSL / VDSL over PTM** as the interface that you want to configure. The Device uses the VDSL technology for data transmission over the DSL port. |
| Mode | 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 routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s). |
| VLAN | This section is available only when you select **ADSL / VDSL over PTM** in the **Type** field. |

**Table 7** Network Setting > Broadband > Add New WAN Interface/Edit (Bridge Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this to add the VLAN Tag (specified below) to the outgoing traffic through this connection. |
| 802.1p | IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.<br>Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. |
| 802.1q | Type the VLAN ID number (from 0 to 4094) for traffic through this connection. |
| QoS | |
| Rate Limit | Enter the rate limit for the connection. This is the maximum transmission rate allowed for traffic on this connection. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

If you select **ADSL over ATM** as the interface type, the following screen appears.

**Figure 26** Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode)




The following table describes the fields in this screen.

**Table 8** Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM - Bridge Mode)

| LABEL | DESCRIPTION |
|---|---|
| General | |
| Active | Select this to activate the WAN configuration settings. |
| Name | Enter a service name of the connection. |
| Type | Select **ADSL over ATM** as the interface for which you want to configure here. The Device uses the ADSL technology for data transmission over the DSL port. |

**Table 8** Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM - Bridge Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Mode | 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 routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s). |
| ATM PVC Configuration (These fields appear when the **Type** is set to **ADSL over ATM**.) | |
| 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. |
| DSL Link Type | This field is not editable. The selection depends on the setting in the **Encapsulation** field.<br><br>**EoA** (Ethernet over ATM) uses an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. EoA supports ENET ENCAP (IPoE), PPPoE and RFC1483/2684 bridging encapsulation methods.<br><br>**PPPoA** (PPP over ATM) allows just one PPPoA connection over a PVC.<br><br>**IPoA** (IP over ATM) allows just one RFC 1483 routing connection over a PVC. |
| Encapsulation Mode | Select the method of multiplexing used by your ISP from the drop-down list box. Choices are:<br><br>• **LLC/SNAP-BRIDGING:** In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select **IPoE** or **PPPoE** in the Select DSL Link Type field.<br>• **VC/MUX:** In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.<br>• **LLC/ENCAPSULATION:** More than one protocol can be carried over the same VC. This is available only when you select **PPPoA** in the **Encapsulation** field.<br>• **LLC/SNAP-ROUTING:** In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LCC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select **IPoA** in the **Encapsulation** field. |
| Service Category | Select **UBR Without PCR** or **UBR With PCR** for applications that are non-time sensitive, such as e-mail.<br><br>Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.<br><br>Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.<br><br>Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that 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.This field is not available when you select **UBR Without PCR**. |
| Sustainable Cell Rate | The Sustainable 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.<br><br>This field is available only when you select **Non Realtime VBR** or **Realtime VBR**. |
| 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.<br><br>This field is available only when you select **Non Realtime VBR** or **Realtime VBR**. |

**Table 8** Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM - Bridge Mode) (continued)

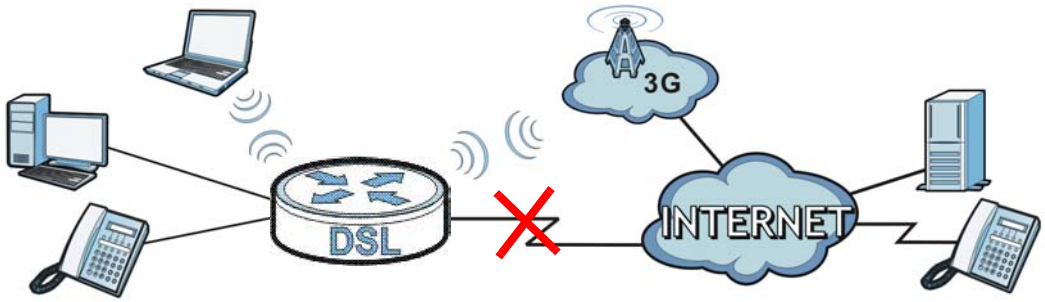
| LABEL | DESCRIPTION |
|---|---|
| QoS | |
| Rate Limit | Enter the rate limit for the connection. This is the maximum transmission rate allowed for traffic on this connection. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 4.3 The 3G Backup Screen

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

Note: This Device supports connecting one 3G dongle at a time.

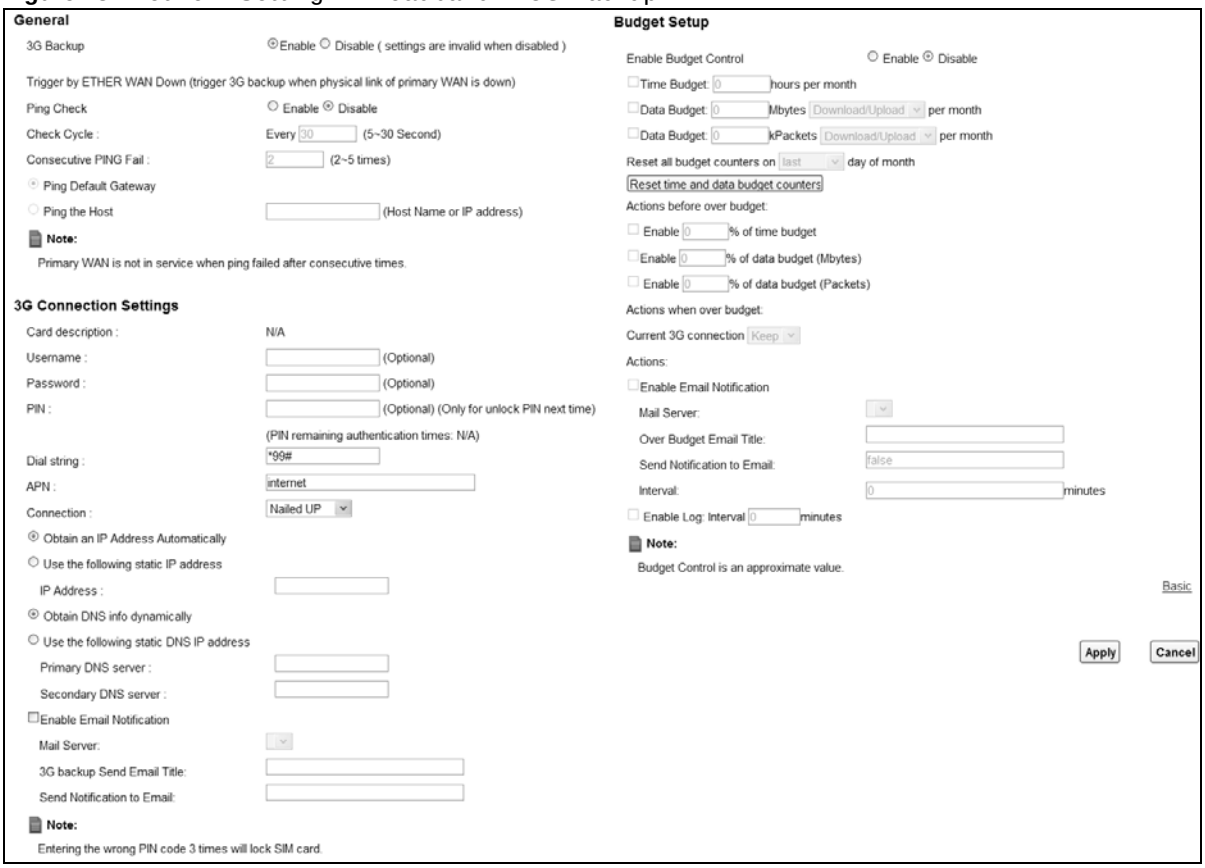
**Figure 27** Internet Access Application: 3G WAN




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 28** Network Setting **>** Broadband > 3G Backup




The following table describes the labels in this screen.

**Table 9** 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. |
| Ping Check | Select **Enable** if you want the Device to ping check the connection status of your WAN. You can configure the frequency of the ping check and number of consecutive failures before triggering 3G backup. |
| Check Cycle | Enter the frequency of the ping check in this field. |
| Consecutive PING Fail | Enter how many consecutive failures are required before 3G backup is triggered. |
| Ping Default Gateway | Select this to have the Device ping the WAN interface's default gateway IP address. |
| Ping the Host | Select this to have the Device ping the particular host name or IP address you typed in this field. |
| 3G Connection Settings | |
| 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**. |

**Table 9** Network Setting **>** Broadband > 3G Backup (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>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.<br>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.<br>For example, *99# is the dial string to establish a GPRS or 3G connection in Taiwan. |
| 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.<br>You can enter up to 32 ASCII printable characters. Spaces are allowed. |
| Connection | Select **Nailed UP** if you do not want the connection to time out.<br>Select **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. |
| 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 bythe ISP. |
| Enable Email Notification | Select this to enable the e-mail notification function. The Device will e-mail you a notification when the 3G connection is up. |
| Mail Server | Select a mail server for the e-mail address specified below.<br>If you do not select a mail server, e-mail notifications cannot be sent via e-mail. You must have configured a mail server already in the **Maintenance** > **Email Notification** screen. |
| 3G backup Send Email Title | Type a title that you want to be in the subject line of the e-mail notifications that the Device sends. |

**Table 9** Network Setting **>** Broadband > 3G Backup (continued)

| LABEL | DESCRIPTION |
|---|---|
| Send Notification to Email | Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications cannot be sent via e-mail. |
| Advanced | Click this to show the advanced 3G backup settings. |
| Budget Setup | |
| Enable Budget Control | Select **Enable** to set a monthly limit for the user account of the installed 3G card. You can set a limit on the total traffic and/or call time. The Device takes the actions you specified when a limit is exceeded during the month. |
| Time Budget | Select this and specify the amount of time (in hours) that the 3G connection can be used within one month. If you change the value after you configure and enable budget control, the Device resets the statistics. |
| Data Budget (Mbytes) | Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted via the 3G connection within one month.<br>Select **Download/Upload** to set a limit on the total traffic in both directions.<br>Select **Download** to set a limit on the downstream traffic (from the ISP to the Device).<br>Select **Upload** to set a limit on the upstream traffic (from the Device to the ISP).<br>If you change the value after you configure and enable budget control, the Device resets the statistics. |
| Data Budget (kPackets) | Select this and specify how much downstream and/or upstream data (in k Packets) can be transmitted via the 3G connection within one month.<br>Select **Download/Upload** to set a limit on the total traffic in both directions.<br>Select **Download** to set a limit on the downstream traffic (from the ISPto the Device).<br>Select **Upload** to set a limit on the upstream traffic (from the Device to the ISP).<br>If you change the value after you configure and enable budget control, the Device resets the statistics. |
| Reset all budget counters on | Select the date on which the Device resets the budget every month. Select **last** if you want the Device to reset the budget on the last day of the month. Select **specific** and enter the number of the date you want the Device to reset the budget |
| Reset time and data budget counters | Click this button to reset the time and data budgets immediately. The count starts over with the 3G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart; so if you configured the time and data budget counters to reset on the second day of the month and you use this button on the first, the time and data budget counters will still reset on the second. |
| Actions before over budget | Specify the actions the Device takes before the time or data limit exceeds. |
| Enable % of time budget/ data budget (Mbytes)/data budget (kPackets) | Select **Enable** and enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the Device resets the statistics. |
| Actions when over budget | Specify the actions the Device takes when the time or data limit is exceeded. |
| Current 3G connection | Select **Keep** to maintain an existing 3G connection or **Drop** to disconnect it. |
| Actions | |
| Enable Email Notification | Select this to enable the e-mail notification function. The Device will e-mail you a notification when there over budget occurs. |

**Table 9** Network Setting **>** Broadband > 3G Backup (continued)

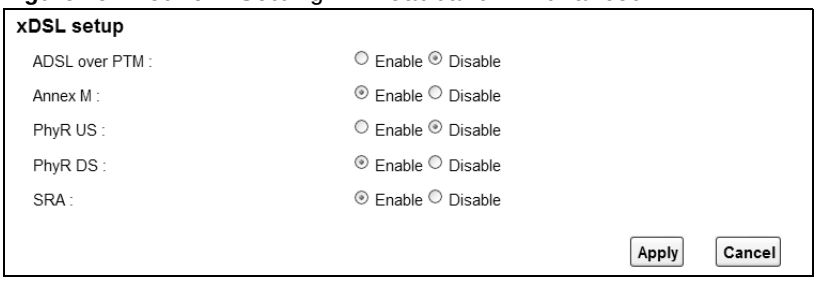
| LABEL | DESCRIPTION |
|---|---|
| Mail Server | Select a mail server for the e-mail address specified below.<br><br>If you do not select a mail server, e-mail notifications cannot be sent via e-mail. You must have configured a mail server already in the **Maintenance** > **Email Notification** screen. |
| Over Budget Email Title | Type a title that you want to be in the subject line of the e-mail notifications that the Device sends. |
| Send Notification to Email | Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications cannot be sent via e-mail. |
| Interval | Enter the interval of how many minutes you want the Device to e-mail you. |
| Enable Log | Select this to activate the logging function at the interval you set in this field. |
| Basic | Click this to hide the advanced settings of 3G backup. |
| Apply | Click **Apply** to save your changes back to the Device. |
| Cancel | Click **Cancel** to return to the previous configuration. |

# 4.4 The Advanced Screen

Use the **Advanced** screen to enable or disable ADSL over PTM, Annex M, DSL PhyR, and SRA (Seamless Rate Adaption) functions. The Device supports the PhyR retransmission scheme. PhyR is a retransmission scheme designed to provide protection against noise on the DSL line. It improves voice, video and data transmission resilience by utilizing a retransmission buffer.

Click **Network Setting > Broadband** > **Advanced** to display the following screen.

**Figure 29** Network Setting **>** Broadband > Advanced




The following table describes the labels in this screen.

**Table 10** Network Setting **>** Network Setting > Broadband

| LABEL | DESCRIPTION |
|---|---|
| ADSL over PTM | Select **Enable** to use ADSL over PTM. Since PTM has less overhead than ATM, some ISPs use ADSL over PTM for better performance. |
| Annex M | You can enable **Annex M** for the Device to use double upstream mode to increase the maximum upstream transfer rate. |
| PhyR US | Enable or disable **PhyR US** (upstream) for upstream transmission to the WAN. PhyR US should be enabled if data being transmitted upstream is sensitive to noise. However, enabling PhyR US can decrease the US line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled. |

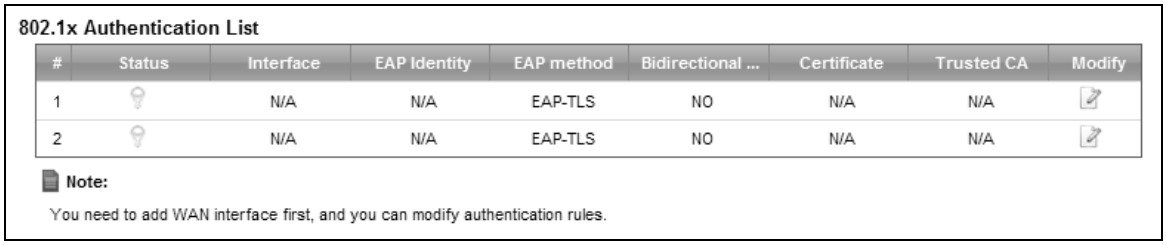
**Table 10** Network Setting **>** Network Setting > Broadband (continued)

| LABEL | DESCRIPTION |
|---|---|
| PhyR DS | Enable or disable **PhyR DS** (downstream) for downstream transmission from the WAN. PhyR DS should be enabled if data being transmitted downstream is sensitive to noise. However, enabling PhyR DS can decrease the DS line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled. |
| SRA | Enable or disable Seamless Rate Adaption (SRA). Select **Enable** to have the Device automatically adjust the connection's data rate according to line conditions without interrupting service. |
| Apply | Click **Apply** to save your changes back to the Device. |
| Cancel | Click **Cancel** to return to the previous configuration. |

# 4.5 The 802.1x Screen

You can view and configure the 802.1X authentication settings in the **802.1x** screen. Click **Network Setting** > **Broadband** > **802.1x** to display the following screen.

**Figure 30** Network Setting > Broadband > 802.1x




The following table describes the labels in this screen.

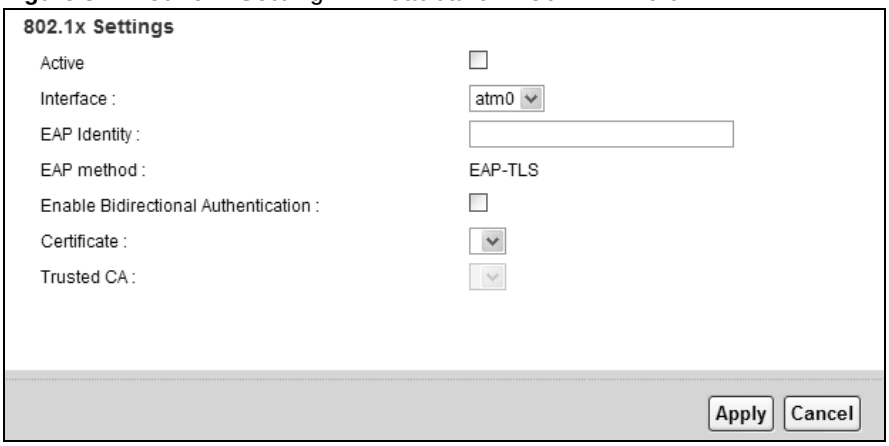
**Table 11** Network Setting > Network Setting > 802.1x

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the entry. |
| Status | This field displays whether the authentication is active or not. A yellow bulb signifies that this authentication is active. A gray bulb signifies that this authentication is not active. |
| Interface | This is the interface that uses the authentication. This displays **N/A** when there is no interface assigned. |
| EAP Identity | This shows the EAP identity of the authentication. This displays **N/A** when there is no EAP identity assigned. |
| EAP method | This shows the EAP method used in the authentication. This displays **N/A** when there is no EAP method assigned. |
| Bidirectional Authentication | This shows whether bidirectional authentication is allowed. |
| Certificate | This shows the certificate used for this authentication. This displays **N/A** when there is no certificate assigned. |
| Trusted CA | This shows the Trusted CA used for this authentication. This displays **N/A** when there is no Trusted CA assigned. |
| Apply | Click **Apply** to save your changes back to the Device. |
| Cancel | Click **Cancel** to return to the previous configuration. |

### 4.5.1 Edit 802.1X Settings

Use this screen to edit 802.1X authentication settings. Click the **Edit** icon next to the rule you want to edit. The screen shown next appears.

**Figure 31** Network Setting **>** Broadband > 802.1x: Edit




The following table describes the labels in this screen.

**Table 12** Network Setting **>** Broadband > 802.1x: Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | This field allows you to activate/deactivate the authentication.<br><br>Select this to enable the authentication. Clear this to disable this authentication without having to delete the entry. |
| Interface | Select an interface to which the authentication applies. |
| EAP Identity | Enter the EAP identity of the authentication. |
| EAP method | This is the EAP method used for this authentication. |
| Enable Bidirectional Authentication | Select this to allow bidirectional authentication. |
| Certificate | Select the certificate you want to assign to the authentication. You need to import the certificate in the **Security** > **Certificates** > **Local Certificates** screen. |
| Trusted CA | Select the Trusted CA you want to assign to the authentication. You need to import the certificate in the **Security** > **Certificates** > **Trusted CA** screen. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 4.6 Technical Reference

The following section contains additional technical information about the Device features described in this chapter.

## Encapsulation

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

## IP over Ethernet

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

## PPP over ATM (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 access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

## PPP over Ethernet (PPPoE)

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

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

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

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

By implementing PPPoE directly on the 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.

## RFC 1483

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

## Multiplexing

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

VC-based Multiplexing

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

LLC-based Multiplexing

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

## Traffic Shaping

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

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

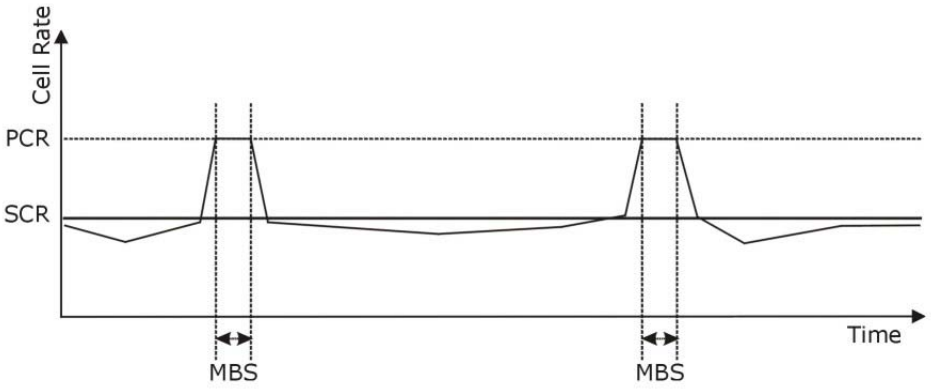
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

**Figure 32** Example of Traffic Shaping




## ATM Traffic Classes

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

Constant Bit Rate (CBR)

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

Variable Bit Rate (VBR)

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

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

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

Unspecified Bit Rate (UBR)

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

## IP Address Assignment

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

## Introduction to VLANs

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

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

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

## Introduction to IEEE 802.1Q Tagged VLAN

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

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

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

## Multicast

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

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

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

## DNS Server Address Assignment

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

The Device can get the DNS server addresses in the following ways.

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

## IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

## IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address

compose the network address. The prefix length is written as “/x” where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (2001:db8) is the subnet prefix.

# 5

# Wireless

## 5.1 Overview

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

### 5.1.1 What You Can Do in this Chapter

This section describes the Device's **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 70).
- Use the **More AP** screen to set up multiple wireless networks on your Device (Section 5.3 on page 77).
- 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 81).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 5.5 on page 82).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications (Section 5.6 on page 83).
- Use the **WDS** screen to set up a Wireless Distribution System, in which the Device acts as a bridge with other ZyXEL access points (Section 5.7 on page 84).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold (Section 5.8 on page 86).
- Use the **Channel Status** screen to scan wireless LAN channel noises and view the results (Section 5.9 on page 89).

### 5.1.2 What You Need to Know

#### 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 89 for advanced technical information on wireless networks.

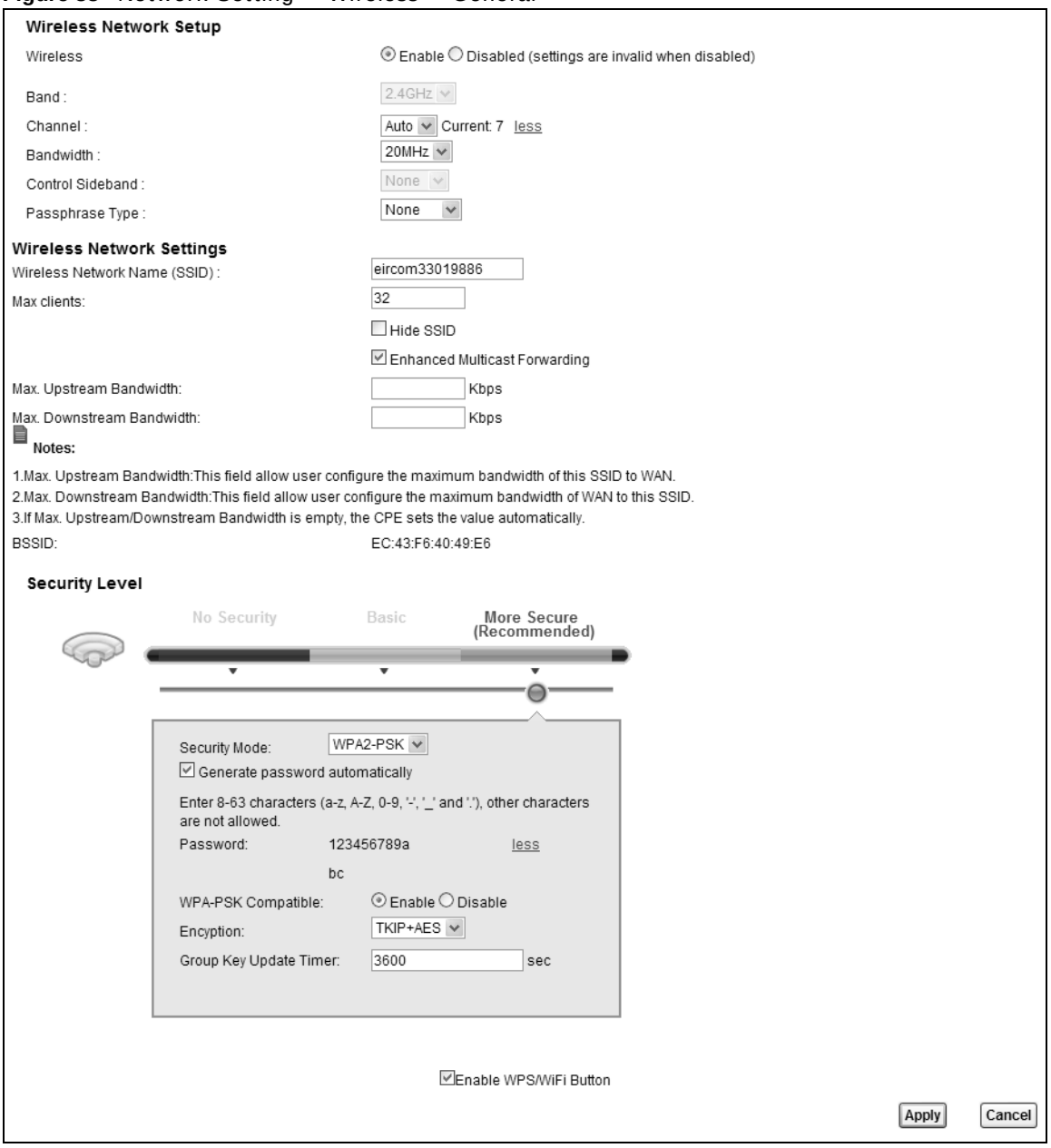
## 5.2 The General Screen

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 33** Network Setting > Wireless > General




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

**Table 13** Network Setting > Wireless > General

| LABEL | DESCRIPTION |
|---|---|
| Wireless Network Setup | |
| Wireless | You can **Enable** or **Disable** the wireless LAN in this field. |
| Band | This shows the wireless band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n wireless clients. |

**Table 13** Network Setting > Wireless > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Channel | Set the channel depending on your particular region.<br><br>Select a channel or use **Auto** to have the Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the Device is currently using then displays next to this field. |
| more.../less | Click **more...** to show more information. Click **less** to hide them. |
| Bandwidth | Select whether the Device uses a wireless channel width of **20MHz** or **40MHz**.<br><br>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.<br><br>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.<br><br>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. |
| Control Sideband | This is available for some regions when you select a specific channel and set the Bandwidth field to **40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands. |
| Passphrase Type | If you set security for the wireless LAN and have the Device generate a password, the setting in this field determines how the Device generates the password.<br><br>Select **None** to set the Device's password generation to not be based on a passphrase.<br><br>Select **Fixed** to use a 16 character passphrase for generating a password.<br><br>Select **Variable** to use a 16 to 63 character passphrase for generating a password. |
| Passphrase Key | For a fixed type passphrase enter 16 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive.<br><br>For a variable type passphrase enter 16 to 63 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive. |
| 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.<br><br>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN. |
| Max clients | Specify the maximum number of clients that can connect to this network at the same time. |
| 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. |
| Enhanced Multicast Forwarding | Select this check box to allow the Device to convert wireless multicast traffic into wireless unicast traffic. |
| Max. Upstream Bandwidth | Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps). |
| Max. Downstream Bandwidth | Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps). |
| BSSID | This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled. |
| Security Level | |

**Table 13** Network Setting > Wireless > General (continued)

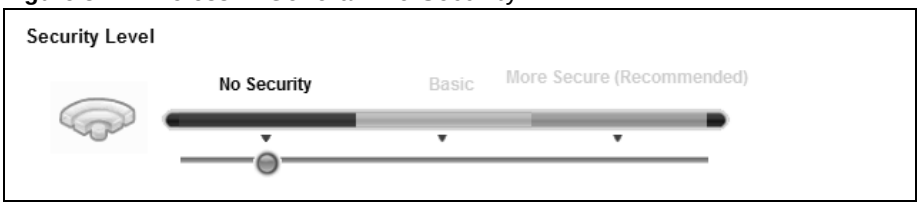
| LABEL | DESCRIPTION |
|---|---|
| Security Mode | Select **Basic (WEP, 802.1X)** or **More Secure (WPA(2)-PSK, WPA(2))** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. When you select to use a security, additional options appears in this screen.<br><br>Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication.<br><br>See the following sections for more details about this field. |
| Enable WPS/ WiFi Button | Select this to allow the WPS and WiFi buttons on the rear panel of the Device to control the corresponding functions. Clear this to disable both buttons. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** 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 34** Wireless > General: No Security




The following table describes the labels in this screen.

**Table 14** Wireless > General: No Security

| LABEL | DESCRIPTION |
|---|---|
| Security Level | Choose **No Security** to allow all wireless connections without data encryption or authentication. |

## 5.2.2 Basic (WEP Encryption)

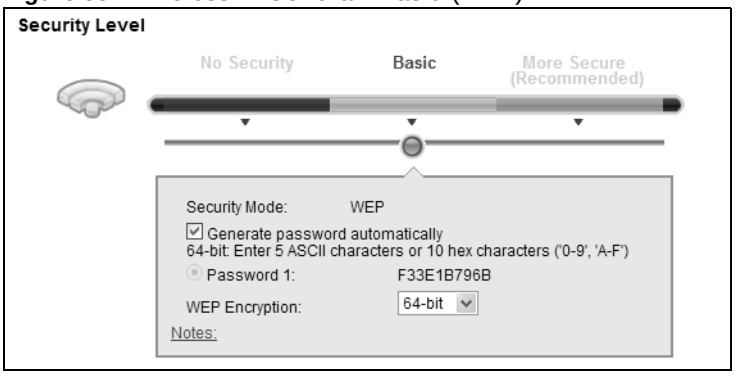
WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

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 up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

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 35** Wireless > General: Basic (WEP)




The following table describes the labels in this screen.

**Table 15** Wireless > General: Basic (WEP)

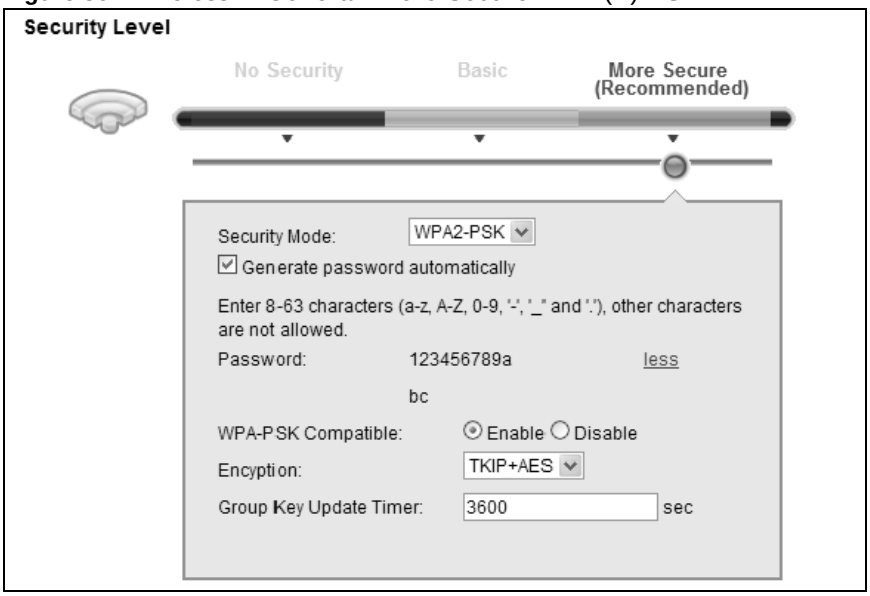
| LABEL | DESCRIPTION |
|---|---|
| Security Level | Select **Basic** to enable WEP data encryption. |
| Generate password automatically | Select this option to have the Device automatically generate a password. The password field will not be configurable when you select this option. |
| Password 1 | The password (WEP key) is used to encrypt data. Both the Device and the wireless stations must use the same password (WEP key) for data transmission.<br>If you chose **64-bit** WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").<br>If you chose **128-bit** WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). |
| password unmask | This field is available when the **Generate password automatically** checkbox is cleared. Select **password unmask** to show your entered password in plain text. |
| WEP Encryption | Select **64-bits** or **128-bits**.<br>This dictates the length of the security key that the network is going to use. |
| Notes | Click **Notes:** to show more information about the WEP key. |

## 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 36** Wireless > General: More Secure: WPA(2)-PSK




The following table describes the labels in this screen.

**Table 16** 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. |
| 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 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.<br><br>If you did not select **Generate password automatically**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters. |
| more.../less | Click **more...** to show more fields in this section. Click **less** to hide them. |
| WPA-PSK Compatible | This field appears when you choose **WPA-PSK2** as the **Security Mode**.<br><br>Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your Device. The Device supports WPA-PSK and WPA2-PSK simultaneously. |

**Table 16** Wireless > General: More Secure: WPA(2)-PSK (continued)

| LABEL | DESCRIPTION |
|---|---|
| Encryption | Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption.<br>Select **TKIP** if your wireless clients can all use TKIP.<br>Select **AES** if your wireless clients can all use AES.<br>Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES. |
| 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. |

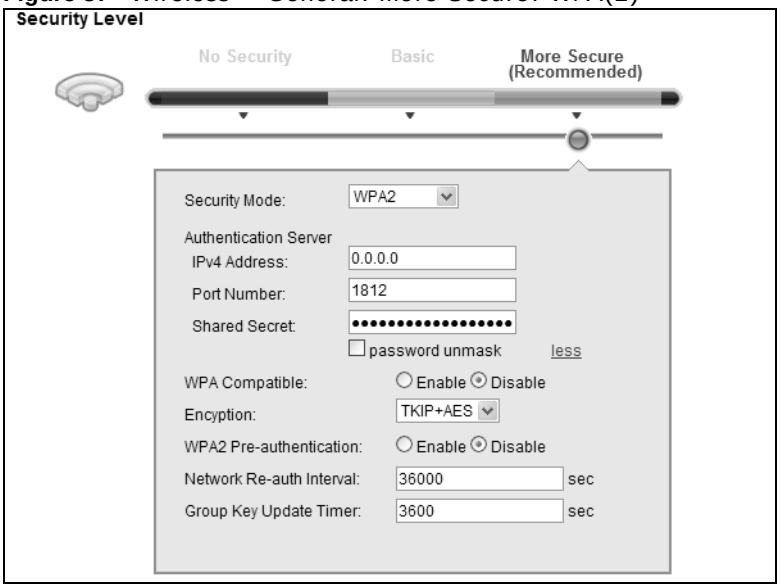
## 5.2.4 WPA(2) Authentication

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 37** Wireless > General: More Secure: WPA(2)




The following table describes the labels in this screen.

**Table 17** Wireless > General: More Secure: WPA(2)

| LABEL | DESCRIPTION |
|---|---|
| Security Level | Select **More Secure** to enable WPA(2)-PSK data encryption. |
| Security Mode | Choose **WPA** or **WPA2** from the drop-down list box. |
| Authentication Server | |

**Table 17** Wireless > General: More Secure: WPA(2) (continued)

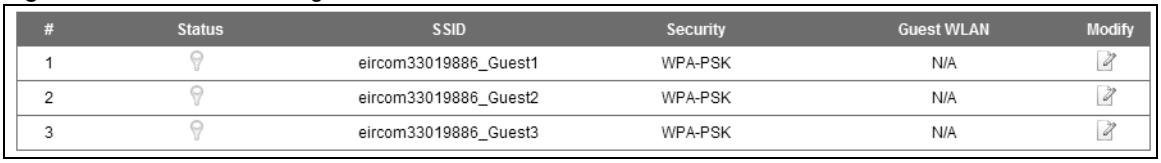
| LABEL | DESCRIPTION |
|---|---|
| IP Address | Enter the IP address of the external authentication server in dotted decimal notation. |
| Port Number | Enter the port number of the external authentication server. The default port number is **1812**.<br>You need not change this value unless your network 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.<br>The key must be the same on the external authentication server and your Device. The key is not sent over the network.<br>Select **password unmask** to show your entered password in plain text. |
| more.../less | Click **more...** to show more fields in this section. Click **less** to hide them. |
| WPA Compatible | This field is only available for WPA2. Select this if you want the Device to support WPA and WPA2 simultaneously. |
| Encryption | Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption.<br>Select **TKIP** if your wireless clients can all use TKIP.<br>Select **AES** if your wireless clients can all use AES.<br>Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES. |
| WPA2 Pre-Authentication | This field is available only when you select **WPA2**.<br>Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Select **Enabled** to turn on preauthentication in WAP2. Otherwise, select **Disabled**. |
| Network Re-auth Interval | Specify how often wireless stations have to resend usernames and passwords in order to stay connected.<br>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. |
| 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. |

# 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 38** Network Setting > Wireless > More AP



The following table describes the labels in this screen.

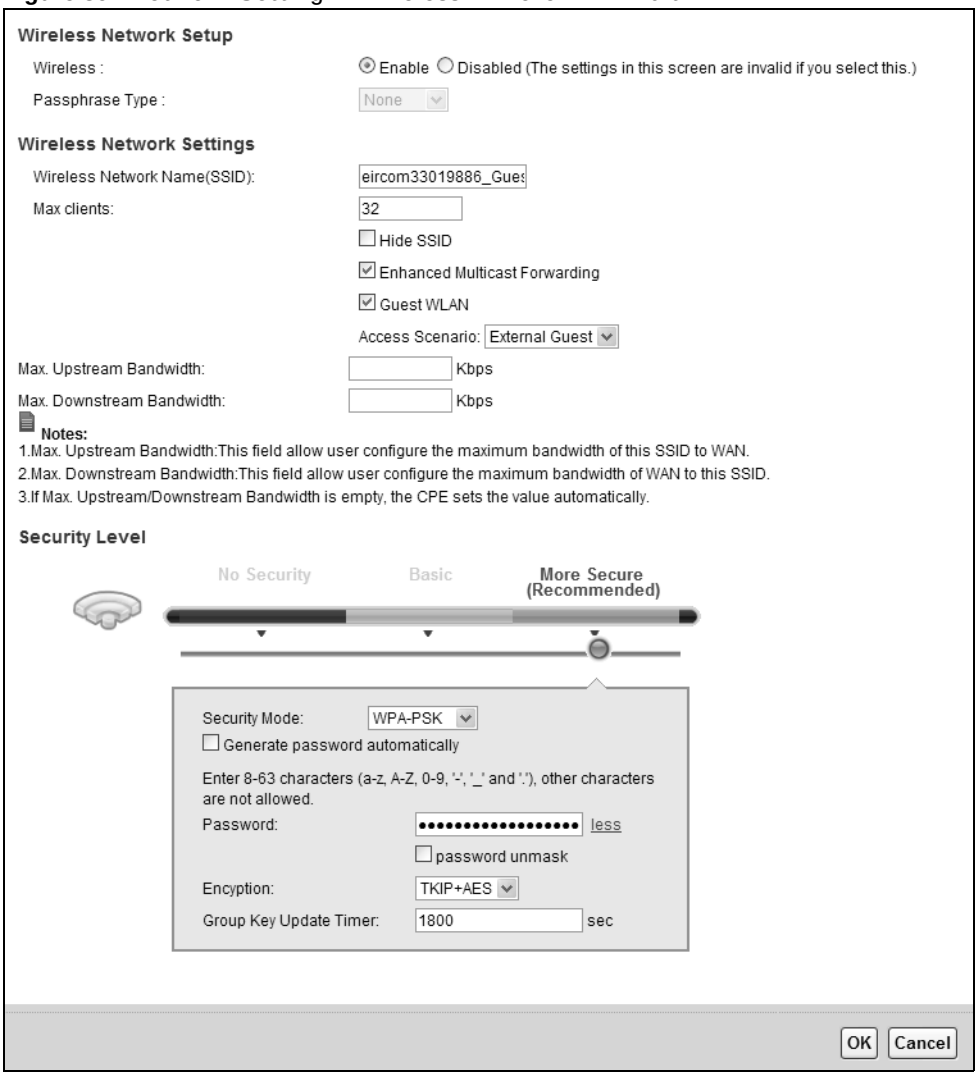
**Table 18** Network Setting > Wireless > More AP

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the entry. |
| Status | 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.<br>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. |
| Guest WLAN | This displays if the guest WLAN function has been enabled for this WLAN.<br>If **Home Guest** displays, clients can connect to each other directly.<br>If **External Guest** displays, clients are blocked from connecting to each other directly.<br>**N/A** displays if guest WLAN is disabled. |
| Modify | Click the **Edit** icon to configure the SSID profile. |

## 5.3.1 Edit More AP

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 39** Network Setting > Wireless > More AP > Edit




The following table describes the fields in this screen.

**Table 19** Network Setting > Wireless > More AP > Edit

| LABEL | DESCRIPTION |
|---|---|
| Wireless Network Setup | |
| Wireless | You can **Enable** or **Disable** the wireless LAN in this field. |
| Passphrase Type | Passphrase type cannot be changed. The default is **None**. |
| 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.<br><br>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN. |

**Table 19** Network Setting > Wireless > More AP > Edit (continued)

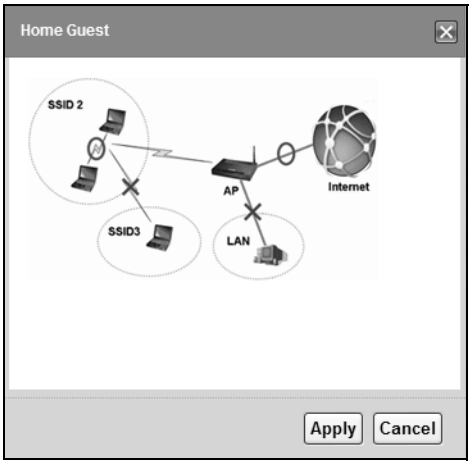
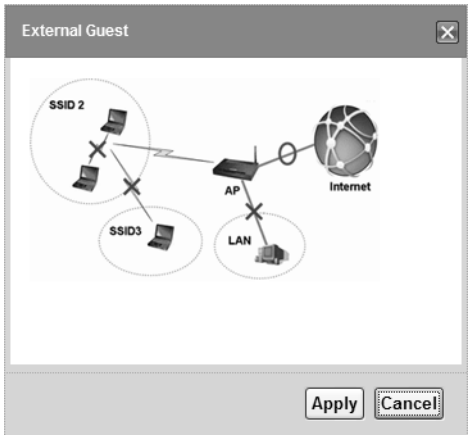
| LABEL | DESCRIPTION |
|---|---|
| Max clients | Specify the maximum number of clients that can connect to this network at the same time. |
| Hide SSID | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |
| Enhanced Multicast Forwarding | Select this check box to allow the Device to convert wireless multicast traffic into wireless unicast traffic. |
| Guest WLAN | Select this to create Guest WLANs for home and external clients. Select the WLAN type in the **Access Scenario** field. |
| Access Scenario | If you select **Guest Home**, clients can connect to each other directly. A **Home Guest** screen appears. A graphic shows whether the wireless clients can access other clients in the same wireless network and in other networks. Click **Apply** to save the change before closing the screen. Click **Cancel** to close the screen without saving the change.<br>  <br>If you select **External Guest**, clients are blocked from connecting to each other directly. A **External Guest** screen appears. A graphic shows whether the wireless clients can access other clients in the same wireless network and in other networks. Click **Apply** to save the change before closing the screen. Click **Cancel** to close the screen without saving the change.<br>  |
| Max. Upstream Bandwidth | Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps). |
| Max. Downstream Bandwidth | Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps). |

**Table 19** Network Setting > Wireless > More AP > Edit (continued)

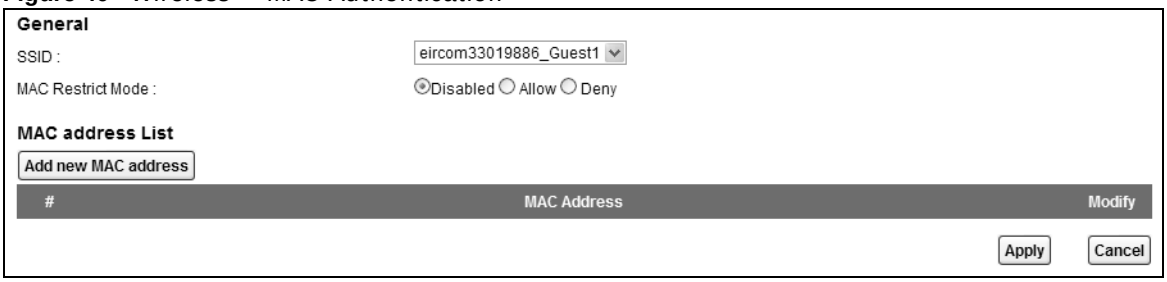
| LABEL | DESCRIPTION |
|---|---|
| Security Level | |
| Security Mode | Select **Basic (WEP, 802.1X)** or **More Secure (WPA(2)-PSK, WPA(2))** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. After you select to use a security, additional options appears in this screen.<br>Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication.<br>See Section 5.2.1 on page 73 for more details about this field. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 5.4 MAC Authentication

This screen allows you to configure the ZyXEL Device to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the ZyXEL 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 40** Wireless > MAC Authentication




The following table describes the labels in this screen.

**Table 20** 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.<br>Select **Disable** to turn off MAC filtering.<br>Select **Deny** to block access to the Device. MAC addresses not listed will be allowed to access the Device.<br>Select **Allow** to permit access to the Device. MAC addresses not listed will be denied access to the Device. |

**Table 20** Wireless > MAC Authentication (continued)

| LABEL | DESCRIPTION |
|---|---|
| Add new MAC address | Click this if you want to add a new MAC address entry to the MAC filter list below.<br>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. |
| Delete | 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

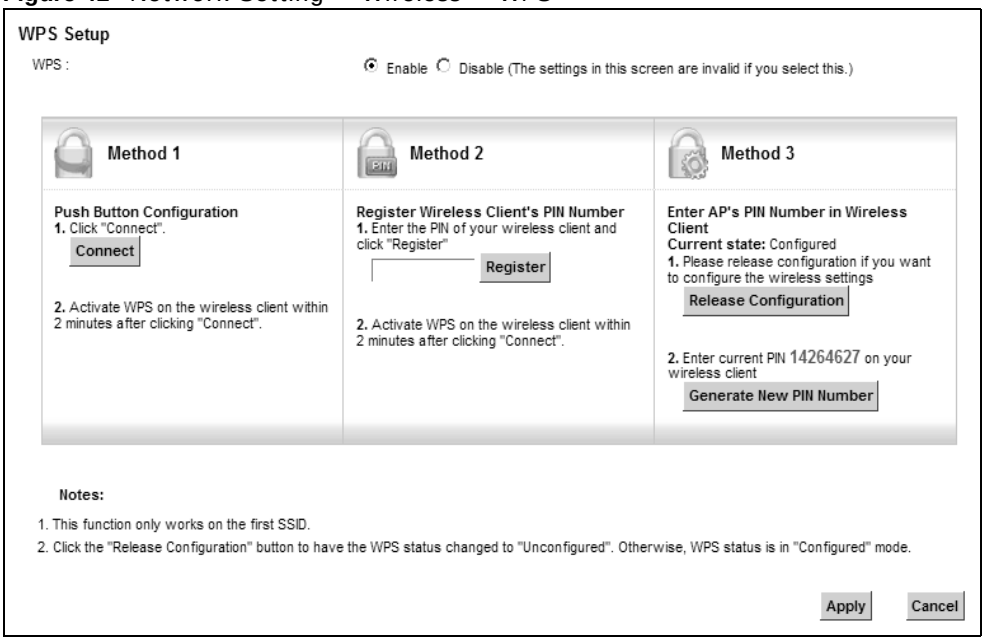
Use this screen to configure WiFi Protected Setup (WPS) on your Device.

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 5.10.9.3 on page 98 for more information about WPS.

Note: The Device applies the security settings of the **SSID1** profile (see Section 5.2 on page 70). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **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 41** Network Setting > Wireless > WPS



The following table describes the labels in this screen.

**Table 21** Network Setting > Wireless > WPS

| LABEL | DESCRIPTION |
|---|---|
| WPS | Select **Enable** to activate WPS on the Device. |
| Method 1 | Use this section to set up a WPS wireless network using Push Button Configuration (PBC). |
| Connect | 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 **Connect** button on this screen.<br><br>Note: You must press the other wireless device's WPS button within two minutes of pressing this button. |
| Method 2 | 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.<br><br>You can find the PIN either on the outside of the device, or by checking the device's settings.<br><br>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Device. |
| Method 3 | Use this section to set up a WPS wireless network by entering the PIN of the Device into the client. |
| Release Configuration | The default WPS status is configured.<br><br>Click this button to remove all configured wireless and wireless security settings for WPS connections on the Device. |
| Generate New PIN Number | 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.<br><br>The PIN is not necessary when you use WPS push-button method.<br><br>Click the **Generate New PIN Number** button to have the Device create a new PIN. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 5.6 The WMM Screen

Use this screen to enable Wi-Fi MultiMedia (WMM) and WMM Power Save in wireless networks for multimedia applications.

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

**Figure 42** Network Setting > Wireless > WMM

The following table describes the labels in this screen.

**Table 22** Network Setting > Wireless > WMM

| LABEL | DESCRIPTION |
|---|---|
| WMM | Select **On** to have the Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. |
| WMM Automatic Power Save Delivery | Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the Device until the Device "wakes up". The Device wakes up periodically to check for incoming data.<br><br>Note: Note: This works only if the wireless device to which the Device is connected also supports this feature. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 5.7 The WDS Screen

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

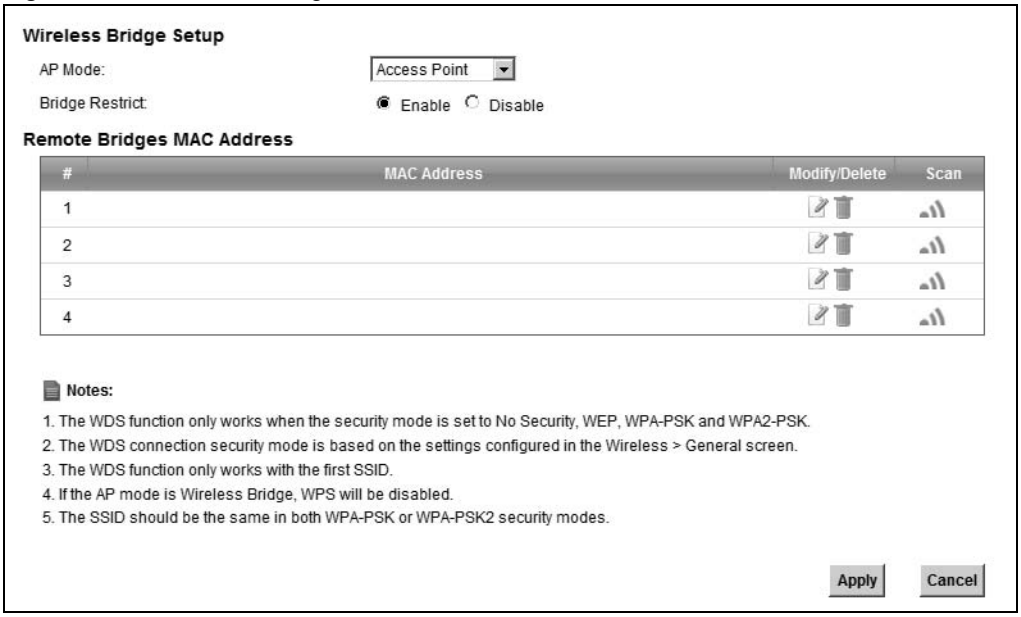
Use this screen to set up your WDS (Wireless Distribution System) links between the Device and other wireless APs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between devices is made.

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

Note: At the time of writing, WDS is compatible with other ZyXEL APs only. Not all models support WDS links. Check your other AP's documentation.

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

**Figure 43** Network Setting > Wireless > WDS




The following table describes the labels in this screen.

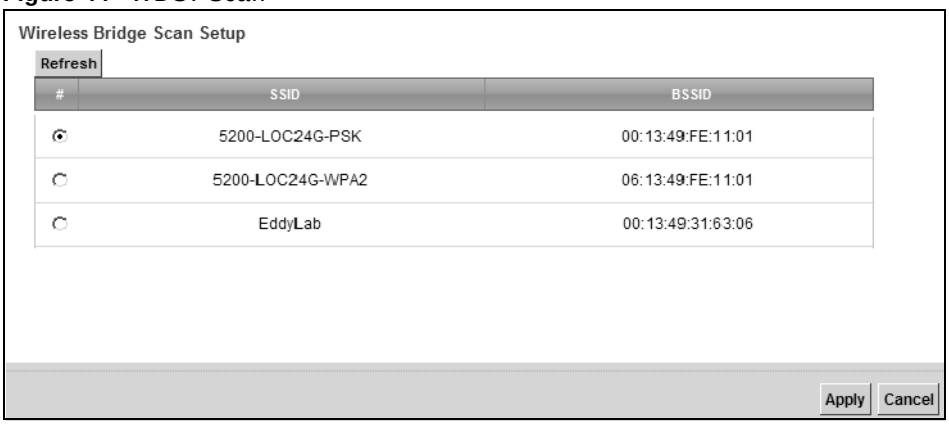
**Table 23** Network Setting > Wireless > WDS

| LABEL | DESCRIPTION |
|---|---|
| Wireless Bridge Setup | |
| AP Mode | Select the operating mode for your Device.<br>• **Access Point** - The Device functions as a bridge and access point simultaneously.<br>• **Wireless Bridge** - The Device acts as a wireless network bridge and establishes wireless links with other APs. In this mode, clients cannot connect to the Device wirelessly. |
| Bridge Restrict | This field is available only when you set operating mode to **Access Point**.<br>Select **Enabled** to turn on WDS and enter the peer device's MAC address manually in the table below. Select **Disable** to turn off WDS. |
| Remote Bridge MAC Address | You can enter the MAC address of the peer device by clicking the **Edit** icon under **Modify**. |
| # | This is the index number of the entry. |
| MAC Address | This shows the MAC address of the peer device.<br>You can connect to up to 4 peer devices. |
| Modify | Click the **Edit** icon and 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).<br>Click the **Delete** icon to remove this entry. |
| Scan | Click the **Scan** icon to search and display the available APs within range. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

### 5.7.1 WDS Scan

You can click the **Scan** icon in **Wireless > WDS** to have the Device automatically search and display the available APs within range. Select an AP and click **Apply** to have the Device establish a wireless link with the selected wireless device.

**Figure 44** WDS: Scan




The following table describes the labels in this screen.

**Table 24** WDS: Scan

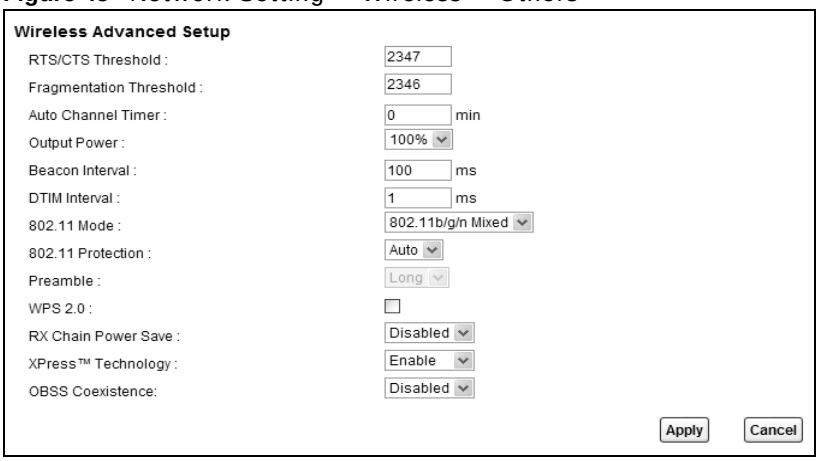
| LABEL | DESCRIPTION |
|---|---|
| Wireless Bridge Scan Setup | |
| Refresh | Click **Refresh** to update the table. |
| # | This is the index number of the entry. |
| SSID | This shows the SSID of the available wireless device within range. |
| BSSID | This shows the MAC address of the available wireless device within range. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

## 5.8 The Others Screen

Use this screen to configure advanced wireless settings. Click **Network Setting > Wireless > Others**. The screen appears as shown.

See Section 5.10.2 on page 91 for detailed definitions of the terms listed in this screen.

**Figure 45** Network Setting > Wireless > Others




The following table describes the labels in this screen.

**Table 25** Network Setting > Wireless > Others

| LABEL | DESCRIPTION |
|---|---|
| RTS/CTS Threshold | Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake.<br><br>Enter a value between 0 and 2347. |
| Fragmentation Threshold | This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346. |
| Auto Channel Timer | If you set the channel to **Auto** in the **Network Setting > Wireless > General** screen, specify the interval in minutes for how often the Device scans for the best channel. Enter 0 to disable the periodical scan. |
| 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: **20%**, **40%**, **60%**, **80%** or **100%**. |
| Beacon Interval | When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again.<br><br>The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50ms to 1000ms. A high value helps save current consumption of the access point. |
| DTIM Interval | Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255. |

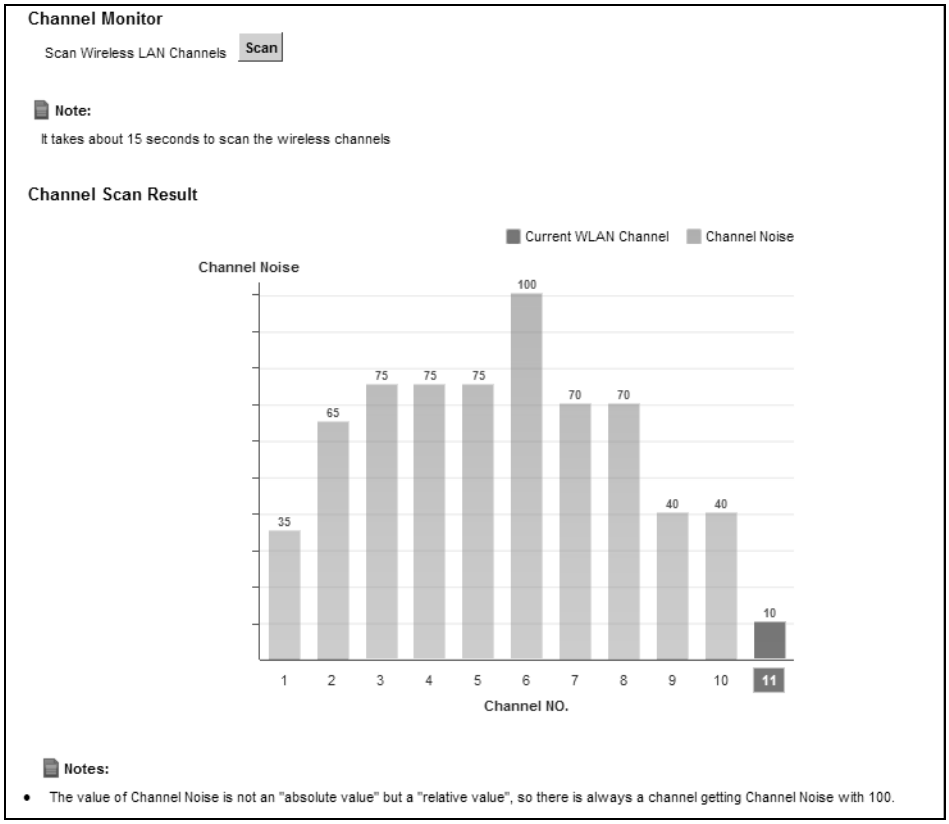
**Table 25** Network Setting > Wireless > Others (continued)

| LABEL | DESCRIPTION |
|---|---|
| 802.11 Mode | Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Device.<br><br>Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Device.<br><br>Select **802.11n Only** to allow only IEEE 802.11n compliant WLAN devices to associate with the Device.<br><br>Select **802.11b/g Mixed** 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.<br><br>Select **802.11b/g/n Mixed** 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. |
| 802.11 Protection | Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).<br><br>Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.<br><br>Select **Off** to disable 802.11 protection. The transmission rate of your Device might be reduced in a mixed-mode network.<br><br>This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**. |
| Preamble | Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 5.10.7 on page 95 for more information.<br><br>This field is configurable only when you set 802.11 Mode to **802.11b**. |
| WPS 2.0 | Select this to support WPS 2.0. |
| RX Chain Power Save | Select **Enable** to activate the RX Chain Power Save feature. It turns off one of the Receive chains to save power. |
| XPress™ Technology | Select **Enable** for higher speeds, especially if you have both IEEE 802.11b and IEEE 802.11g wireless clients. The wireless clients do not have to support XPress™ Technology, although the performance enhancement is greater if they do. |
| OBSS Coexistence | Select **Enable** to allow coexistence between 20 MHz and 40 MHz Overlapping Basic Service Sets (OBSS) in wireless local area networks. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 5.9 The Channel Status Screen

Use the **Channel Status** screen to scan wireless LAN channel noises and view the results. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown. Click **Scan** to scan the wireless LAN channels. You can view the results in the **Channel Scan Result** section.

**Figure 46** Network Setting > Wireless > Channel Status




# 5.10 Technical Reference

This section discusses wireless LANs in depth. For more information, see Appendix D on page 325.

## 5.10.1 Wireless Network Overview

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

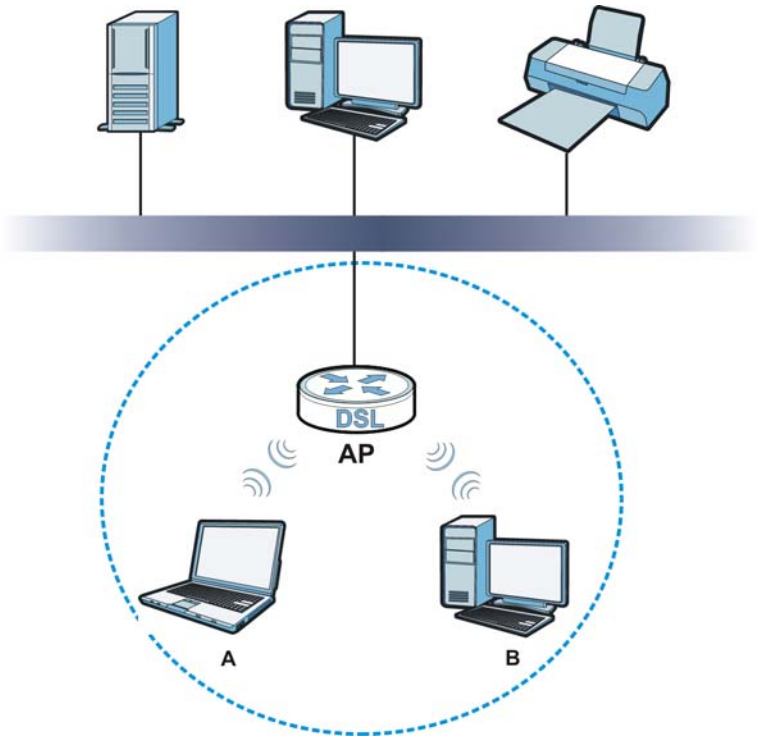
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, 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 47** 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 26** Additional Wireless Terms

| TERM | DESCRIPTION |
|---|---|
| RTS/CTS Threshold | In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.<br><br>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the Device. The lower the value, the more often the devices must get permission.<br><br>If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the Device. |
| 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.

### 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

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.

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 92 for information about this.)

**Table 27** 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. 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

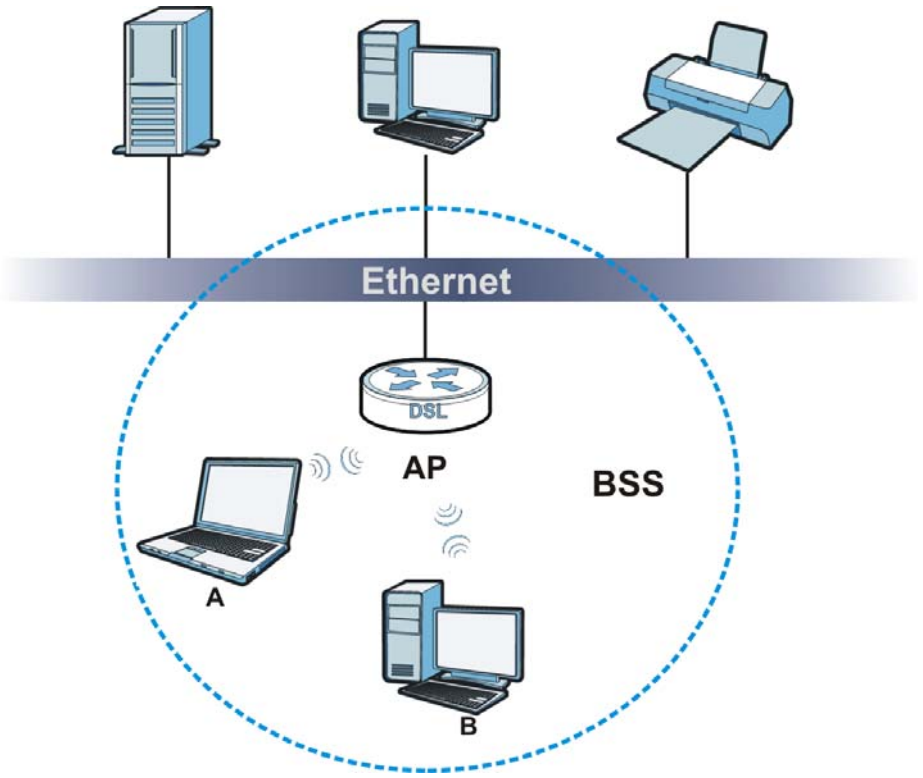
coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

## 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 48** 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 Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the Device uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

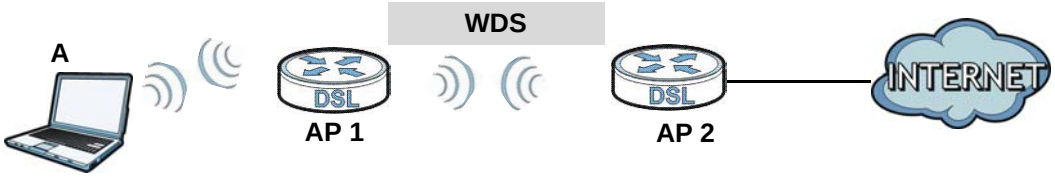
## 5.10.8 Wireless Distribution System (WDS)

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 compatible with other ZyXEL access points only. 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 49** WDS Link Example




## 5.10.9 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.

### 5.10.9.1 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 83).
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.

### 5.10.9.2 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.

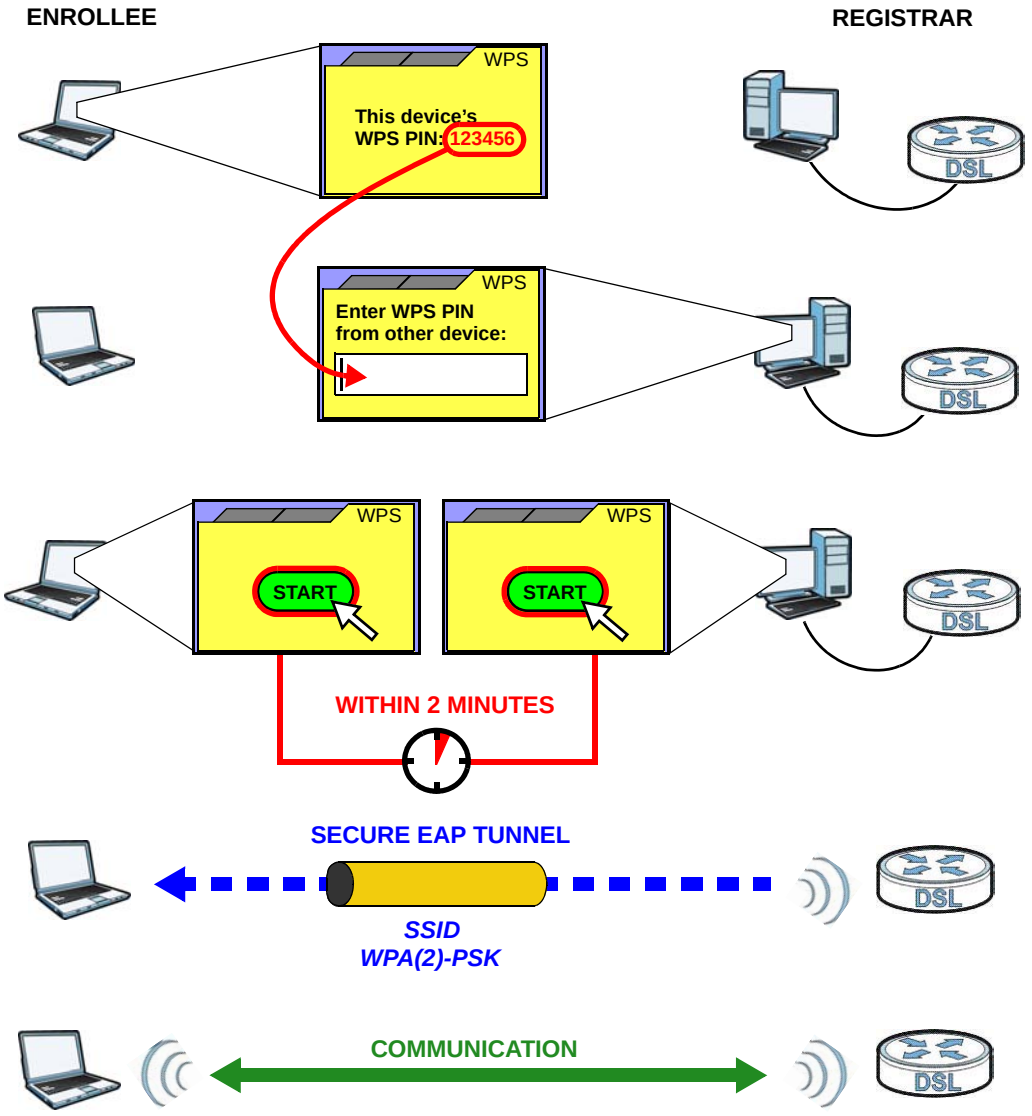
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

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 82).
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 50** Example WPS Process: PIN Method

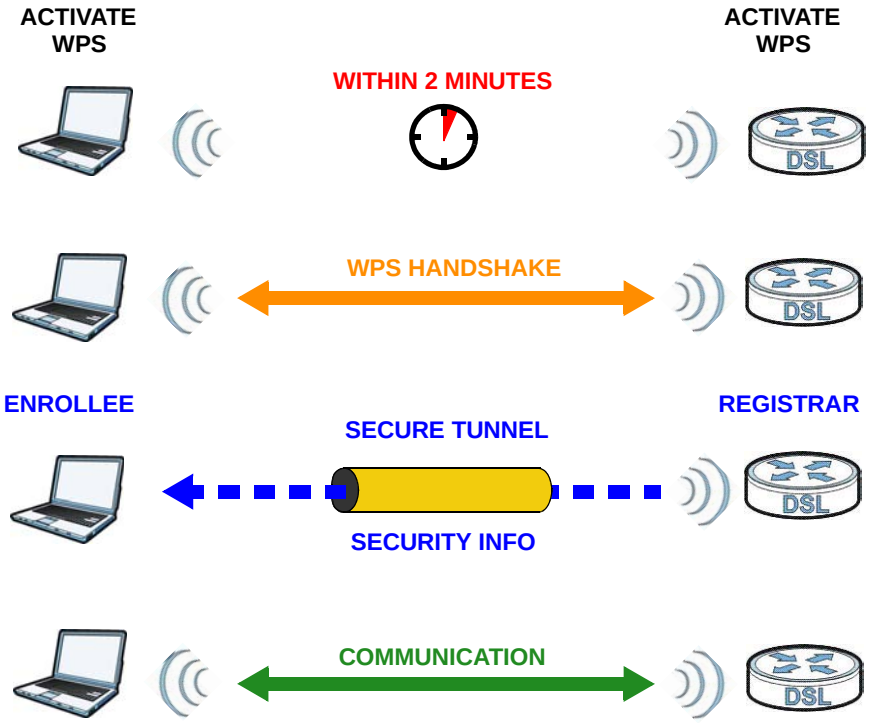



## 5.10.9.3 How WPS Works

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 51** 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.

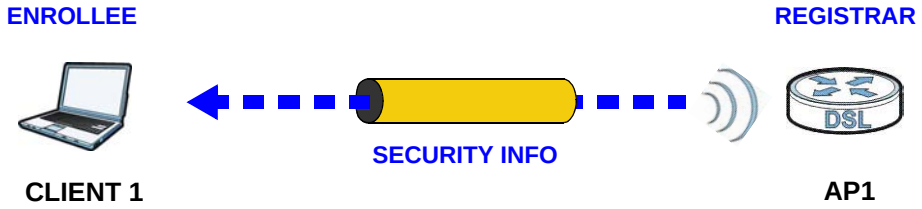
### 5.10.9.4 Example WPS Network Setup

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**

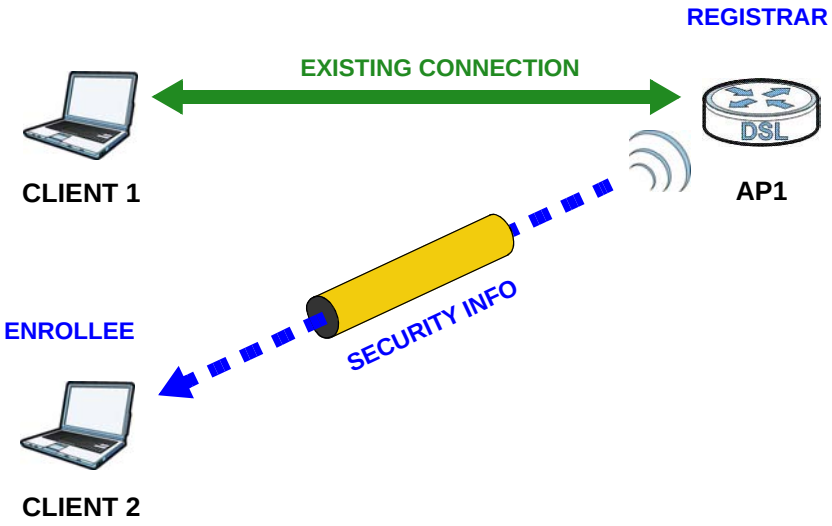
is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

**Figure 52** WPS: Example Network Step 1



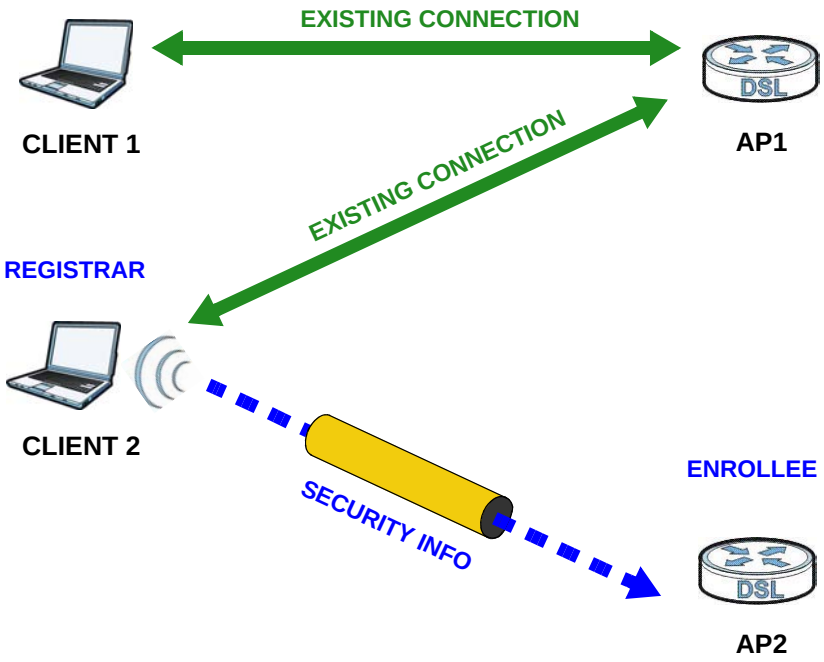

In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the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

**Figure 53** 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 54** WPS: Example Network Step 3




### 5.10.9.5 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.

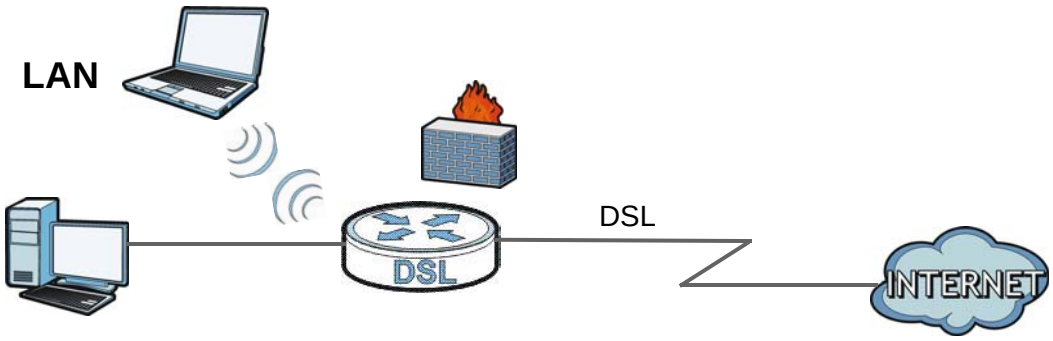
# 6

# 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 this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your Device (Section 6.2 on page 105).
- 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 109).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the Device (Section 6.4 on page 110).
- Use the **Additional Subnet** screen to configure IP alias and public static IP (Section 6.7 on page 120).
- Use the **STB Vendor ID** screen to have the Device automatically create static DHCP entries for Set Top Box (STB) devices when they request IP addresses (Section 6.8 on page 121)
- Use the **5th Ethernet Port** screen to configure the **WAN** port as the Ethernet WAN port or a LAN port (Section 6.9 on page 121).
- Use the **LAN VLAN** screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent out through individual LAN ports (Section 6.10 on page 122).
- Use the **Wake on Lan** screen to remotely turn on a device on the network. (Section 6.11 on page 123).

## 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.

#### RADVD (Router Advertisement Daemon)

When an IPv6 host sends a Router Solicitation (RS) request to discover the available routers, RADVD with Router Advertisement (RA) messages in response to the request. It specifies the minimum and maximum intervals of RA broadcasts. RA messages containing the address prefix. IPv6 hosts can be generated with the IPv6 prefix an IPv6 address.

### 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.

See the Chapter 9 on page 153 for more information on NAT.

### Cautions with UPnP

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

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the 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.

### UPnP and ZyXEL

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

See Section 6.5 on page 111 for examples of installing and using UPnP.

### Finding Out More

See Section 6.12 on page 124 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 and subnet mask of your Device. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

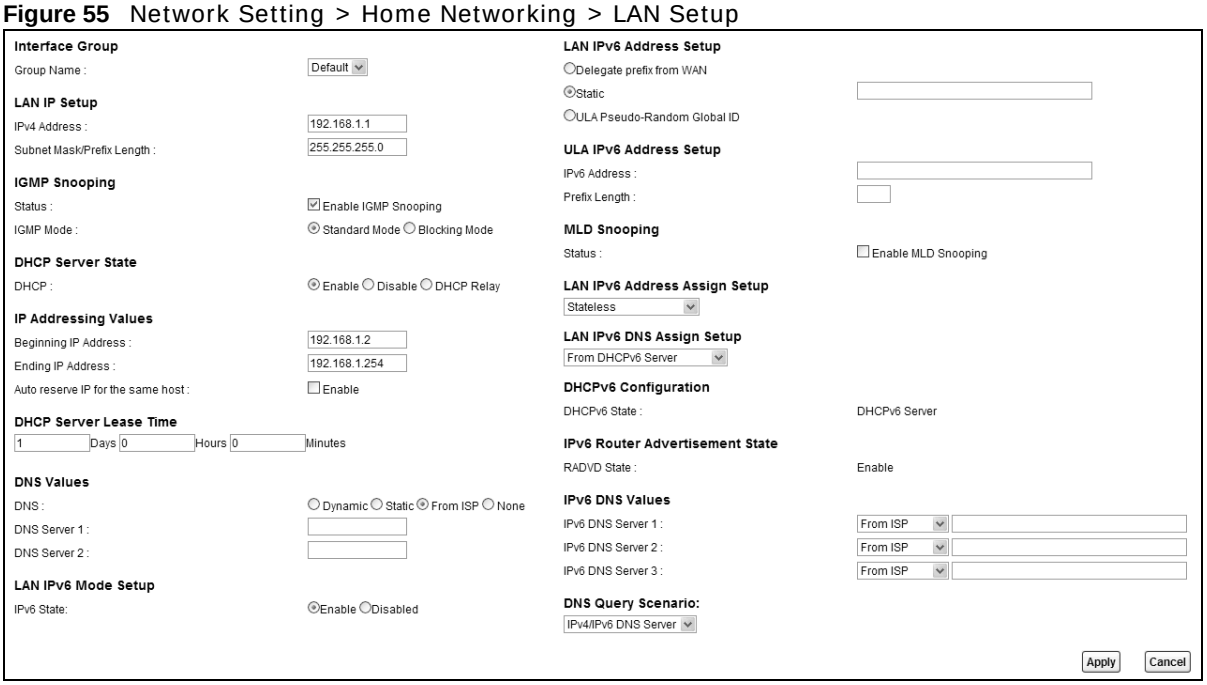
Follow these steps to configure your LAN settings.

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

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

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

**Figure 55** Network Setting > Home Networking > LAN Setup




The following table describes the fields in this screen.

**Table 28** Network Setting > Home Networking > LAN Setup

| LABEL | DESCRIPTION |
|---|---|
| Interface Group | |
| Group Name | Select the interface group name for which you want to configure LAN settings. See Chapter 11 on page 175 for how to create a new interface group. |
| LAN IP Setup | |
| IPv4 Address | Enter the LAN IPv4 IP address you want to assign to your Device in dotted decimal notation, for example, 192.168.1.1 (factory default). |
| Subnet Mask/ Prefix Length | 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. |
| IGMP Snooping | |
| Status | Select the **Enable IGMP Snooping** checkbox to allows the Device to passively learn multicast group. |
| IGMP Mode | Select **Standard Mode** to have the Device forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports.<br>Select **Blocking Mode** to have the Device block all unknown multicast packets from the WAN. |
| DHCP Server State | |
| DHCP | Select **Enable** to have the Device act as a DHCP server or DHCP relay agent.<br>Select **Disable** to stop the DHCP server on the Device.<br>Select **DHCP Relay** to have the Device forward DHCP request to the DHCP server. |
| DHCP Relay Server Address | This field is only available when you select **DHCP Relay** in the **DHCP** field. |

**Table 28** Network Setting > Home Networking > LAN Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| IPv4 Address | Enter the IPv4 IP address of the actual remote DHCP server in this field. |
| IP Addressing Values | This field is only available when you select **Enable** in the **DHCP** field. |
| Beginning IP Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Ending IP Address | This field specifies the last of the contiguous addresses in the IP address pool. |
| Auto reserve IP for the same host | Select **Enable** to have the Device record DHCP IP addresses with the MAC addresses the IP addresses are assigned to. The Device assigns the same IP address to the same MAC address when the host requests an IP address again through DHCP. |
| DHCP Server Lease Time | This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are “recycled” and made available for future reassignment to other systems.<br>This field is only available when you select **Enable** in the **DHCP** field. |
| Days/Hours/ Minutes | Enter the lease time of the DHCP server. |
| DNS Values | This field is only available when you select **Enable** in the **DHCP** field. |
| DNS | Select the type of service that you are registered for from your Dynamic DNS service provider.<br>Select **Dynamic** if you have the Dynamic DNS service.<br>Select **Static** if you have the Static DNS service. |
| DNS Server 1<br>DNS Server 2 | Enter the first and second DNS (Domain Name System) server IP address the Device passes to the DHCP clients. |
| LAN IPv6 Mode Setup | |
| IPv6 State | Select **Enable** to activate the IPv6 mode and configure IPv6 settings on the Device. |
| LAN IPv6 Address Setup | |
| 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. |
| ULA Pseudo-Random Global ID | A unique local address (ULA) is a unique IPv6 address for use in private networks but not routable in the global IPv6 Internet.<br>Select this to have the Device automatically generate a globally unique address for the LAN IPv6 address. The address format is like fdxx:xxxx:xxxx:xxxx::/64. |
| ULA IPv6 Address Setup | |
| IPv6 Address | 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.<br>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. |

**Table 28** Network Setting > Home Networking > LAN Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 **Enable MLD Snooping** 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. |
| MLD Mode | Select **Standard Mode** to have the Device forward IPv6 multicast packets to a port that joins the IPv6 multicast group and broadcast unknown IPv6 multicast packets from the WAN to all LAN ports.<br>Select **Blocking Mode** to have the Device block all unknown IPv6 multicast packets from the WAN. |
| LAN IPv6 Address Assign Setup | Select how you want to obtain an IPv6 address:<br>• **Stateless**: The Device uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled.<br>• **Stateful**: The Device uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.<br>• **Stateless and Stateful**: The Device uses both IPv6 stateless and stateful autoconfiguration. The LAN IPv6 clients can obtain IPv6 addresses either through router advertisements or through DHCPv6.<br>• |
| LAN IPv6 DNS Assign Setup | Select how the Device provide DNS server and domain name information to the clients:<br>• **From Router Advertisement**: The Device provides DNS information through router advertisements.<br>• **From DHCPv6 Server**: The Device provides DNS information through DHCPv6.<br>• **From RA & DHCPv6 Server**: The Device provides DNS information through both router advertisements and DHCPv6. |
| DHCPv6 Configuration | |
| DHCPv6 State | This shows the status of the DHCPv6. |
| IPv6 Router Advertisement State | |
| RADVD State | This shows whether RADVD is enabled or not. |
| IPv6 DNS Values | |
| IPv6 DNS Server 1-3 | Select **From ISP** if your ISP dynamically assigns IPv6 DNS server information.<br>Select **User-Defined** if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Device passes to the DHCP clients.<br>Select **None** if you do not want to configure IPv6 DNS servers. |
| DNS Query Scenario | Select how the Device handles clients' DNS information requests.<br>• **IPv4/IPv6 DNS Server**: The Device forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives.<br>• **IPv6 DNS Server Only**: The Device forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives.<br>• **IPv4 DNS Server Only**: The Device forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives.<br>• **IPv6 DNS Server First**: The Device forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives.<br>• **IPv4 DNS Server First**: The Device forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

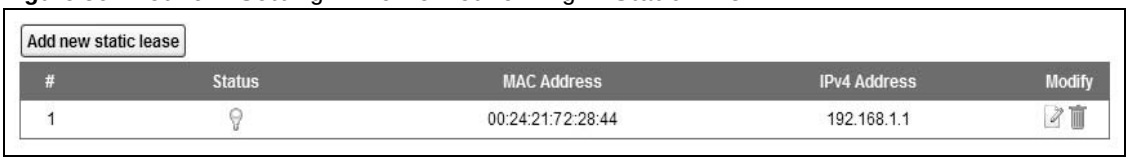
# 6.3 The Static DHCP Screen

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 56** Network Setting > Home Networking > Static DHCP



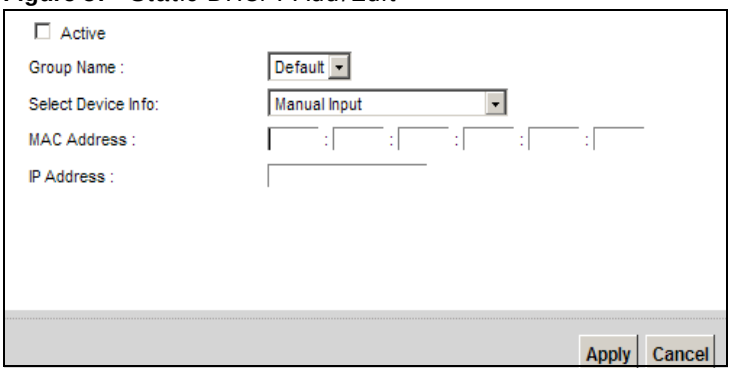

The following table describes the labels in this screen.

**Table 29** 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. |
| Status | This field displays whether the static DHCP is active or not. A yellow bulb signifies that this static DHCP is active. A gray bulb signifies that this static DHCP is not active. You can click the bulb to enable/disable it. |
| 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).<br>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. |
| IPv4 Address | This field displays the IPv4 IP address relative to the # field listed above. |
| Modify | Click the **Edit** icon to have the IP address field editable and change it.<br>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 57** Static DHCP: Add/Edit




The following table describes the labels in this screen.

**Table 30** Static DHCP: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this to activate the connection between the client and the Device. |
| Group Name | Select the interface group name for which you want to configure static DHCP settings. See Chapter 11 on page 175 for how to create a new interface group. |
| Select Device Info | Select a device or computer from the drop-down list or select **Manual Input** to manually enter a device's MAC address and IP address in the following fields. |
| MAC Address | If you select **Manual Input**, enter the MAC address of a computer on your LAN. |
| IP Address | If you select **Manual Input**, enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

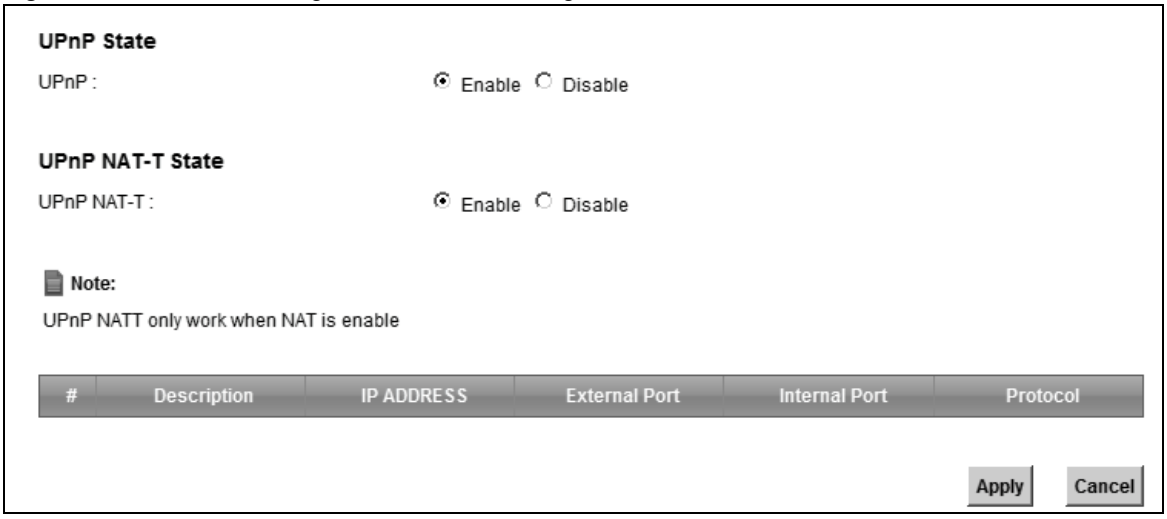
# 6.4 The UPnP Screen

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 104 for more information on UPnP.

Use the following screen to configure the UPnP settings on your Device. Click **Network Setting > Home Networking > UPnP** to display the screen shown next.

**Figure 58** Network Setting > Home Networking > UPnP




The following table describes the labels in this screen.

**Table 31** 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). |
| UPnP NAT-T | Select **Enable** to allow UPnP-enabled applications to automatically configure the Device so that they can communicate through the Device by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.<br>The table below displays the NAT port forwarding rules added automatically by UPnP NAT-T. |
| # | This is the index number of the UPnP NAT-T connection. |
| Description | This is the description of the UPnP NAT-T connection. |
| IP Address | This is the IP address of the other connected UPnP enabled device. |
| External Port | This is the external port number that identifies the service. |
| Internal Port | This is the internal port number that identifies the service. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 6.5 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

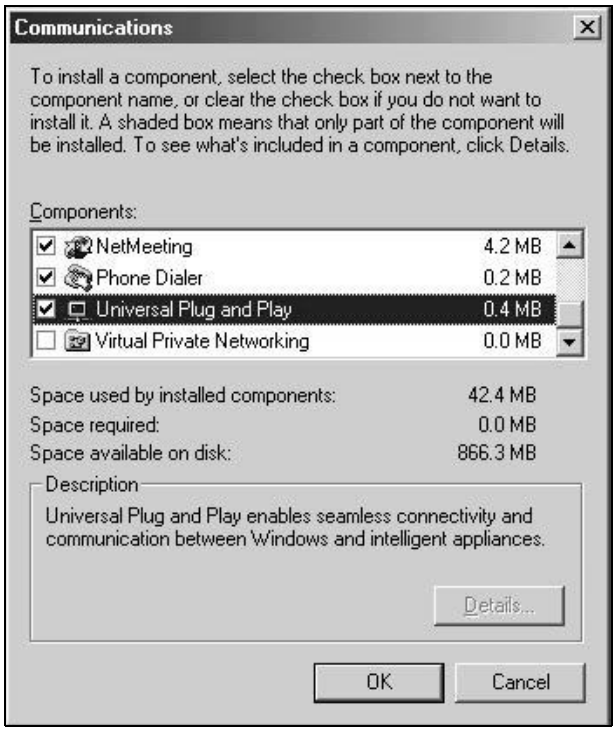
## Installing UPnP in Windows Me

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

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.




4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

## Installing UPnP in Windows XP

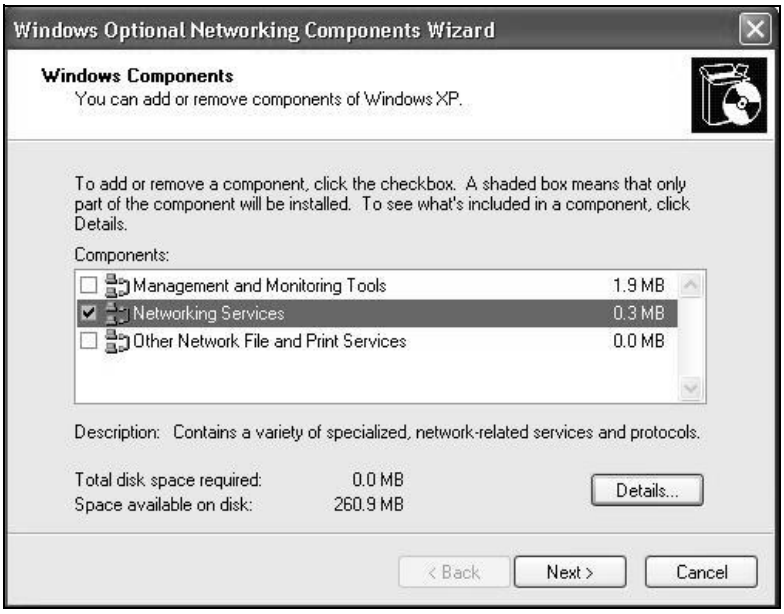
Follow the steps below to install the UPnP in Windows XP.

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

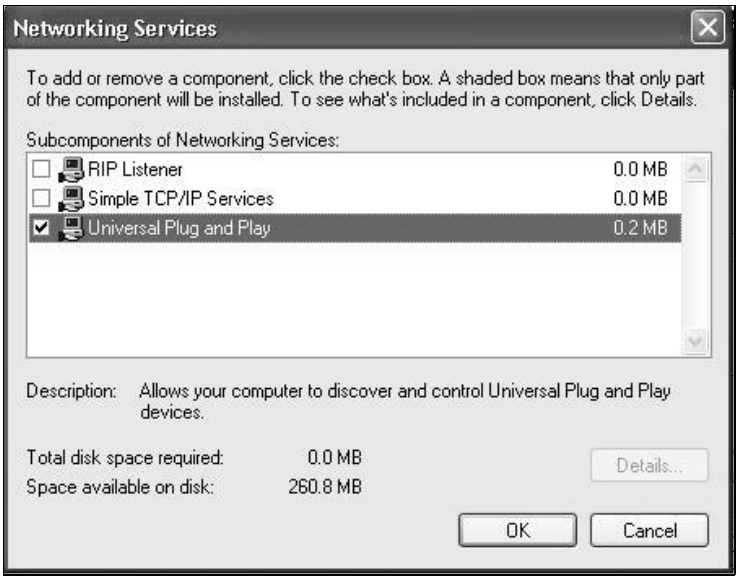
2 Double-click **Network Connections**.

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

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




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




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

# 6.6 Using UPnP in Windows XP Example

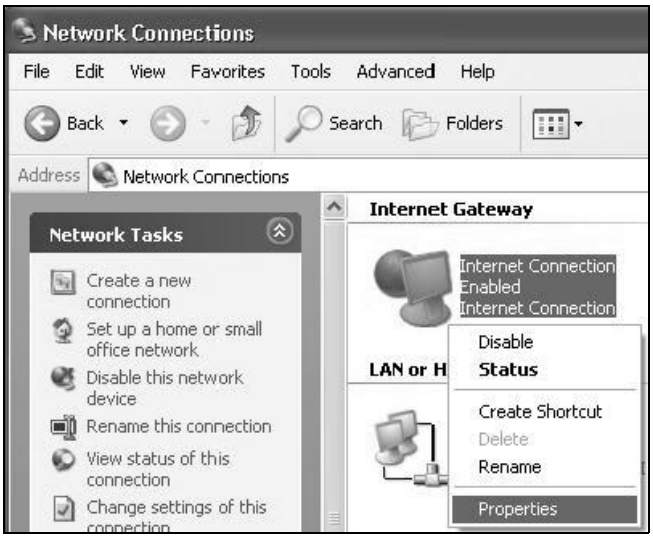
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the Device.

Make sure the computer is connected to a LAN port of the Device. Turn on your computer and the Device.

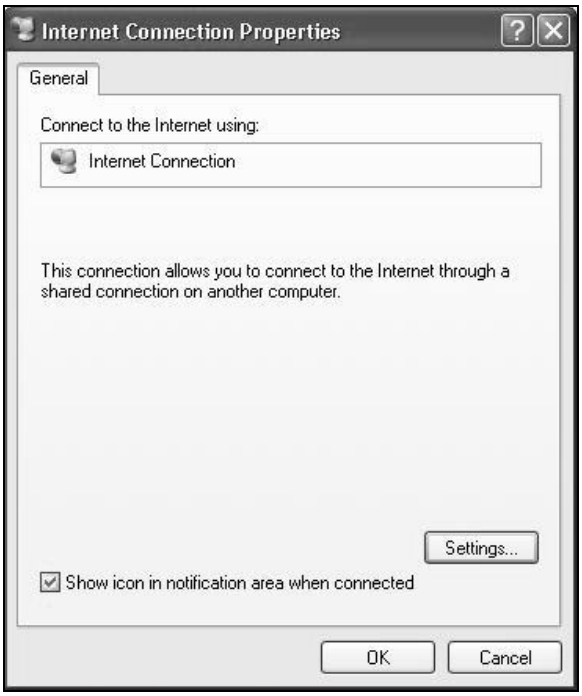
## Auto-discover Your UPnP-enabled Network Device

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

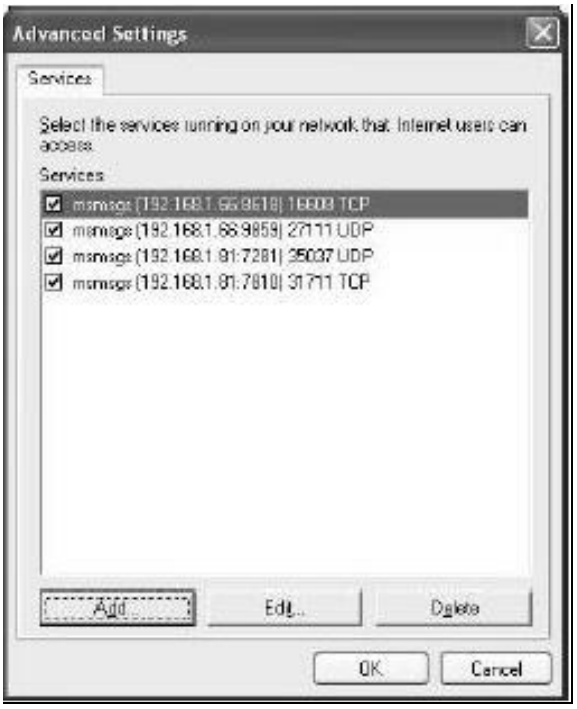
2 Right-click the icon and select **Properties**.

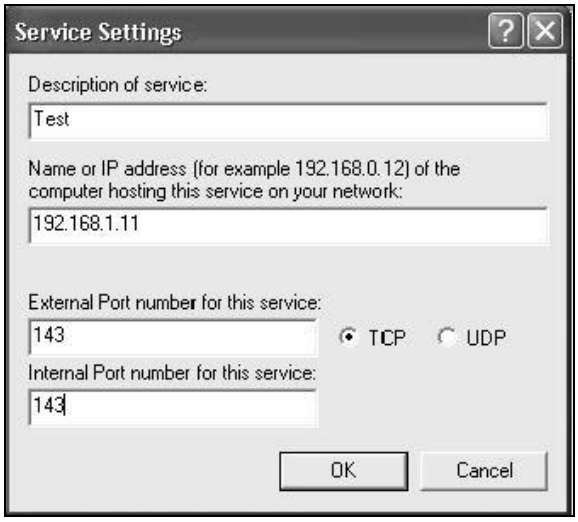



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.



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

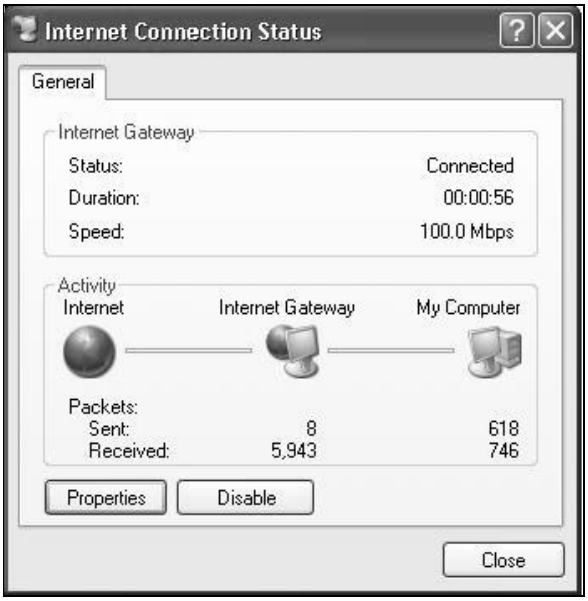



5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

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

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




### Web Configurator Easy Access

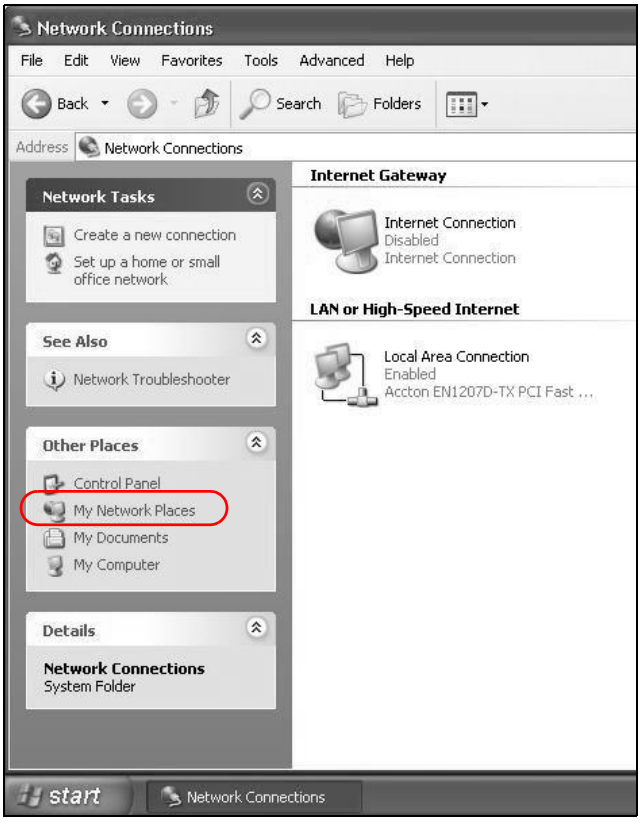
With UPnP, you can access the web-based configurator on the Device without finding out the IP address of the Device first. This comes helpful if you do not know the IP address of the Device.

Follow the steps below to access the web configurator.

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

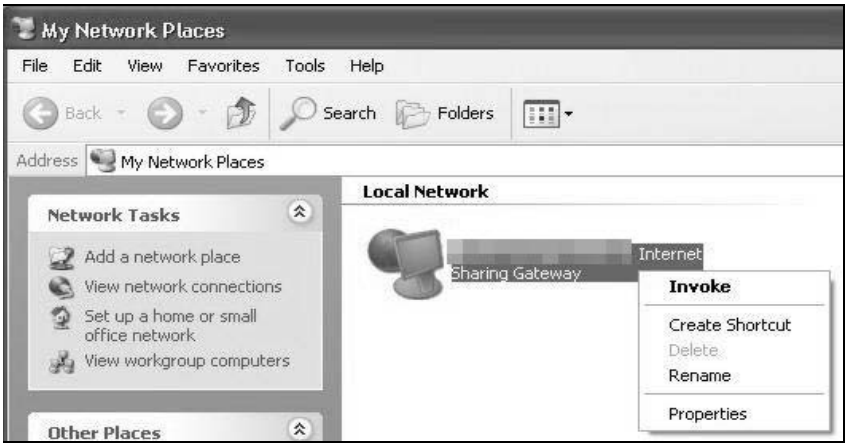
2 Double-click **Network Connections**.

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




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

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



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

# 6.7 The Additional Subnet Screen

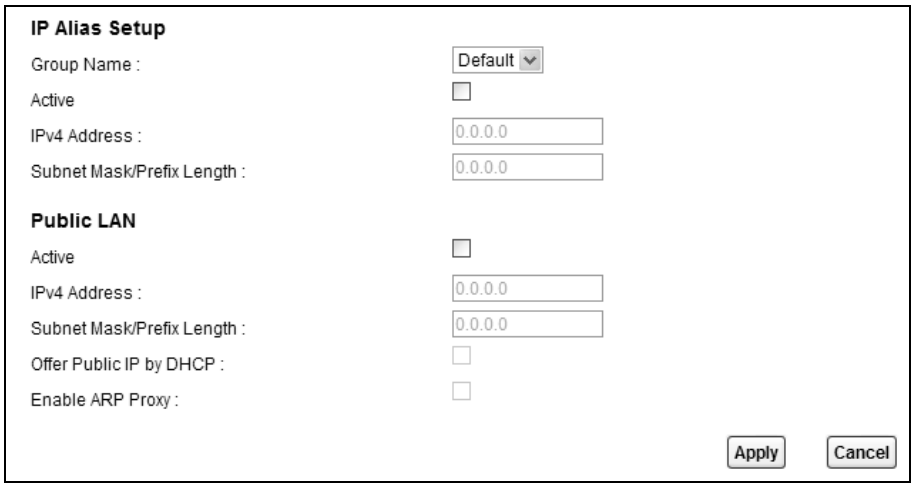
Use the **Additional Subnet** screen to configure IP alias and public static IP.

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).

If your ISP provides the Public LAN service, the Device may use an LAN IP address that can be accessed from the WAN.

Click **Network Setting > Home Networking > Additional Subnet** to display the screen shown next.

**Figure 59** Network Setting > Home Networking > Additional Subnet




The following table describes the labels in this screen.

**Table 32** Network Setting > Home Networking > Additional Subnet

| LABEL | DESCRIPTION |
|---|---|
| IP Alias Setup | |
| Group Name | Select the interface group name for which you want to configure the IP alias settings. See Chapter 11 on page 175 for how to create a new interface group. |
| Active | Select the checkbox to configure a LAN network for the Device. |
| IPv4 Address | Enter the IPv4 IP address of your Device in dotted decimal notation. |
| Subnet Mask/ Prefix Length | 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. |
| Public LAN | |
| Active | Select the checkbox to enable the Public LAN feature. Your ISP must support Public LAN and Static IP. |
| IPv4 Address | Enter the public IPv4 IP address provided by your ISP. |
| Subnet Mask/ Prefix Length | Enter the public IP subnet mask provided by your ISP. |

**Table 32** Network Setting > Home Networking > Additional Subnet (continued)

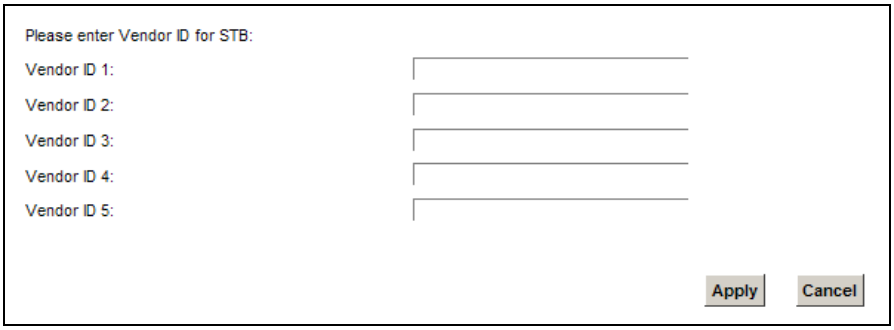
| LABEL | DESCRIPTION |
|---|---|
| Offer Public IP by DHCP | Select the checkbox to enable the Device to provide public IP addresses by DHCP server. |
| Enable ARP Proxy | Select the checkbox to enable the ARP (Address Resolution Protocol) proxy. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 6.8 The STB Vendor ID Screen

Set Top Box (STB) devices with dynamic IP addresses sometimes don't renew their IP addresses before the lease time expires. This could lead to IP address conflicts if the STB continues to use an IP address that gets assigned to another device. Use this screen to list the Vendor IDs of connected STBs to have the Device automatically create static DHCP entries for them when they request IP addresses.

Click **Network Setting** > **Home Networking** > **STB Vendor ID** to open this screen.

**Figure 60** Network Setting > Home Networking > STB Vendor ID




The following table describes the labels in this screen.

**Table 33** Network Setting > Home Networking > STB Vendor ID

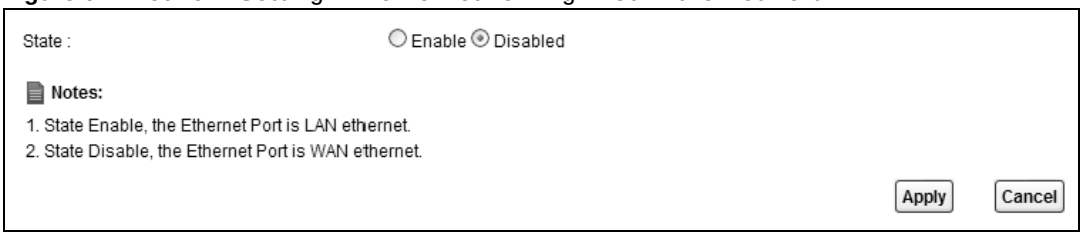
| LABEL | DESCRIPTION |
|---|---|
| Vendor ID 1 ~ 5 | Enter the STB's vendor ID. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 6.9 The 5th Ethernet Port Screen

If you use a DSL connection, you can configure your Ethernet WAN port as an extra LAN port. This Gigabit Ethernet port provides faster transmission speeds. Click **Network Setting** > **Home Networking** > **5th Ethernet Port** to open this screen.

Note: The Device needs to restart to make the role change take effect.

**Figure 61** Network Setting > Home Networking > 5th Ethernet Port




The following table describes the labels in this screen.

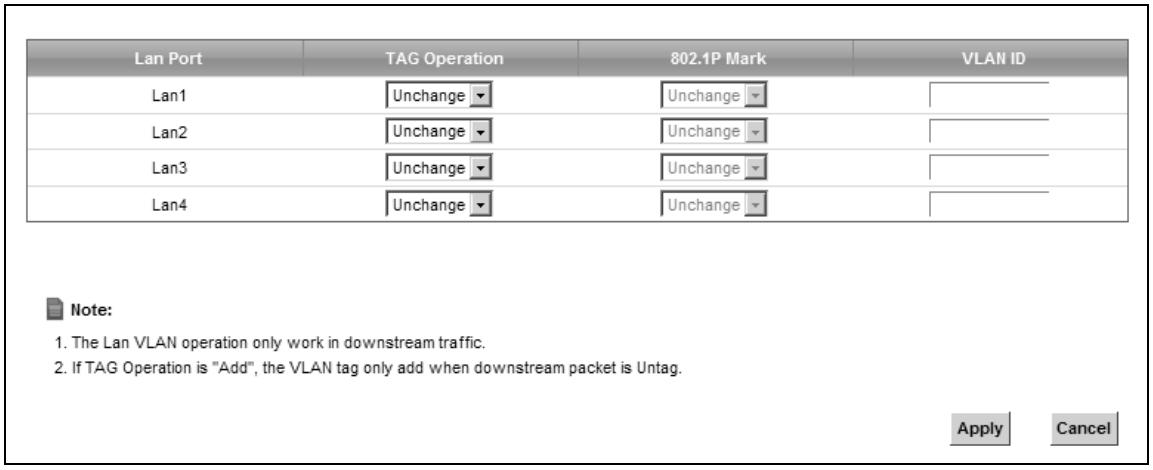
**Table 34** Network Setting > Home Networking > 5th Ethernet Port

| LABEL | DESCRIPTION |
|---|---|
| State | Select **Enable** to use the Ethernet WAN port as a LAN port on the Device. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 6.10 The LAN VLAN Screen

Click **Network Setting** > **Home Networking** > **LAN VLAN** to open this screen. Use this screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent out through individual LAN ports.

**Figure 62** Network Setting > Home Networking > LAN VLAN



The following table describes the labels in this screen.

**Table 35** Network Setting > Home Networking > LAN VLAN

| LABEL | DESCRIPTION |
|---|---|
| Lan Port | These represent the Device's LAN ports. |
| Tag Operation | Select what you want the Device to do to the IEEE 802.1q VLAN ID and priority tags of downstream traffic before sending it out through this LAN port.<br>• **Unchange** - Don't do anything to the traffic's VLAN ID and priority tags.<br>• **Add** - Add VLAN ID and priority tags to untagged traffic.<br>• **Remove** - Delete one tag from tagged traffic. If the frame has double tags, this removes the outer tag. This does not affect untagged traffic.<br>• **Remark** - Change the value of the outer VLAN ID and priority tags. |
| 802.1P Mark | Use this option to set what to do for the IEEE 802.1p priority tags when you add or remark the tags for a LAN port's downstream traffic. Either select **Unchange** to not modify the traffic's priority tags or select an priority from 0 to 7 to use. The larger the number, the higher the priority. |
| VLAN ID | If you will add or remark tags for this LAN port's downstream traffic, specify the VLAN ID (from 0 to 4094) to use here. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

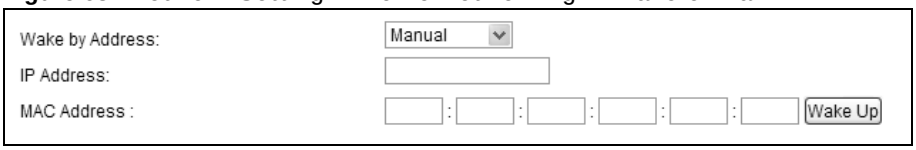
# 6.11 The Wake on LAN Screen

Use this screen to turn on a device on the LAN network. To use this feature, the remote device must also support Wake On LAN.

You need to know the MAC address of the LAN device. It may be on a label on the device or in its documentation.

Click **Network Setting** > **Home Networking** > **Wake on Lan** to open this screen.

**Figure 63** Network Setting > Home Networking > Wake on Lan




The following table describes the labels in this screen.

**Table 36** Network Setting > Home Networking > Wake on Lan

| LABEL | DESCRIPTION |
|---|---|
| Wake by Address | Select **Manual** and enter the IP address or MAC address of the device to turn it on remotely. The drop-down list also lists the IP addresses that can be found in the Device's ARP table. Select an IP address and it will then automatically update the IP address and MAC address in the following fields. |
| IP Address | Enter the IPv4 IP address of the device to turn it on. |
| MAC Address | Enter the MAC address of the device to turn it on. A MAC address consists of six hexadecimal character pairs. |
| Wake up | Click this to send a wake up packet to wake up the specified device. |

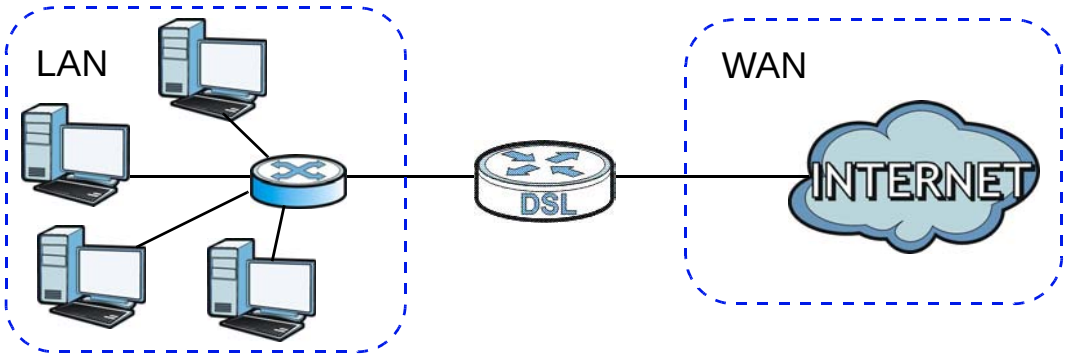
# 6.12 Technical Reference

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

## 6.12.1 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 64** LAN and WAN IP Addresses




## 6.12.2 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). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

## 6.12.3 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.

## 6.12.4 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, 192.168.1.1, 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”.

# 7

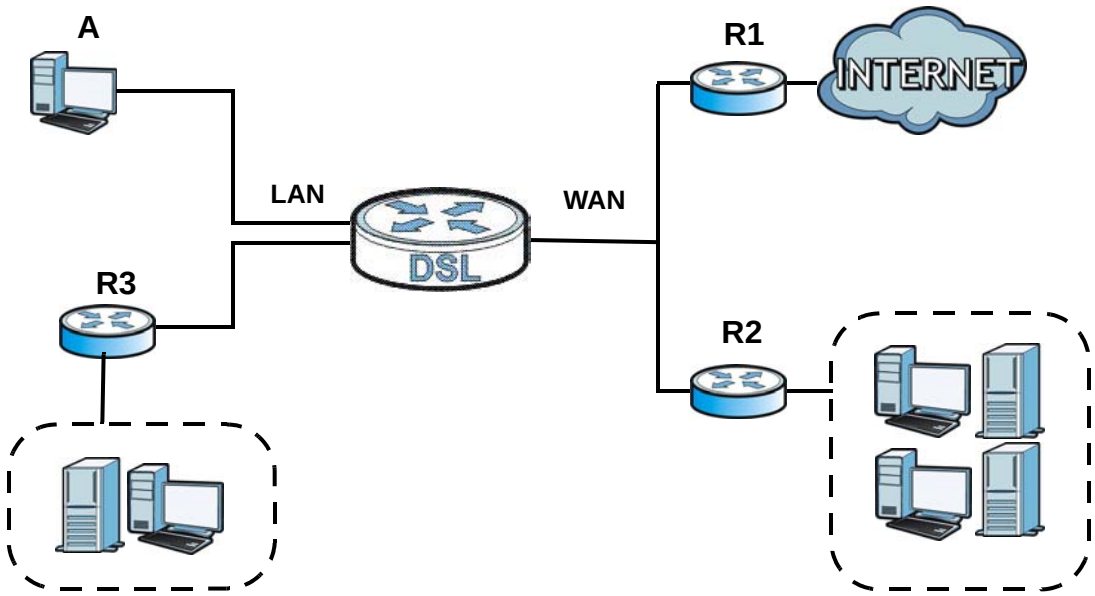
# Routing

## 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.

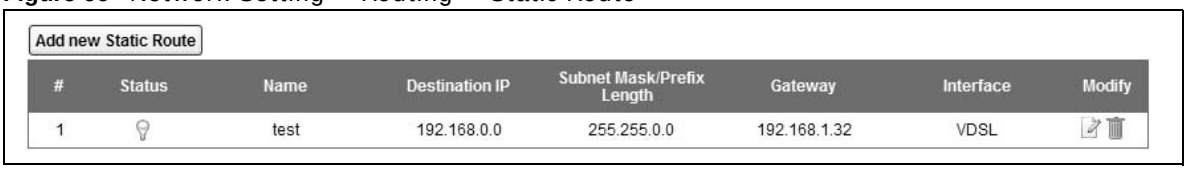
**Figure 65** Example of Routing Topology



# 7.2 The Routing Screen

Use this screen to view and configure the static route rules on the Device. Click **Network Setting > Routing > Static Route** to open the following screen.

**Figure 66** Network Setting > Routing > Static Route




The following table describes the labels in this screen.

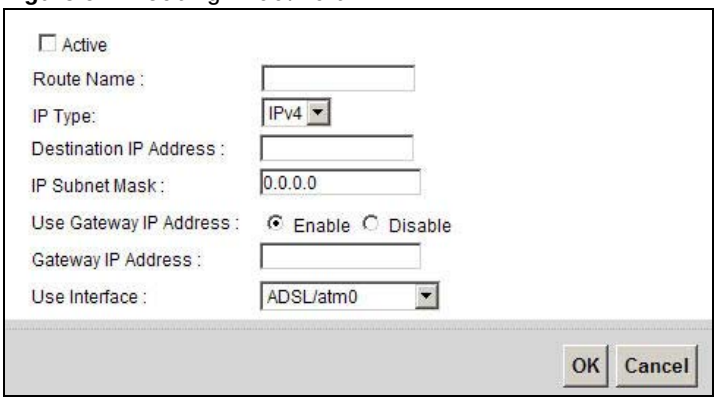
**Table 37** Network Setting > Routing > Static Route

| LABEL | DESCRIPTION |
|---|---|
| Add new static route | Click this to configure a new static route. |
| # | This is the index number of the entry. |
| Status | This field displays whether the static route is active or not. A yellow bulb signifies that this route is active. A gray bulb signifies that this route is not active. Click the bulb to enable/ disable the static route. |
| Name | This is the name that describes or identifies this route. |
| Destination IP | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |
| Subnet Mask/ Prefix Length | This parameter specifies the IP network subnet mask of the final destination. |
| 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. |
| Interface | This is the WAN interface used for this static route. |
| Modify | Click the **Edit** icon to edit the static route on the Device.<br>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 Add/Edit Static Route

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

**Figure 67** Routing: Add/Edit




The following table describes the labels in this screen.

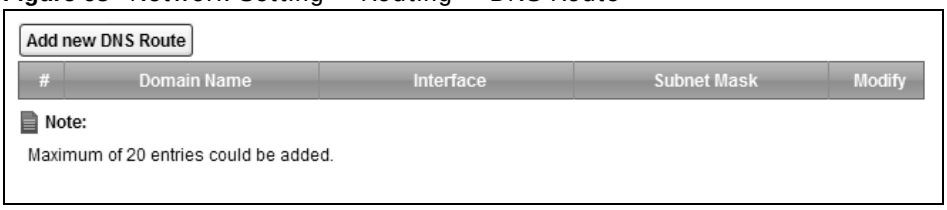
**Table 38** Routing: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | This field allows you to activate/deactivate this static route.<br>Select this to enable the static route. Clear this to disable this static route without having to delete the entry. |
| Route Name | Enter a descriptive name for the static route. |
| IP Type | Select whether your IP type is **IPv4** or **IPv6**. |
| Destination IP Address | Enter the IPv4 or IPv6 network address of the final destination. |
| IP Subnet Mask | If you are using IPv4 and 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. Enter the IP subnet mask here. |
| Use Gateway IP Address | 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.<br>If you want to use the gateway IP address, select **Enable**. |
| Gateway IP Address | Enter the IP address of the gateway. |
| Use Interface | Select the WAN interface you want to use for this static route. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 7.3 The DNS Route Screen

Use this screen to view and configure DNS routes on the Device. Click **Network Setting > Routing > DNS Route** to open the following screen.

**Figure 68** Network Setting > Routing > DNS Route




The following table describes the labels in this screen.

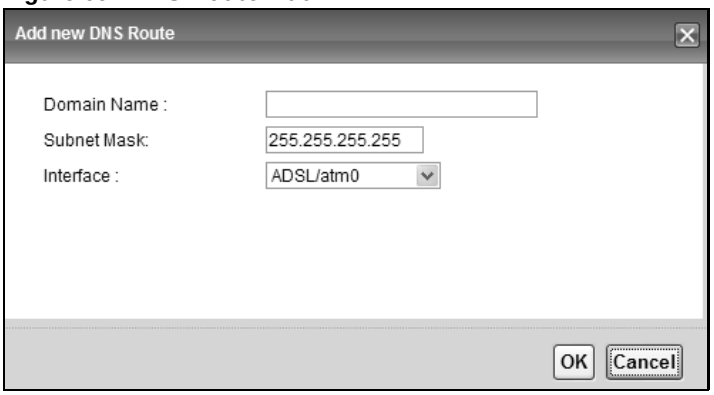
**Table 39** Network Setting > Routing > DNS Route

| LABEL | DESCRIPTION |
|---|---|
| Add new DNS Route | Click this to add a new DNS route. |
| # | This is the index number of a DNS route. |
| Domain Name | This is the host name or domain name of the DNS route entry. |
| Interface | This is the WAN connection through which the Device forwards DNS requests for this domain name. |
| Subnet Mask | This is the subnet mask of the DNS route entry. |
| Modify | Click the **Edit** icon to modify the DNS route.<br>Click the **Delete** icon to delete the DNS route. |

## 7.3.1 The DNS Route Add Screen

You can manually add the Device's DNS route entry. Click **Add new DNS Route** in the **Network Setting > Routing > DNS Route** screen. The screen shown next appears.

**Figure 69** DNS Route Add



The following table describes the labels in this screen.

**Table 40** DNS Route Add

| LABEL | DESCRIPTION |
|---|---|
| Domain Name | Enter the domain name of the DNS route entry. |
| Interface | Select the WAN connection through which the Device forwards DNS requests for this domain name. |
| Subnet Mask | Enter the subnet mask of the DNS route entry. |
| OK | Click this to save your changes. |
| Cancel | Click this to exit this screen without saving any changes. |

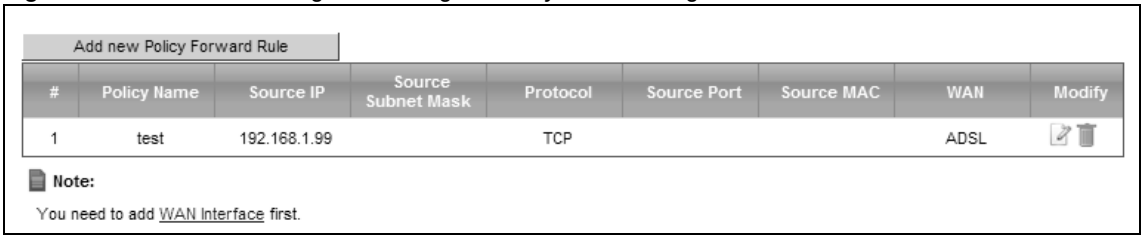
# 7.4 The Policy Forwarding Screen

Traditionally, routing is based on the destination address only and the Device takes the shortest path to forward a packet. Policy forwarding allows the Device to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

The **Policy Forwarding** screen let you view and configure routing policies on the Device. Click **Network Setting > Routing > Policy Forwarding** to open the following screen.

**Figure 70** Network Setting > Routing > Policy Forwarding




The following table describes the labels in this screen.

**Table 41** Network Setting > Routing >Policy Forwarding

| LABEL | DESCRIPTION |
|---|---|
| Add new Policy Forward Rule | Click this to create a new policy forwarding rule. |
| # | This is the index number of the entry. |
| Policy Name | This is the name of the rule. |
| Source IP | This is the source IP address. |
| Source Subnet Mask | his is the source subnet mask address. |
| Protocol | This is the transport layer protocol. |
| Source Port | This is the source port number. |

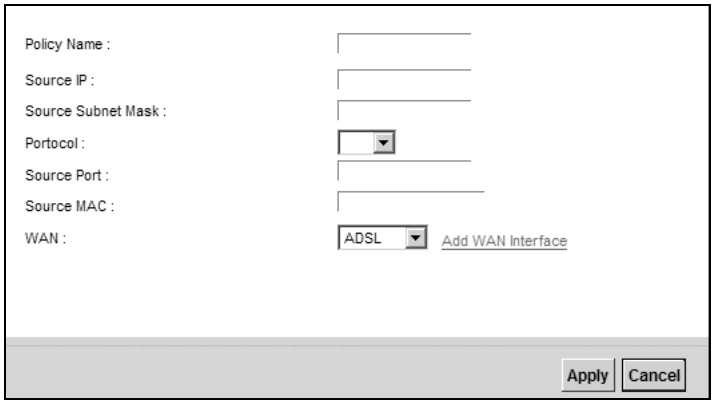
**Table 41** Network Setting > Routing >Policy Forwarding (continued)

| LABEL | DESCRIPTION |
|---|---|
| WAN | This is the WAN interface through which the traffic is routed. |
| Modify | Click the **Edit** icon to edit this policy.<br>Click the **Delete** icon to remove a policy from the Device. A window displays asking you to confirm that you want to delete the policy. |

## 7.4.1 Add/Edit Policy Forwarding

Click **Add new Policy Forward Rule** in the **Policy Forwarding** screen or click the **Edit** icon next to a policy. Use this screen to configure the required information for a policy route.

**Figure 71** Policy Forwarding: Add/Edit




The following table describes the labels in this screen.

**Table 42** Policy Forwarding: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Policy Name | Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces. |
| Source IP | Enter the source IP address. |
| Source Subnet Mask | Enter the source subnet mask address. |
| Protocol | Select the transport layer protocol (**TCP** or **UDP**). |
| Source Port | Enter the source port number. |
| Source MAC | Enter the source MAC address. |
| WAN | Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **Broadband** screens. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

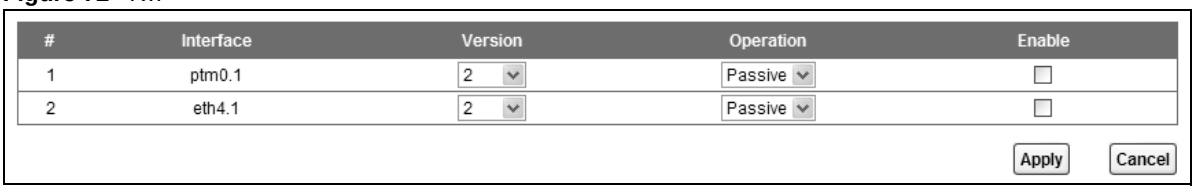
# 7.5 RIP

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

## 7.5.1 The RIP Screen

Click **Network Setting > Routing > RIP** to open the **RIP** screen.

**Figure 72** RIP




The following table describes the labels in this screen.

**Table 43** RIP

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index of the interface in which the RIP setting is used. |
| Interface | This is the name of the interface in which the RIP setting is used. |
| Version | The RIP version controls the format and the broadcasting method of the RIP packets that the Device sends (it recognizes both formats when receiving). RIP version **1** is universally supported but RIP version **2** carries more information. RIP version **1** is probably adequate for most networks, unless you have an unusual network topology. |
| Operation | Select **Passive** to have the Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface.<br>Select **Active** to have the Device advertise its route information and also listen for routing updates from neighboring routers. |
| Enabled | Select the check box to activate the settings. |
| Apply | Click **Apply** to save your changes back to the Device. |

# 8

# Quality of Service (QoS)

## 8.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is 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 application such as video-on-demand.

Configure QoS on the Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

1 Configure classifiers to sort traffic into different flows.

2 Assign priority and define actions to be performed for a classified traffic flow.

The Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority 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.

This chapter contains information about configuring QoS and editing classifiers.

### 8.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth (Section 8.3 on page 137).
- The **Queue Setup** screen lets you configure QoS queue assignment (Section 8.4 on page 138).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers (Section 8.5 on page 140).
- The **Policer Setup** screen lets you add, edit or delete QoS policers (Section 8.5 on page 140).

## 8.2 What You Need to Know

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

#### QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping

similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

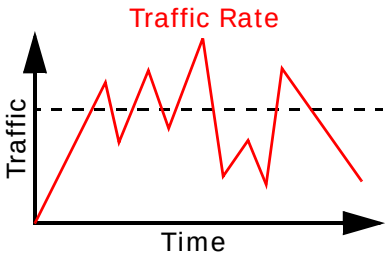
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

## Tagging and Marking

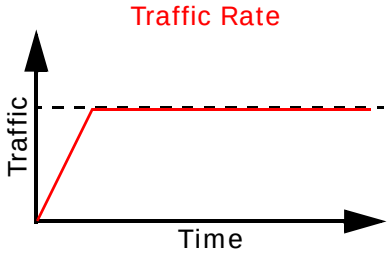
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or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

## Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your Device uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



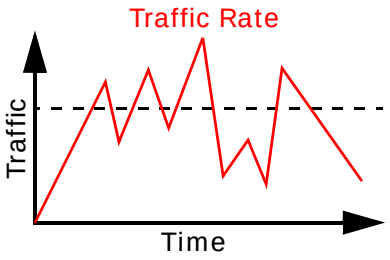

(Before Traffic Shaping)



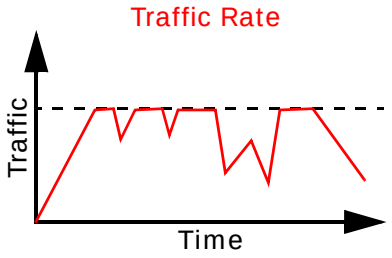

(After Traffic Shaping)

## Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.




(Before Traffic Policing)




(After Traffic Policing)

The Device supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions

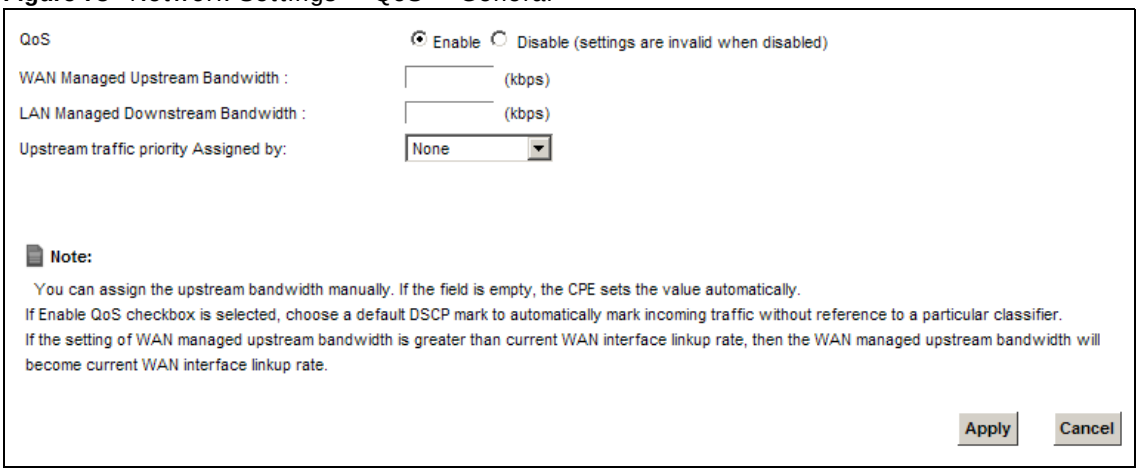
which are performed on the colored packets. See Section 8.8 on page 148 for more information on each metering algorithm.

# 8.3 The Quality of Service General Screen

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

Use this screen to enable or disable QoS and set the upstream bandwidth. See Section 8.1 on page 135 for more information.

**Figure 73** Network Settings > QoS > General




The following table describes the labels in this screen.

**Table 44** Network Setting > QoS > General

| LABEL | DESCRIPTION |
|---|---|
| QoS | Select the **Enable** check box to turn on QoS to improve your network performance. |
| WAN Managed Upstream Bandwidth | Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS.<br><br>The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps.<br><br>You can set this number higher than the interfaces' actual transmission speed. The Device uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed.<br><br>You can also set this number lower than the interfaces' actual transmission speed. This will cause the Device to not use some of the interfaces' available bandwidth.<br><br>If you leave this field blank, the Device automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed. |

**Table 44** Network Setting > QoS > General (continued) (continued)

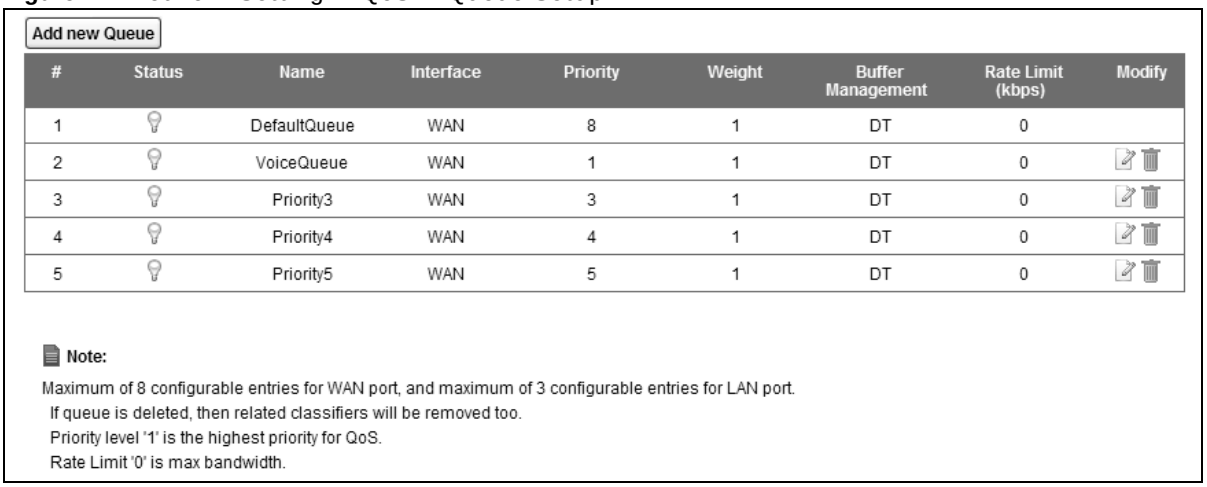
| LABEL | DESCRIPTION |
|---|---|
| LAN Managed Downstream Bandwidth | Enter the amount of downstream bandwidth for the LAN interfaces (including WLAN) that you want to allocate using QoS.<br>The recommendation is to set this speed to match the WAN interfaces' actual transmission speed. For example, set the LAN managed downstream bandwidth to 100000 kbps if you use a 100 Mbps wired Ethernet WAN connection.<br>You can also set this number lower than the WAN interfaces' actual transmission speed. This will cause the Device to not use some of the interfaces' available bandwidth.<br>If you leave this field blank, the Device automatically sets this to the LAN interfaces' maximum supported connection speed. |
| Upstream traffic priority Assigned by | Select how the Device assigns priorities to various upstream traffic flows.<br>• **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.<br>• **Ethernet Priority:** Automatically assign priority based on the IEEE 802.1p priority level.<br>• **IP Precedence:** Automatically assign priority based on the first three bits of the TOS field in the IP header.<br>• **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 **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 8.4 The Queue Setup Screen

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

Use this screen to configure QoS queue assignment.

**Figure 74** Network Setting > QoS > Queue Setup



The following table describes the labels in this screen.

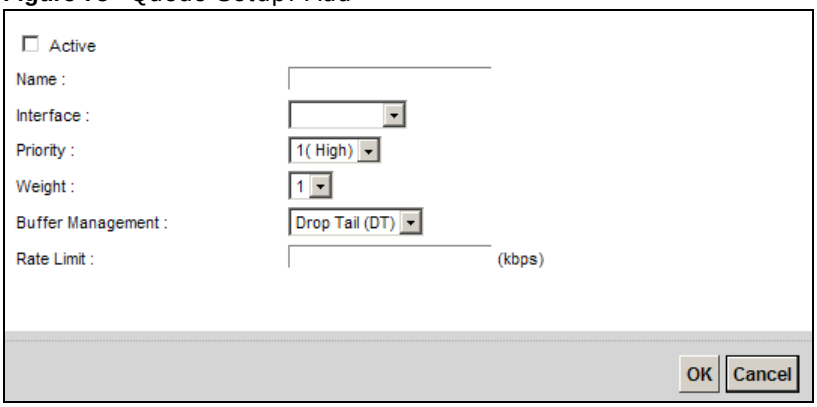
**Table 45** Network Setting > QoS > Queue Setup

| LABEL | DESCRIPTION |
|---|---|
| Add new Queue | Click this button to create a new queue entry. |
| # | 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. Click the bulb to enable/disable this queue. |
| 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. |
| Buffer Management | This shows the queue management algorithm used for this queue.<br>Queue management algorithms determine how the Device should handle packets when it receives too many (network congestion). |
| Rate Limit | This shows the maximum transmission rate allowed for traffic on this queue. |
| Modify | Click the **Edit** icon to edit the queue.<br>Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action. |

## 8.4.1 Adding a QoS Queue

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

**Figure 75** Queue Setup: Add




The following table describes the labels in this screen.

**Table 46** Queue Setup: Add

| 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.<br>This field is read-only if you are editing the queue. |

**Table 46** Queue Setup: Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Priority | Select the priority level (from 1 to 7) of this queue.<br>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.<br>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. |
| Buffer Management | This field displays **Drop Tail (DT)**. **Drop Tail (DT)** is a simple queue management algorithm that allows the Device buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it). |
| 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. |

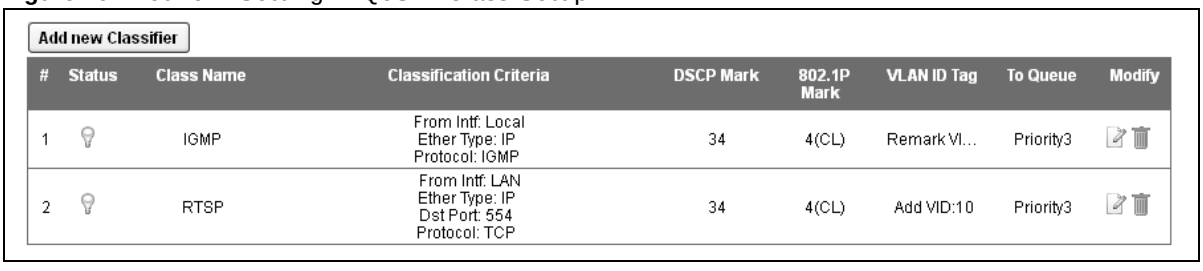
# 8.5 The Class Setup Screen

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 following screen.

**Figure 76** Network Setting > QoS > Class Setup




The following table describes the labels in this screen.

**Table 47** Network Setting > QoS > Class Setup

| LABEL | DESCRIPTION |
|---|---|
| Add new Classifier | Click this to create a new classifier. |
| # | This is the index number of the entry. |

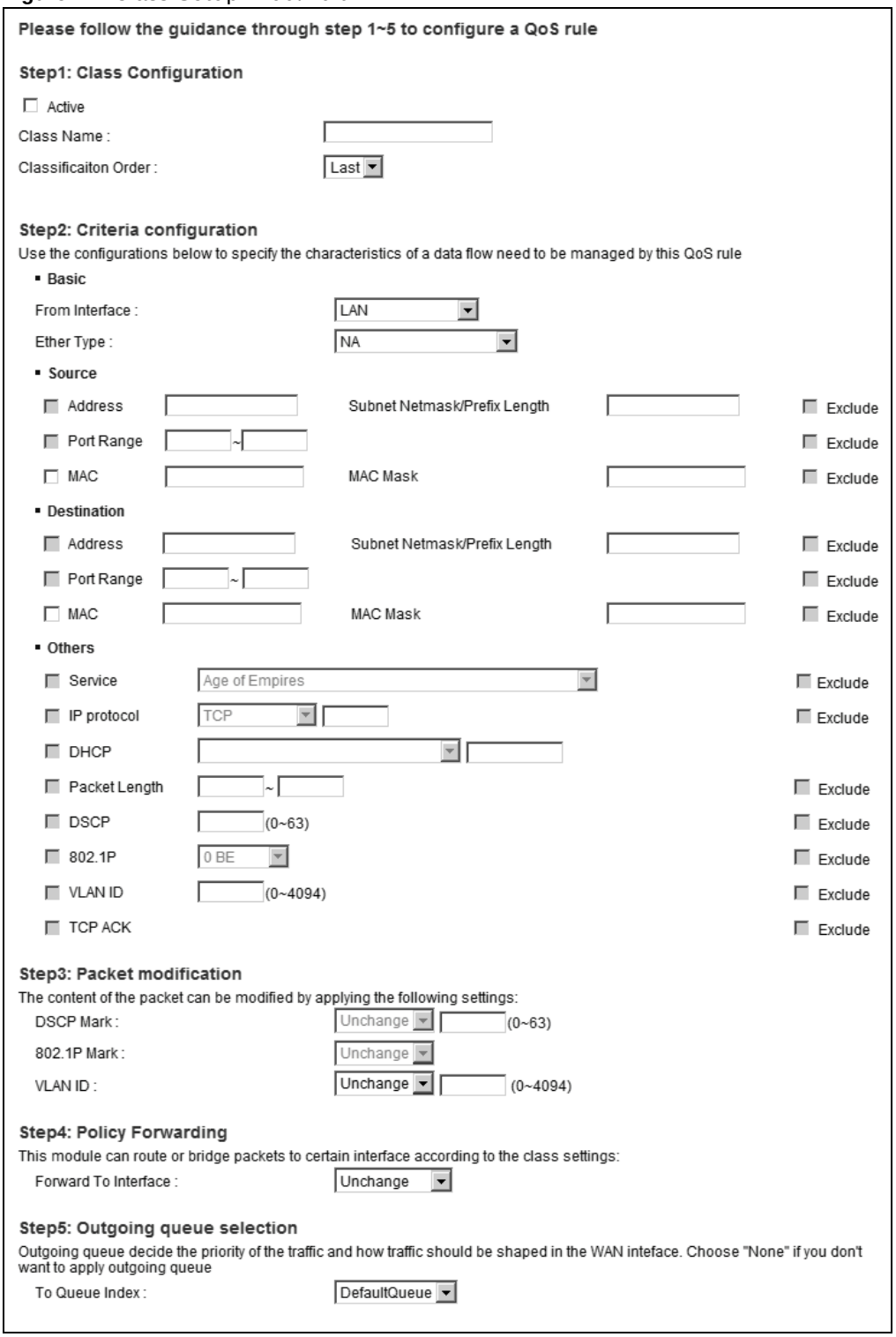
**Table 47** Network Setting > QoS > Class Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. Click the bulb to enable/disable the classifier. |
| Class Name | This is the name of the classifier. |
| Classification Criteria | This shows criteria specified in this classifier, for example the interface from which traffic of this class should come. |
| DSCP Mark | This is the DSCP number added to traffic of this classifier. |
| 802.1P Mark | This is the IEEE 802.1p priority level assigned to traffic of this classifier. |
| VLAN ID Tag | This is the VLAN ID number 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.<br>Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action. |

## 8.5.1 Add/Edit QoS Class

Click **Add new Classifier** in the **Class Setup** screen or the **Edit** icon next to a classifier to open the following screen.

**Figure 77** Class Setup: Add/Edit



The following table describes the labels in this screen.

**Table 48** Class Setup: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this to enable this classifier. |
| Class Name | Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces. |
| Classification Order | Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**.<br>Select **Last** to put this rule in the back of the classifier list. |
| From Interface | If you want to classify the traffic by an ingress interface, select an interface from the **From Interface** drop-down list box. |
| Ether Type | Select a predefined application to configure a class for the matched traffic.<br>If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type.<br>If you select **802.1Q**, you can configure an 802.1p priority level. |
| Source | |
| Address | Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address. |
| Subnet Netmask | Enter the source subnet mask. |
| Port Range | If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source. |
| MAC | Select the check box and enter the source MAC address of the packet. |
| MAC Mask | Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.<br>Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. |
| Exclude | Select this option to exclude the packets that match the specified criteria from this classifier. |
| Destination | |
| Address | Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address. |
| Subnet Netmask | Enter the source subnet mask. |
| Port Range | If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source. |
| MAC | Select the check box and enter the source MAC address of the packet. |
| MAC Mask | Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.<br>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 | |

**Table 48** Class Setup: Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Service | This field is available only when you select **IP** in the **Ether Type** field.<br>This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields. |
| IP Protocol | This field is available only when you select **IP** in the **Ether Type** field.<br>Select this option and select the protocol (service type) from **TCP**, **UDP**, **ICMP** or **IGMP**. If you select **User defined**, enter the protocol (service type) number. |
| DHCP | This field is available only when you select **IP** in the **Ether Type** field.<br>Select this option and select a DHCP option.<br>If you select **Vendor Class ID (DHCP Option 60)**, enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.<br>If you select **User Class ID (DHCP Option 77)**, enter a string that identifies the user's category or application type in the matched DHCP packets. |
| Packet Length | This field is available only when you select **IP** in the **Ether Type** field.<br>Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided. |
| DSCP | This field is available only when you select **IP** in the **Ether Type** field.<br>Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided. |
| 802.1P | This field is available only when you select **802.1Q** in the **Ether Type** field.<br>Select this option and select a priority level (between 0 and 7) from the drop-down list box.<br>"0" is the lowest priority level and "7" is the highest. |
| VLAN ID | This field is available only when you select **802.1Q** in the **Ether Type** field.<br>Select this option and specify a VLAN ID number. |
| TCP ACK | This field is available only when you select **IP** in the **Ether Type** field.<br>If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag. |
| Exclude | Select this option to exclude the packets that match the specified criteria from this classifier. |
| DSCP Mark | This field is available only when you select **IP** in the **Ether Type** field.<br>If you select **Mark**, enter a DSCP value with which the Device replaces the DSCP field in the packets.<br>If you select **Unchange**, the Device keep the DSCP field in the packets. |
| 802.1P Mark | Select a priority level with which the Device replaces the IEEE 802.1p priority field in the packets.<br>If you select **Unchange**, the Device keep the 802.1p priority field in the packets. |
| VLAN ID | If you select **Remark**, enter a VLAN ID number with which the Device replaces the VLAN ID of the frames.<br>If you select **Remove**, the Device deletes the VLAN ID of the frames before forwarding them out.<br>If you select **Add**, the Device treat all matched traffic untagged and add a second VLAN ID.<br>If you select **Unchange**, the Device keep the VLAN ID in the packets. |
| Forward to Interface | Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the Device forward traffic of this class according to the default routing table. |

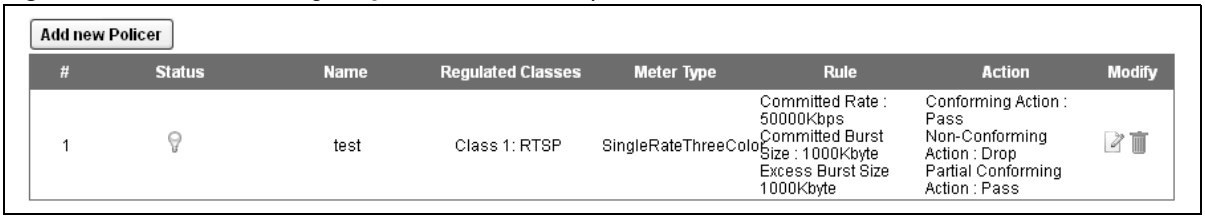
**Table 48** Class Setup: Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| To Queue Index | Select a queue that applies to this class.<br>You should have configured a queue in the **Queue Setup** screen already. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 8.6 The QoS Policer Setup Screen

Use this screen to configure QoS policers that allow you to limit the transmission rate of incoming traffic. Click **Network Setting > QoS > Policer Setup**. The screen appears as shown.

**Figure 78** Network Setting > QoS > Policer Setup




The following table describes the labels in this screen.

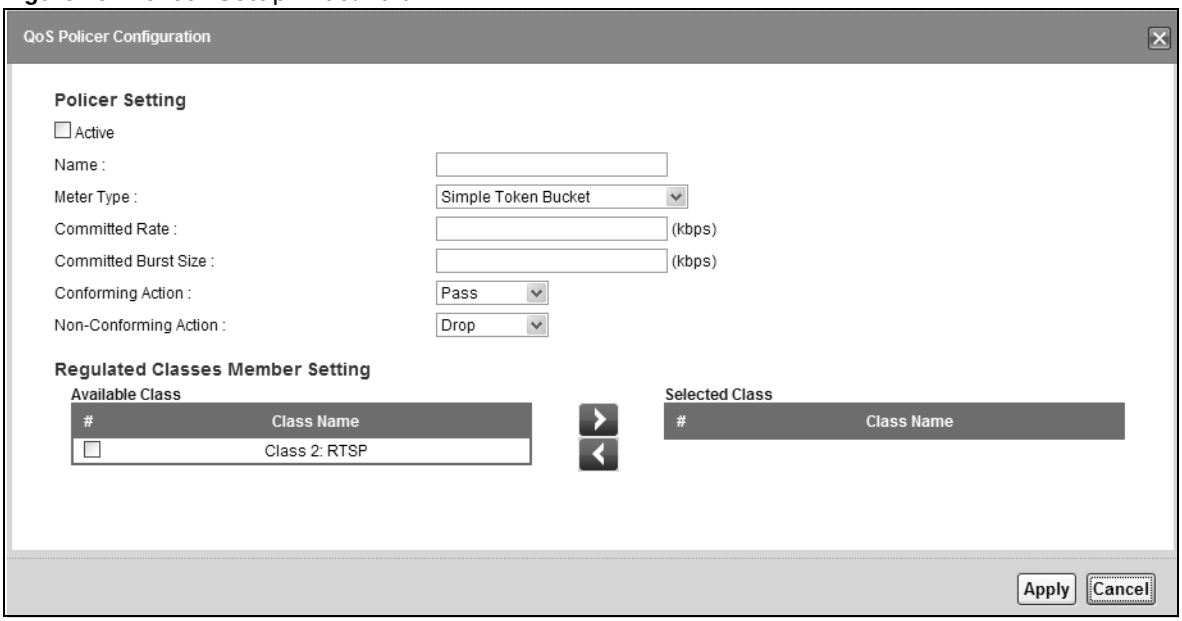
**Table 49** Network Setting > QoS > Policer Setup

| LABEL | DESCRIPTION |
|---|---|
| Add new Policer | Click this to create a new entry. |
| # | This is the index number of the entry. |
| Status | This field displays whether the policer is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this policer is not active. Click the bulb to enable/ disable the policer. |
| Name | This field displays the descriptive name of this policer. |
| Regulated Classes | This field displays the name of a QoS classifier this policer uses. |
| Meter Type | This field displays the type of QoS metering algorithm used in this policer. |
| Rule | These are the rates and burst sizes against which the policer checks the traffic of the member QoS classes. |
| Action | This shows the how the policer has the Device treat different types of traffic belonging to the policer's member QoS classes. |
| Modify | Click the **Edit** icon to edit the policer.<br>Click the **Delete** icon to delete an existing policer. Note that subsequent rules move up by one when you take this action. |

## 8.6.1 Add/Edit a QoS Policer

Click **Add new Policer** in the **Policer Setup** screen or the **Edit** icon next to a policer to show the following screen.

**Figure 79** Policer Setup: Add/Edit




The following table describes the labels in this screen.

**Table 50** Policer Setup: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | Select the check box to activate this policer. |
| Name | Enter the descriptive name of this policer. |
| Meter Type | This shows the traffic metering algorithm used in this policer.<br>The **Simple Token Bucket** algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size.<br>The **Single Rate Three Color Marker** (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS).<br>The **Two Rate Three Color Marker** (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR). |
| Committed Rate | Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic. |
| Committed Burst Size | Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured.<br>This is the maximum size of the (first) token bucket in a traffic metering algorithm. |

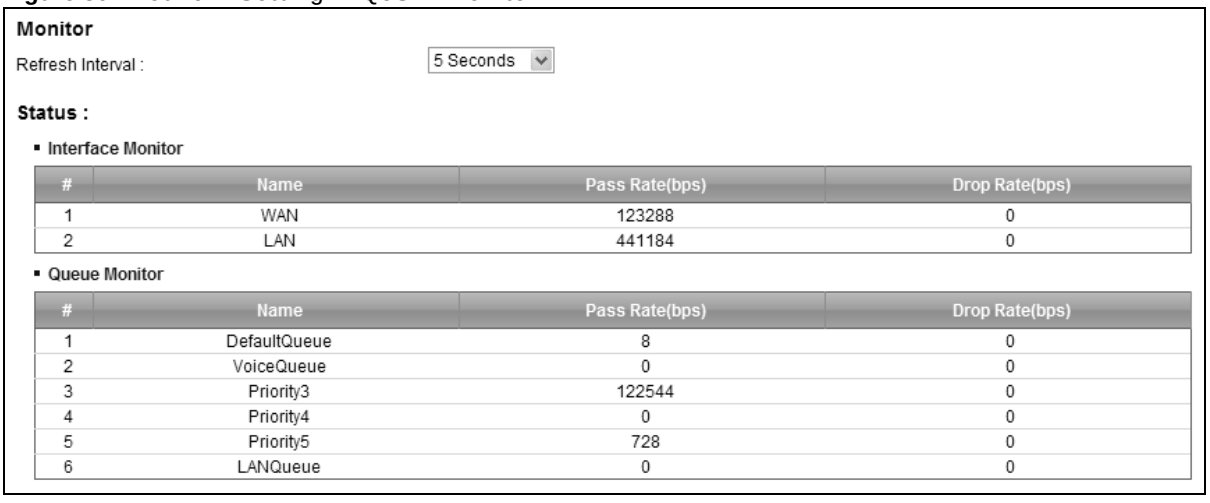
**Table 50** Policer Setup: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Conforming Action | Specify what the Device does for packets within the committed rate and burst size (green-marked packets).<br>• **Pass:** Send the packets without modification.<br>• **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use. |
| Non-Conforming Action | Specify what the Device does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets).<br>• **Drop:** Discard the packets.<br>• **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network. |
| Available Class<br>Selected Class | Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier.<br>Highlight a QoS classifier in the **Available Class** box and use the **>** button to move it to the **Selected Class** box.<br>To remove a QoS classifier from the **Selected Class** box, select it and use the **<** button. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 8.7 The QoS Monitor Screen

This screen is available only when you set a rate limit for a WAN queue in the **Queue Setup** screen and the WAN interface is connected. Use this screen to monitor the traffic statistics for both the WAN and LAN interfaces. To view the Device's QoS packet statistics, click **Network Setting > QoS > Monitor**. The screen appears as shown.

**Figure 80** Network Setting > QoS > Monitor



The following table describes the labels in this screen.

**Table 51** Network Setting > QoS > Monitor

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Enter how often you want the Device to update this screen. Select **No Refresh** to stop refreshing statistics. |
| Interface Monitor | |
| # | This is the index number of the entry. |
| Name | This shows the name of the interface on the Device. |
| Pass Rate | This shows how many packets forwarded to this interface has been transmitted successfully. |
| Drop Rate | This shows how many packets forwarded to this interface has been dropped. |
| Queue Monitor | |
| # | This is the index number of the entry. |
| Name | This shows the name of the queue. |
| Pass Rate | This shows how many packets assigned to this queue has been transmitted successfully. |
| Drop Rate | This shows how many packets assigned to this queue has been dropped. |

# 8.8 Technical Reference

The following section contains additional technical information about the Device features described in this chapter.

## IEEE 802.1Q Tag

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

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

**Table 52** 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”. |

**Table 52** IEEE 802.1p Priority Level and Traffic Type

| PRIORITY LEVEL | TRAFFIC TYPE |
|---|---|
| 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. |

## DiffServ

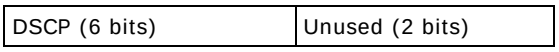
QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

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

## DSCP and Per-Hop Behavior

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

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




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

## 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.

## 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 53** 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<br>001100<br>001010<br>001000 | 250~1100 |
| 4 | 4 | 2 | 010110<br>010100<br>010010<br>010000 | |
| 5 | 5 | 3 | 011110<br>011100<br>011010<br>011000 | <250 |
| 6 | 6 | 4 | 100110<br>100100<br>100010<br>100000 | |
| | | 5 | 101110<br>101000 | |
| 7 | 7 | 6 | 110000 | |
| | | 7 | 111000 | |

## Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size, so the bucket can hold up to *b* tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.

- If there are no tokens in the bucket, the Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the Device treats the packet in either one of the following ways:

  In traffic shaping:

  - Holds it in the queue until enough tokens are available in the bucket.

  In traffic policing:

  - Drops it.
  - Transmits it but adds a DSCP mark. The Device may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

## Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the Device checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

## Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based

on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the Device checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

# 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 this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network (Section 9.2 on page 154).
- Use the **Applications** screen to forward incoming service requests to the server(s) on your local network (Section 9.3 on page 157).
- Use the **Port Triggering** screen to add and configure the Device's trigger port settings (Section 9.4 on page 159).
- Use the **DMZ** screen to configure a default server (Section 9.5 on page 161).
- Use the **ALG** screen to enable and disable the NAT and SIP (VoIP) ALG in the Device (Section 9.6 on page 162).
- Use the **Address Mapping** screen to configure the Device's address mapping settings (Section 9.7 on page 163).
- Use the **Sessions** screen to configure the Device's maximum number of NAT sessions (Section 9.8 on page 165).

### 9.1.2 What You Need To Know

#### 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 9.9 on page 165 for advanced technical information on NAT.

## 9.2 The Port Forwarding Screen

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

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

The most often used port numbers and services are shown in Appendix F on page 347. Please refer to RFC 1700 for further information about port numbers.

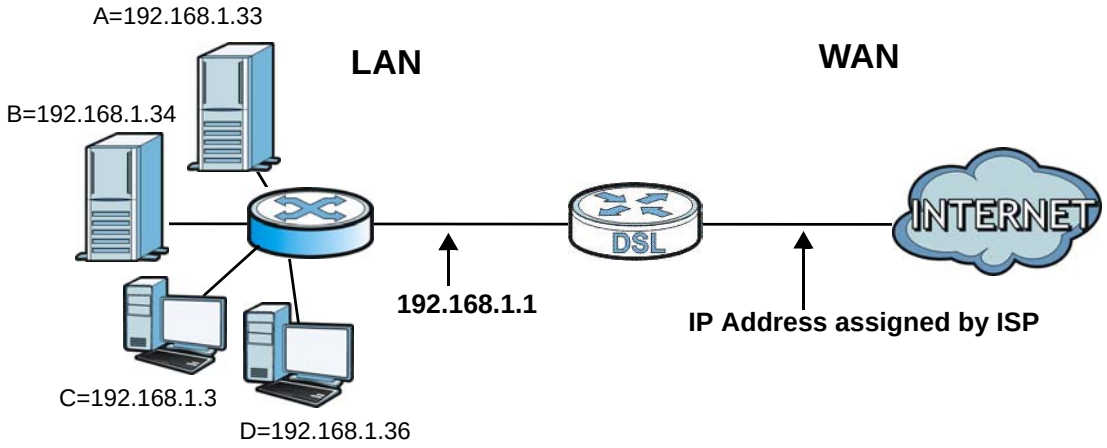
Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your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

### Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a

third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

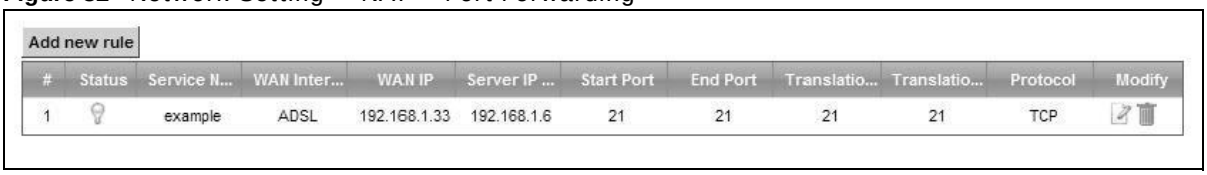
**Figure 81** Multiple Servers Behind NAT Example




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

See Appendix F on page 347 for port numbers commonly used for particular services.

**Figure 82** Network Setting > NAT > Port Forwarding




The following table describes the fields in this screen.

**Table 54** Network Setting > NAT > Port Forwarding

| LABEL | DESCRIPTION |
|---|---|
| Add new rule | Click this to add a new rule. |
| # | This is the index number of the entry. |
| Status | This field displays whether the NAT rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active. |
| Service Name | This shows the service's name. |
| WAN Interface | This shows the WAN interface through which the service is forwarded. |
| WAN IP | This field displays the incoming packet's destination IP address. |
| Server IP Address | This is the server's IP address. |
| Start Port | This is the first external port number that identifies a service. |
| End Port | This is the last external port number that identifies a service. |
| Translation Start Port | This is the first internal port number that identifies a service. |
| Translation End Port | This is the last internal port number that identifies a service. |

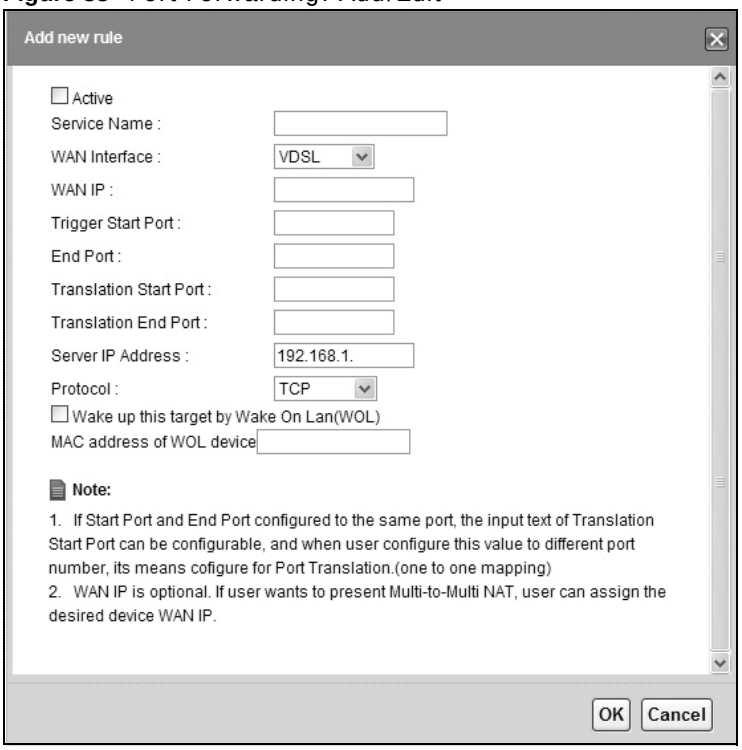
**Table 54** Network Setting > NAT > Port Forwarding (continued)

| LABEL | DESCRIPTION |
|---|---|
| Protocol | This shows the IP protocol supported by this virtual server, whether it is **TCP**, **UDP**, or **TCP / UDP**. |
| Modify | Click the **Edit** icon to edit this rule.<br>Click the **Delete** icon to delete an existing rule. |

## 9.2.1 Add/Edit Port Forwarding

Click **Add new rule** in the **Port Forwarding** screen or click the **Edit** icon next to an existing rule to open the following screen.

**Figure 83** Port Forwarding: Add/Edit




The following table describes the labels in this screen.

**Table 55** Port Forwarding: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | Clear the checkbox to disable the rule. Select the check box to enable it. |
| Service Name | Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on). |
| WAN Interface | Select the WAN interface through which the service is forwarded.<br>You must have already configured a WAN connection with NAT enabled. |
| WAN IP | Enter the WAN IP address for which the incoming service is destined. If the packet's destination IP address doesn't match the one specified here, the port forwarding rule will not be applied. |

**Table 55** Port Forwarding: Add/Edit (continued)

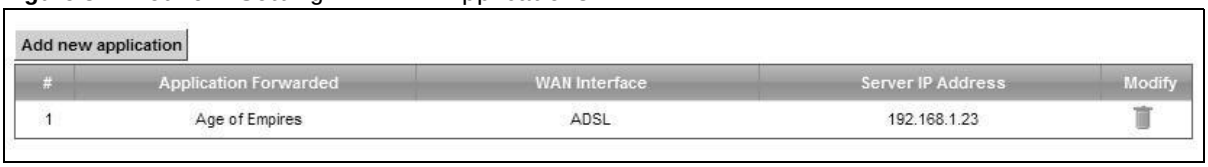
| LABEL | DESCRIPTION |
|---|---|
| Start Port | Enter the original destination port for the packets.<br>To forward only one port, enter the port number again in the **End Port** field.<br>To forward a series of ports, enter the start port number here and the end port number in the **End Port** field. |
| End Port | Enter the last port of the original destination port range.<br>To forward only one port, enter the port number in the **Start Port** field above and then enter it again in this field.<br>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. |
| Translation Start Port | This shows the port number to which you want the Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated. |
| Translation End Port | This shows the last port of the translated port range. |
| Server IP Address | Enter the inside IP address of the virtual server here. |
| Protocol | Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP / UDP**. |
| Wake up this target by Wake On Lan(WOL) | Select this and enter the MAC address of a LAN device if you want to turn the device on remotely from the Internet or the WAN network using this port forwarding rule. |
| MAC address of WOL device | Enter the MAC address of the LAN device. A MAC address consists of six hexadecimal character pairs. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 9.3 The Applications Screen

This screen provides a summary of all NAT applications and their configuration. In addition, this screen allows you to create new applications and/or remove existing ones.

To access this screen, click **Network Setting > NAT > Applications**. The following screen appears.

**Figure 84** Network Setting > NAT > Applications



The following table describes the labels in this screen.

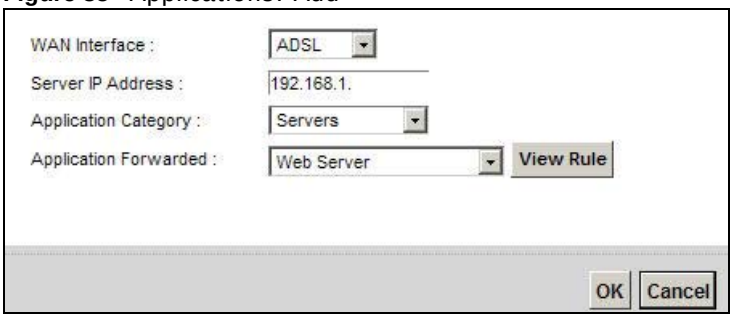
**Table 56** Network Setting > NAT > Applications

| LABEL | DESCRIPTION |
|---|---|
| Add new application | Click this to add a new NAT application rule. |
| Application Forwarded | This field shows the type of application that the service forwards. |
| WAN Interface | This field shows the WAN interface through which the service is forwarded. |
| Server IP Address | This field displays the destination IP address for the service. |
| Modify | Click the **Delete** icon to delete the rule. |

## 9.3.1 Add New Application

This screen lets you create new NAT application rules. Click **Add new application** in the **Applications** screen to open the following screen.

**Figure 85** Applications: Add




The following table describes the labels in this screen.

**Table 57** Applications: Add

| LABEL | DESCRIPTION |
|---|---|
| WAN Interface | Select the WAN interface that you want to apply this NAT rule to. |
| Server IP Address | Enter the inside IP address of the application here. |
| Application Category | Select the category of the application from the drop-down list box. |
| Application Forwarded | Select a service from the drop-down list box and the Device automatically configures the protocol, start, end, and map port number that define the service. |
| View Rule | Click this to display the configuration of the service that you have chosen in **Application Fowarded**. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

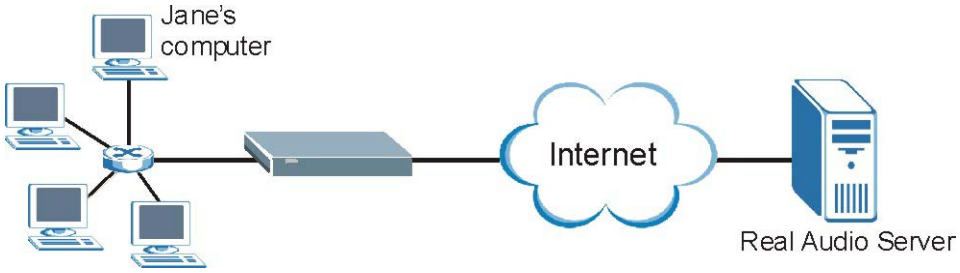
# 9.4 The Port Triggering Screen

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

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

For example:

**Figure 86** Trigger Port Forwarding Process: Example




1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a "trigger" port and causes the Device to record Jane's computer IP address. The Device associates Jane's computer IP address with the "open" port range of 6970-7170.

3 The Real Audio server responds using a port number ranging between 6970-7170.

4 The Device forwards the traffic to Jane's computer IP address.

5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Device times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Setting > NAT > Port Triggering** to open the following screen. Use this screen to view your Device's trigger port settings.

**Figure 87** Network Setting > NAT > Port Triggering

Add new rule

| # | Status | Service Name | WAN Interface | Trigger Start Port | Trigger End Port | Trigger Proto. | Open Start Port | Open End Port | Open Proto. | Modify |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | test | ADSL | 5191 | 5191 | TCP or UDP | 5191 | 5191 | TCP | |

The following table describes the labels in this screen.

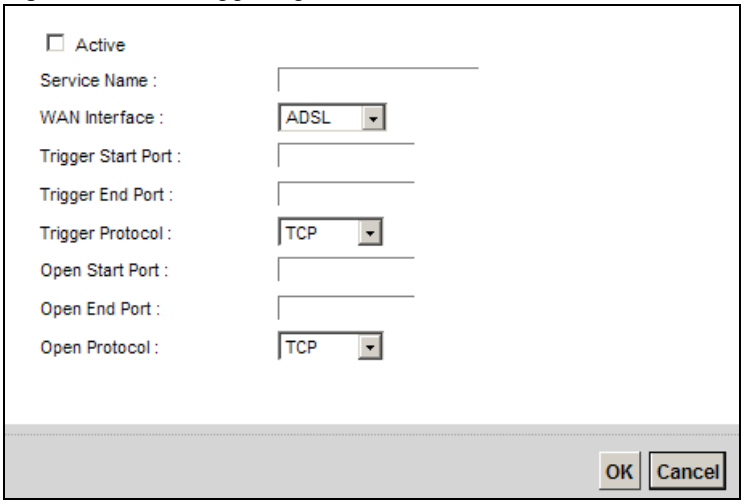
**Table 58** Network Setting > NAT > Port Triggering

| LABEL | DESCRIPTION |
|---|---|
| Add new rule | Click this to create a new rule. |
| # | This is the index number of the entry. |
| Status | This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active. |
| Service Name | This field displays the name of the service used by this rule. |
| WAN Interface | This field shows the WAN interface through which the service is forwarded. |
| Trigger Start Port | The trigger port is a port (or a range of ports) that causes (or triggers) the Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.<br>This is the first port number that identifies a service. |
| Trigger End Port | This is the last port number that identifies a service. |
| Trigger Proto. | This is the trigger transport layer protocol. |
| Open Start Port | The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.<br>This is the first port number that identifies a service. |
| Open End Port | This is the last port number that identifies a service. |
| Open Proto. | This is the open transport layer protocol. |
| Modify | Click the **Edit** icon to edit this rule.<br>Click the **Delete** icon to delete an existing rule. |

## 9.4.1 Add/Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add new rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen.

**Figure 88** Port Triggering: Add/Edit



The following table describes the labels in this screen.

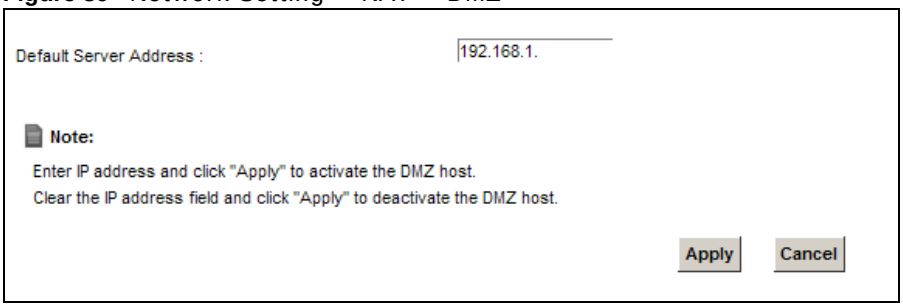
**Table 59** Port Triggering: Configuration Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | Select the check box to enable this rule. |
| Service Name | Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on). |
| WAN Interface | Select a WAN interface for which you want to configure port triggering rules. |
| Trigger Start Port | The trigger port is a port (or a range of ports) that causes (or triggers) the Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.<br>Type a port number or the starting port number in a range of port numbers. |
| Trigger End Port | Type a port number or the ending port number in a range of port numbers. |
| Trigger Protocol | Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**. |
| Open Start Port | The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.<br>Type a port number or the starting port number in a range of port numbers. |
| Open End Port | Type a port number or the ending port number in a range of port numbers. |
| Open Protocol | Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 9.5 The DMZ Screen

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 the **NAT Port Forwarding Setup** screen.

**Figure 89** Network Setting > NAT > DMZ



The following table describes the fields in this screen.

**Table 60** Network Setting > NAT > DMZ

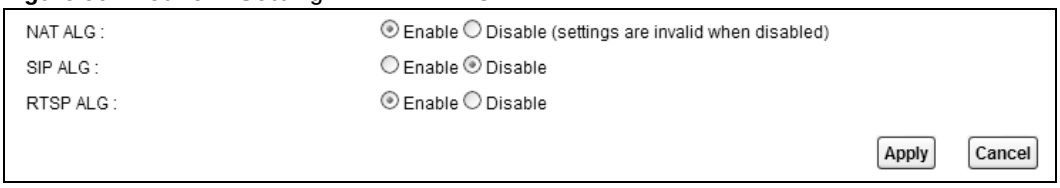
| LABEL | DESCRIPTION |
|---|---|
| Default Server Address | Enter the IP address of the default server which receives packets from ports that are not specified in the **NAT Port Forwarding** screen.<br><br>Note: If you do not assign a **Default Server Address**, the Device discards all packets received 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. |

# 9.6 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 your Device is behind a SIP ALG.

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

**Figure 90** Network Setting > NAT > ALG




The following table describes the fields in this screen.

**Table 61** Network Setting > NAT > ALG

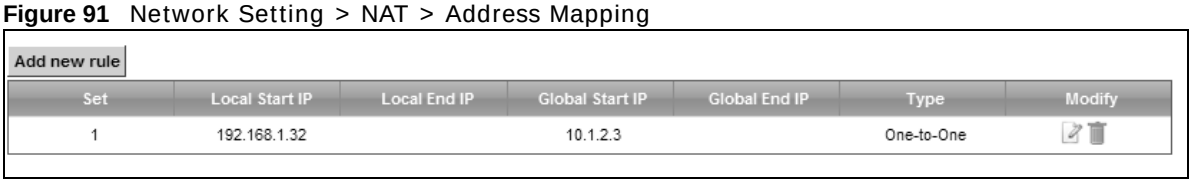
| LABEL | DESCRIPTION |
|---|---|
| NAT ALG | Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules. |
| SIP ALG | Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules. |
| RTSP ALG | Enable this to have the Device detect RTSP traffic and help build RTSP sessions through its NAT. The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 9.7 The Address Mapping Screen

Ordering your rules is important because the Device applies the rules in the order that you specify. When a rule matches the current packet, the Device takes the corresponding action and the remaining rules are ignored.

Click **Network Setting > NAT > Address Mapping** to display the following screen.

**Figure 91** Network Setting > NAT > Address Mapping




The following table describes the fields in this screen.

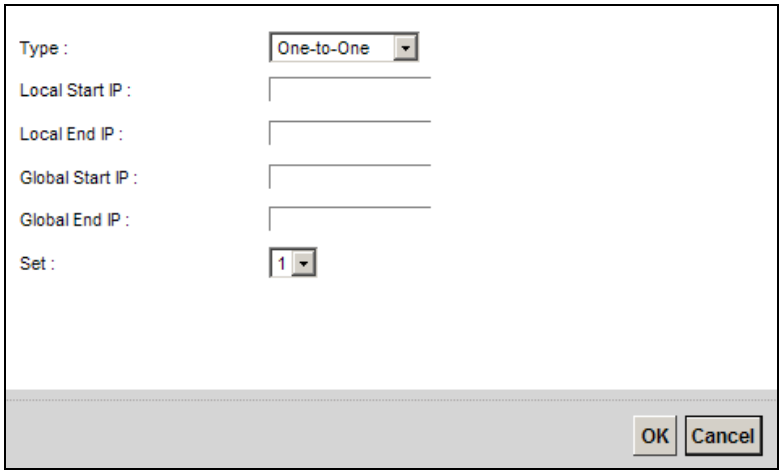
**Table 62** Network Setting > NAT > Address Mapping

| LABEL | DESCRIPTION |
|---|---|
| Add new rule | Click this to create a new rule. |
| Set | This is the index number of the address mapping set. |
| Local Start IP | This is the starting Inside Local IP Address (ILA). |
| Local End IP | This is the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types. |
| Global Start IP | This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the **Many-to-One** mapping type. |
| Global End IP | This is the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types. |
| Type | This is the address mapping type.<br>**One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.<br>**Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only.<br>**Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses. |
| Modify | Click the **Edit** icon to go to the screen where you can edit the address mapping rule.<br>Click the **Delete** icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action. |

## 9.7.1 Add/Edit Address Mapping Rule

To add or edit an address mapping rule, click **Add new rule** or the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

**Figure 92** Address Mapping: Add/Edit




The following table describes the fields in this screen.

**Table 63** Address Mapping: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Type | Choose the IP/port mapping type from one of the following.<br>**One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.<br>**Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only.<br>**Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses. |
| Local Start IP | Enter the starting Inside Local IP Address (ILA). |
| Local End IP | Enter the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types. |
| Global Start IP | Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the **Many-to-One** mapping type. |
| Global End IP | Enter the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types. |
| Set | Select the number of the mapping set for which you want to configure. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 9.8 The Sessions Screen

Use this screen to limit the number of concurrent NAT sessions a client can use. Click **Network Setting > NAT > Sessions** to display the following screen.

**Figure 93** Network Setting > NAT > Sessions


The following table describes the fields in this screen.

**Table 64** Network Setting > NAT > Sessions

| LABEL | DESCRIPTION |
|---|---|
| WAX NAT Session Per Host | Use this field to set a limit to the number of concurrent NAT sessions each client host can have.<br>If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer-to-peer application use, lower this number to ensure no single client uses too many of the available NAT sessions. |
| Apply | Click this to save your changes on this screen. |
| Cancel | Click this to exit this screen without saving any changes. |

# 9.9 Technical Reference

This part contains more information regarding NAT.

## 9.9.1 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 65** 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.

## 9.9.2 What NAT Does

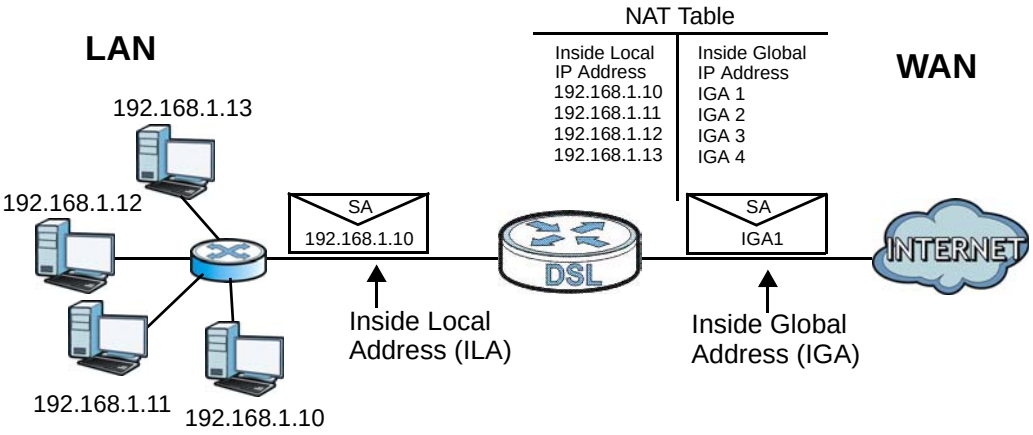
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

## 9.9.3 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.

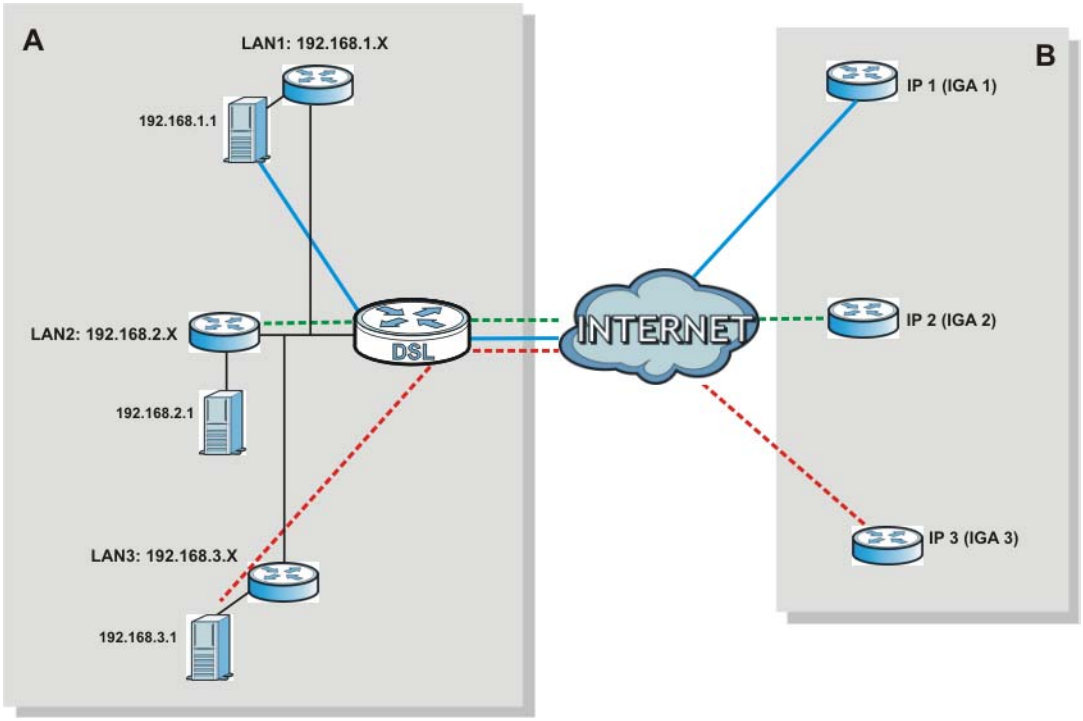
**Figure 94** How NAT Works



## 9.9.4 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 95** NAT Application With IP Alias




### Port Forwarding: Services and Port Numbers

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

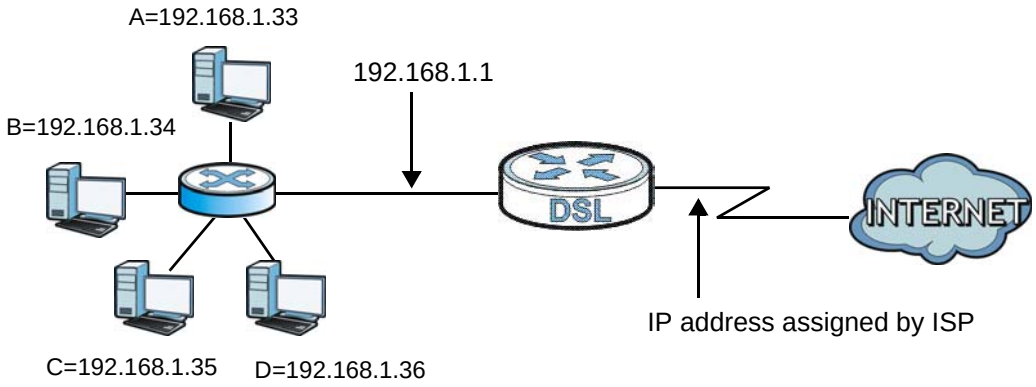
**Table 66** Services and Port Numbers

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

## Port Forwarding Example

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

**Figure 96** Multiple Servers Behind NAT Example



# 10

# Dynamic DNS Setup

## 10.1 Overview

### 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 machine before you can access it.

In addition to the system DNS server(s), each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). The Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

### Dynamic DNS

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

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

### 10.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes (Section 10.2 on page 172).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Device (Section 10.3 on page 173).

### 10.1.2 What You Need To Know

#### DYNDNS Wildcard

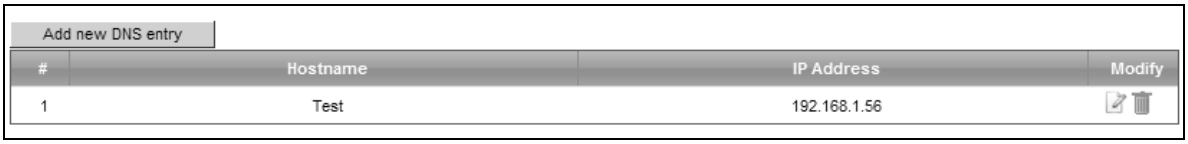
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

## 10.2 The DNS Entry Screen

Use this screen to view and configure DNS routes on the Device. Click **Network Setting > DNS** to open the **DNS Entry** screen.

**Figure 97** Network Setting > DNS > DNS Entry




The following table describes the fields in this screen.

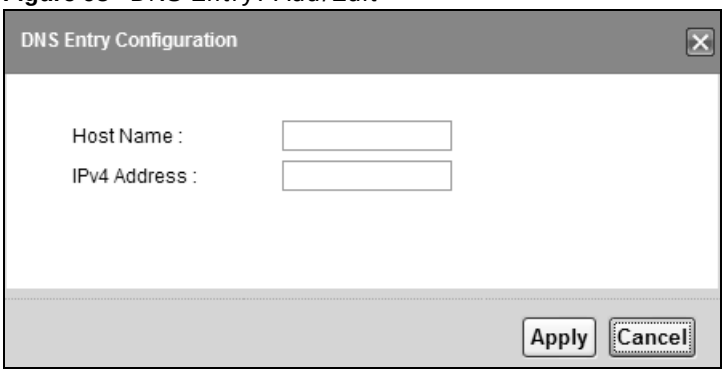
**Table 67** Network Setting > DNS > DNS Entry

| LABEL | DESCRIPTION |
|---|---|
| Add new DNS entry | Click this to create a new DNS entry. |
| # | This is the index number of the entry. |
| Hostname | This indicates the host name or domain name. |
| IP Address | This indicates the IP address assigned to this computer. |
| Modify | Click the **Edit** icon to edit the rule.<br>Click the **Delete** icon to delete an existing rule. |

### 10.2.1 Add/Edit DNS Entry

You can manually add or edit the Device's DNS name and IP address entry. Click **Add new DNS entry** in the **DNS Entry** screen or the **Edit** icon next to the entry you want to edit. The screen shown next appears.

**Figure 98** DNS Entry: Add/Edit




The following table describes the labels in this screen.

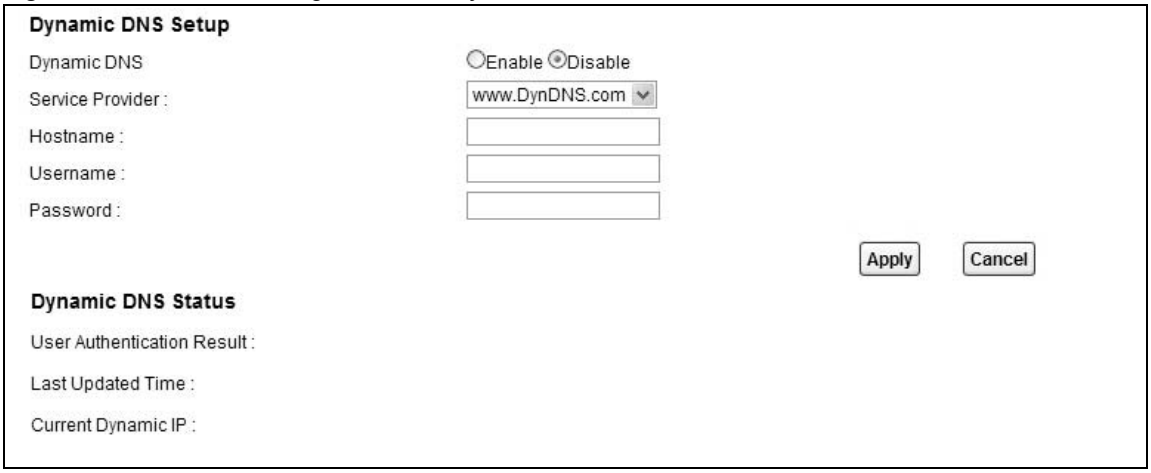
**Table 68** DNS Entry: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Host Name | Enter the host name of the DNS entry. |
| IPv4 Address | Enter the IPv4 IP address of the DNS entry. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 10.3 The Dynamic DNS Screen

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

**Figure 99** Network Setting > DNS > Dynamic DNS



The following table describes the fields in this screen.

**Table 69** Network Setting > DNS > > Dynamic DNS

| LABEL | DESCRIPTION |
|---|---|
| Dynamic DNS Setup | |
| Dynamic DNS | Select **Enable** to use dynamic DNS. |
| Service Provider | Select your Dynamic DNS service provider from the drop-down list box. |
| Hostname | Type the domain name assigned to your Device by your Dynamic DNS provider.<br>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. |
| Dynamic DNS Status | |
| User Authentication Result | This field shows whether or not the DDNS server has accepted the account information you provided to use your DDNS service. |
| Last updated Time | This field shows the most recent date and time the dynamic DNS information was updated. |
| Current Dynamic IP | This field shows the WAN IP address the Device is currently using. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 11

# Interface Group

## 11.1 Overview

By default, all LAN and WAN interfaces on the Device are in the same group and can communicate with each other. Create interface groups to have the Device assign the IP addresses in different domains to different groups. Each group acts as an independent network on the Device. This lets devices connected to an interface group's LAN interfaces communicate through the interface group's WAN or LAN interfaces but not other WAN or LAN interfaces.

### 11.1.1 What You Can Do in this Chapter

The **Interface Group** screens let you create multiple networks on the Device (Section 11.2 on page 175).

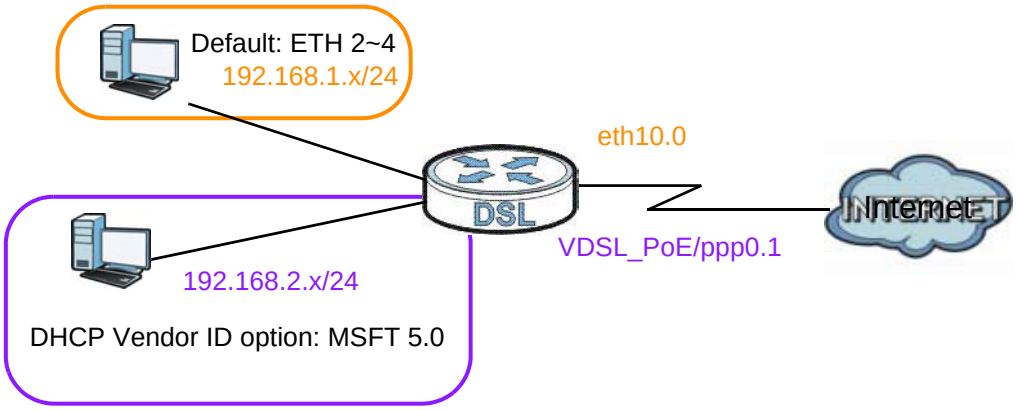
## 11.2 The Interface Group Screen

You can manually add a LAN interface to a new group. Alternatively, you can have the Device automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the Device assigns to the clients in the default and/or user-defined groups. If you set the Device to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See Chapter 6 on page 103 for more information.

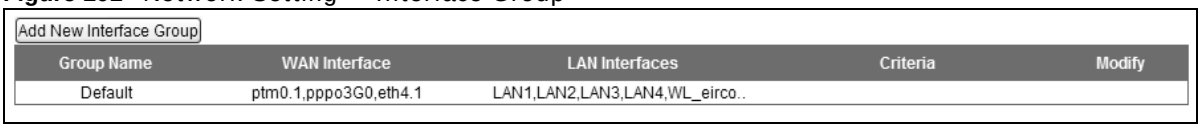
In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN VDSL_PoE/ppp0.1 interface.

**Figure 100** Interface Grouping Application




Click **Network Setting > Interface Group** to open the following screen.

**Figure 101** Network Setting > Interface Group




The following table describes the fields in this screen.

**Table 70** Network Setting > Interface Group

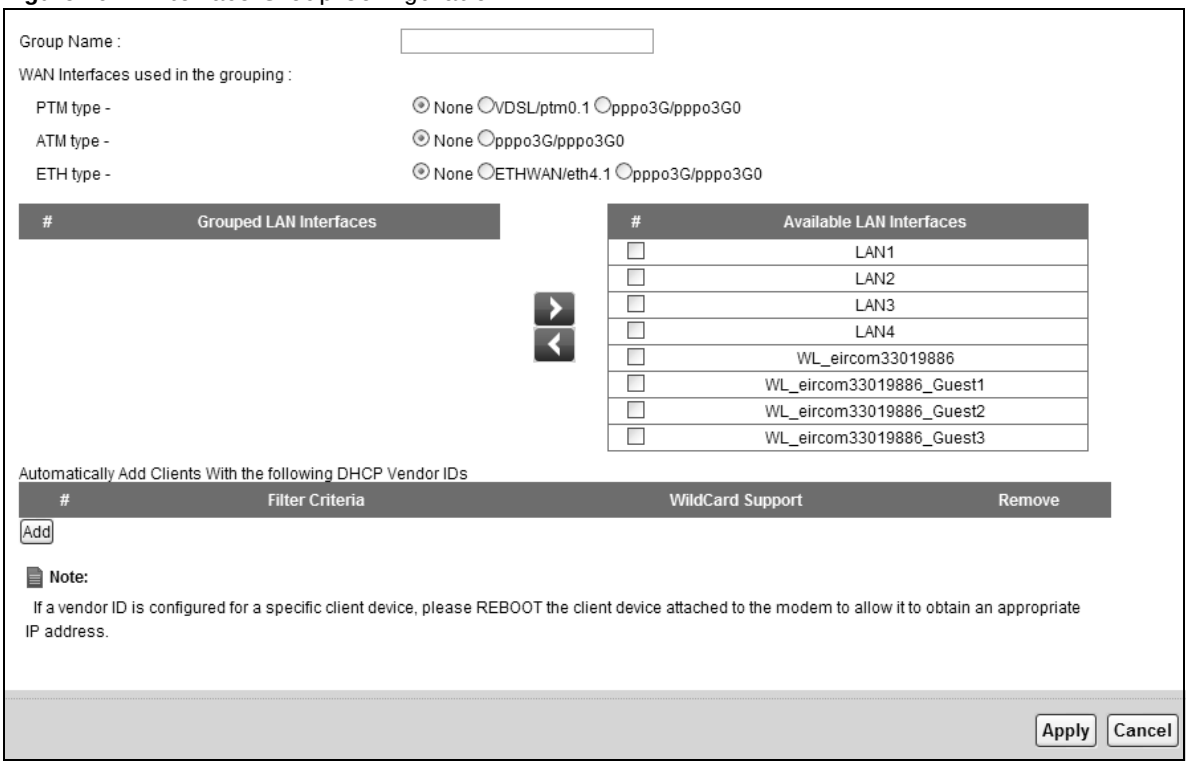
| LABEL | DESCRIPTION |
|---|---|
| Add New Interface Group | Click this button to create a new interface group. |
| Group Name | This shows the descriptive name of the group. |
| WAN Interface | This shows the WAN interfaces in the group. |
| LAN Interfaces | This shows the LAN interfaces in the group. |
| Criteria | This shows the filtering criteria for the group. |
| Modify | Click the **Delete** icon to remove the group. |
| Add | Click this button to create a new group. |

## 11.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Group** screen to open the following screen. Use this screen to create a new interface group.

Note: An interface can belong to only one group at a time.

**Figure 102** Interface Group Configuration




The following table describes the fields in this screen.

**Table 71** Interface Group Configuration

| LABEL | DESCRIPTION |
|---|---|
| Group Name | Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed. |
| WAN Interface used in the grouping | Select the WAN interface this group uses. The group can have up to one PTM interface, up to one ATM interface and up to one ETH interface.<br>Select **None** to not add a WAN interface to this group. |
| Grouped LAN Interfaces<br>Available LAN Interfaces | Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) in the **Available LAN Interfaces** list and use the left arrow to move them to the **Grouped LAN Interfaces** list to add the interfaces to this group.<br>To remove a LAN or wireless LAN interface from the **Grouped LAN Interfaces**, use the right-facing arrow. |
| Automatically Add Clients With the following DHCP Vendor IDs | Click **Add** to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware. See Section 11.2.2 on page 178 for more information. |
| # | This shows the index number of the rule. |
| Filter Criteria | This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically. |
| WildCard Support | This shows if wildcard on DHCP option 60 is enabled. |
| Remove | Click the **Remove** icon to delete this rule from the Device. |

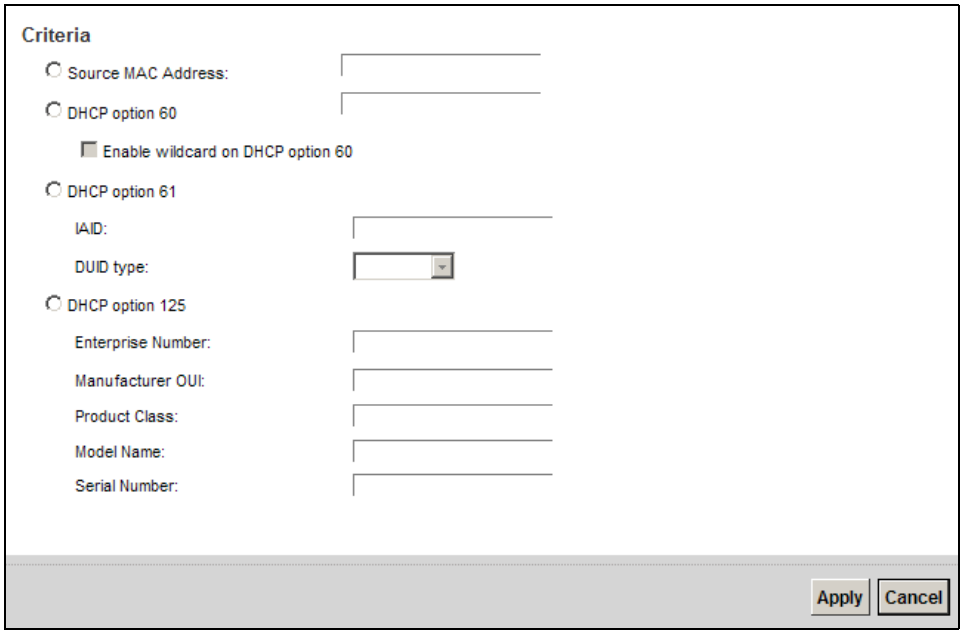
**Table 71** Interface Group Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the Device. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 11.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen.

**Figure 103** Interface Grouping Criteria




The following table describes the fields in this screen.

**Table 72** Interface Grouping Criteria

| LABEL | DESCRIPTION |
|---|---|
| Source MAC Address | Enter the source MAC address of the packet. |
| DHCP Option 60 | Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware. |
| Enable wildcard on DHCP option 60 option | Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60. |
| DHCP Option 61 | Select this and enter the device identity of the matched traffic. |
| IAID | Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number. |

**Table 72** Interface Grouping Criteria (continued)

| LABEL | DESCRIPTION |
|---|---|
| DUID type | Select **DUID-LLT** (DUID Based on Link-layer Address Plus Time) to enter the hardware type, a time value and the MAC address of the device.<br>Select **DUID-EN** (DUID Assigned by Vendor Based upon Enterprise Number) to enter the vendor's registered enterprise number.<br>Select **DUID-LL** (DUID Based on Link-layer Address) to enter the device's hardware type and hardware address (MAC address) in the following fields.<br>Select **Other** to enter any string that identifies the device in the DUID field. |
| DHCP Option 125 | Select this and enter vendor specific information of the matched traffic. |
| Enterprise Number | Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority). |
| Manufacturer OUI | Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address. |
| Product Class | Enter the product class of the device. |
| Model Name | Enter the model name of the device. |
| Serial Number | Enter the serial number of the device. |
| Apply | Click **Apply** to save your changes back to the Device. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 12

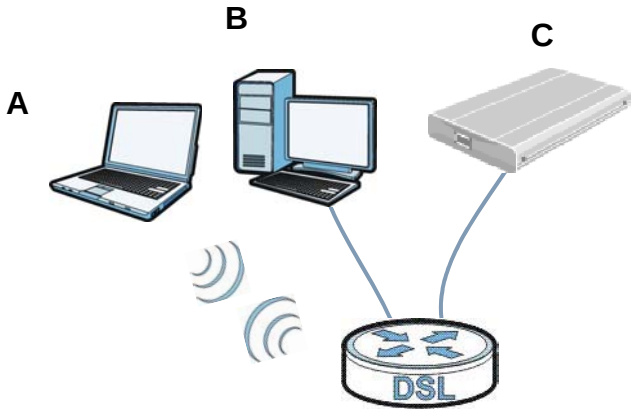
# USB Service

## 12.1 Overview

You can 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 104** File Sharing Overview




The Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

### 12.1.1 What You Can Do in this Chapter

- Use the **File Sharing** screen to enable file-sharing server (Section 12.2 on page 183).
- Use the **Media Server** screen to enable or disable the sharing of media files (Section 12.3 on page 184).
- Use the **Printer Server** screen to enable the print server (Section 12.4.2 on page 185).

### 12.1.2 What You Need To Know

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

### 12.1.2.1 About File Sharing

#### 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.

#### Common Internet File System

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).

### 12.1.2.2 About Printer Server

#### 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.

#### TCP/IP

TCP/IP (Transmission Control Protocol/ Internet Protocol) is a set of communications protocols that most of the Internet runs on.

#### 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.

### Supported OSs

Your operating system must support TCP/IP ports for printing and be compatible with the RAW (port 9100) protocol.

The following OSs support Device's printer sharing feature.

- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows Me, Windows NT 4.0, Windows 2000, Windows XP or Macintosh OS X.

## 12.1.3 Before You Begin

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

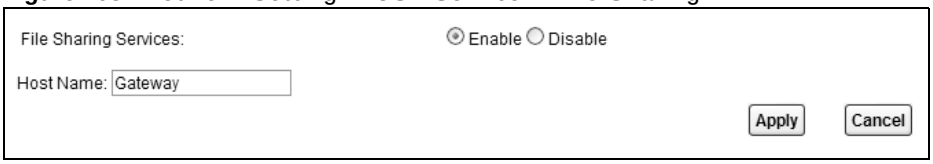
1. Connect the USB device to one of the Device's USB port. Make sure the Device is connected to your network.
2. The Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected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

Note: If your USB device cannot be detected by the Device, see the troubleshooting for suggestions.

# 12.2 The File Sharing Screen

Use this screen to set up file sharing through the Device. The Device's LAN users can access the shared folder (or share) from the USB device inserted in the Device. To access this screen, click **Network Setting > USB Service > File Sharing**.

**Figure 105** Network Setting > USB Service > File Sharing




Each field is described in the following table.

**Table 73** Network Setting > Home Networking > File Sharing

| LABEL | DESCRIPTION |
|---|---|
| File Sharing Services | Select **Enable** to activate file sharing through the Device. |
| Host Name | Enter the host name on the share. |
| Apply | Click this to save your changes to the Device. |
| Cancel | Click this to restore your previously saved settings. |

# 12.3 The Media Server Screen

The media server feature lets anyone on your network play video, music, and photos from the USB storage device connected to your Device (without having to copy them to another computer). The Device can function as a DLNA-compliant media server. The Device streams files to DLNA-compliant media clients (like Windows Media Player). The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

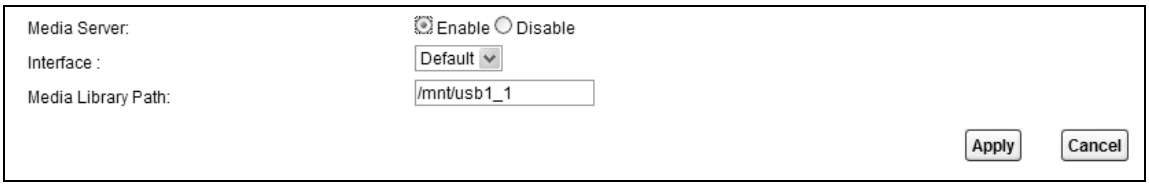
The Device media server enables you to:

- Publish all shares for everyone to play media files in the USB storage device connected to the Device.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

To change your Device's media server settings, click **Network Setting > USB Service > Media Server**. The screen appears as shown.

**Figure 106** Network Setting > USB Service > Media Server




The following table describes the labels in this menu.

**Table 74** Network Setting > USB Service > Media Server

| LABEL | DESCRIPTION |
|---|---|
| Media Server | Select **Enable** to have the Device function as a DLNA-compliant media server.<br><br>Enable the media server to let (DLNA-compliant) media clients on your network play media files located in the shares. |
| Interface | Select an interface on which you want to enable the media server function. |
| Media Library Path | Enter the path clients use to access the media files on a USB storage device connected to the Device. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 12.4 Printer 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 configuring a TCP/IP port on the computers connected to your network.

## 12.4.1 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.
- A USB printer with the driver already installed on your computer.
- The computers on your network must have the printer software already installed before they can create a TCP/IP port for printing via the network. Follow your printer manufacturers instructions on how to install the printer software on your computer.

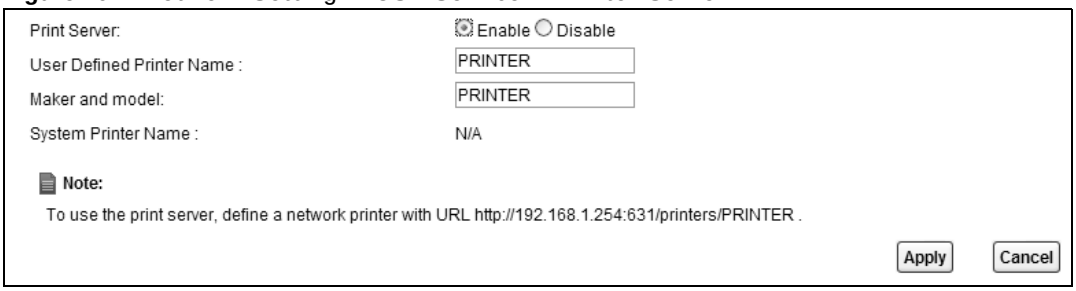
Note: Your printer's installation instructions may ask that you connect the printer to your computer. Connect your printer to the Device instead.

## 12.4.2 The Printer Server Screen

Use this screen to enable or disable sharing of a USB printer via your Device.

To access this screen, click **Network Setting > USB Service > Printer Server**.

**Figure 107** Network Setting > USB Service > Printer Server




The following table describes the labels in this menu.

**Table 75** Network Setting > USB Service > Print Server

| LABEL | DESCRIPTION |
|---|---|
| Printer Server | Select **Enable** to have the Device share a USB printer. |
| User Defined Printer Name | Type the name for the printer. |
| Maker and model | Type up to 80 characters for the manufacturer and model number of the printer. |
| System Printer Name | This field shows the printer's system name the Device has detected from one of the USB ports. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 13

# Firewall

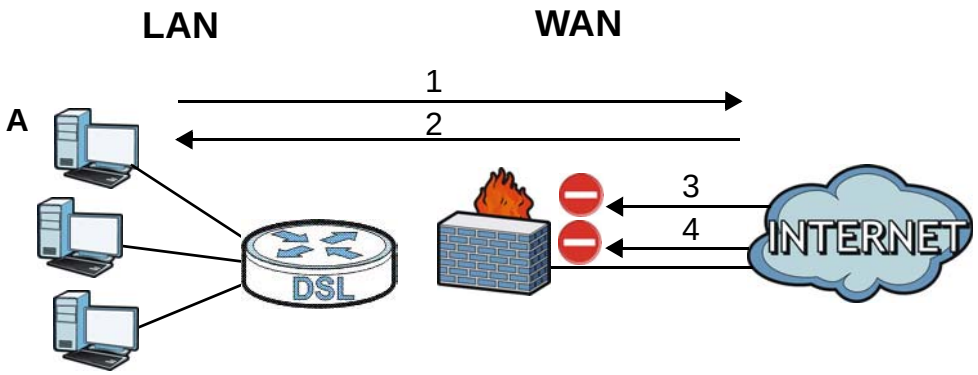
## 13.1 Overview

This chapter shows you how to enable and configure the Device's security settings. Use the firewall to protect your Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

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

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

**Figure 108** Default Firewall Action




### 13.1.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Device (Section 13.2 on page 189).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 13.3 on page 189).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules (Section 13.4 on page 191).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (.Section 13.5 on page 194).

## 13.1.2 What You Need to Know

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

### DDoS

A 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 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

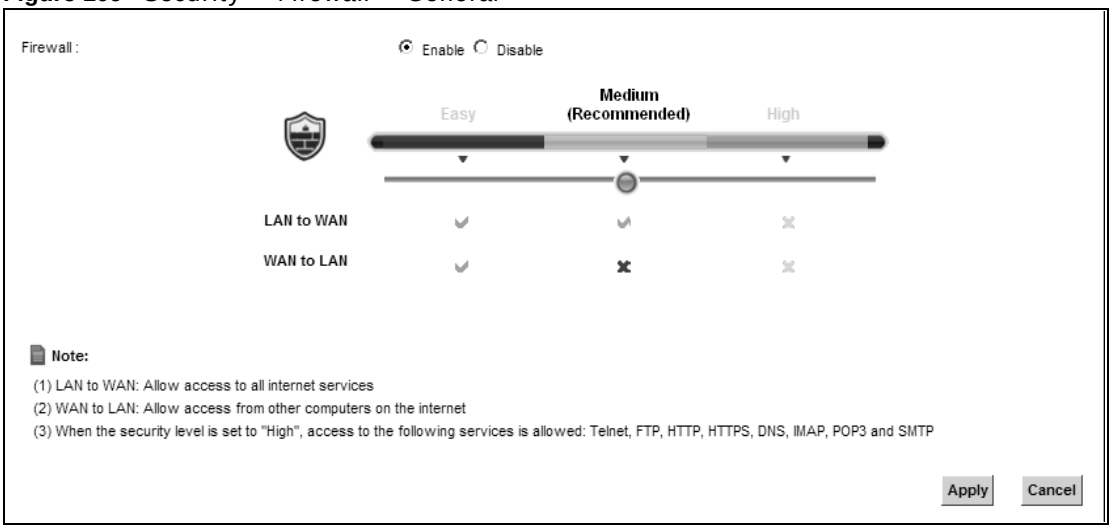
Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

# 13.2 The Firewall Screen

Use this screen to set the security level of the firewall on the Device. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Click **Security > Firewall** to display the **General** screen.

**Figure 109** Security > Firewall > General




The following table describes the labels in this screen.

**Table 76** Security > Firewall > General

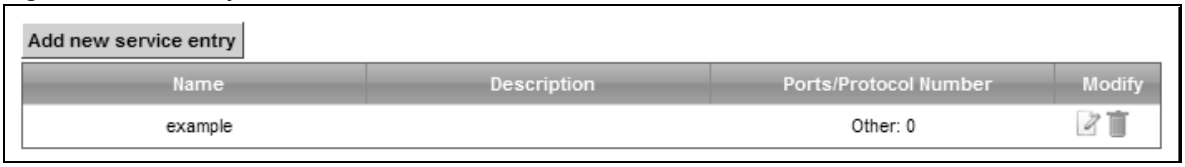
| LABEL | DESCRIPTION |
|---|---|
| Firewall | Select **Enable** to activate the firewall feature on the Device. |
| Easy | Select **Easy** to allow LAN to WAN and WAN to LAN packet directions. |
| Medium | Select **Medium** to allow LAN to WAN but deny WAN to LAN packet directions. |
| High | Select **High** to deny LAN to WAN and WAN to LAN packet directions. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 13.3 The Protocol Screen

You can configure customized services and port numbers in the **Protocol** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See Appendix F on page 347 for some examples.

Click **Security > Firewall > Protocol** to display the following screen.

**Figure 110** Security > Firewall > Protocol




The following table describes the labels in this screen.

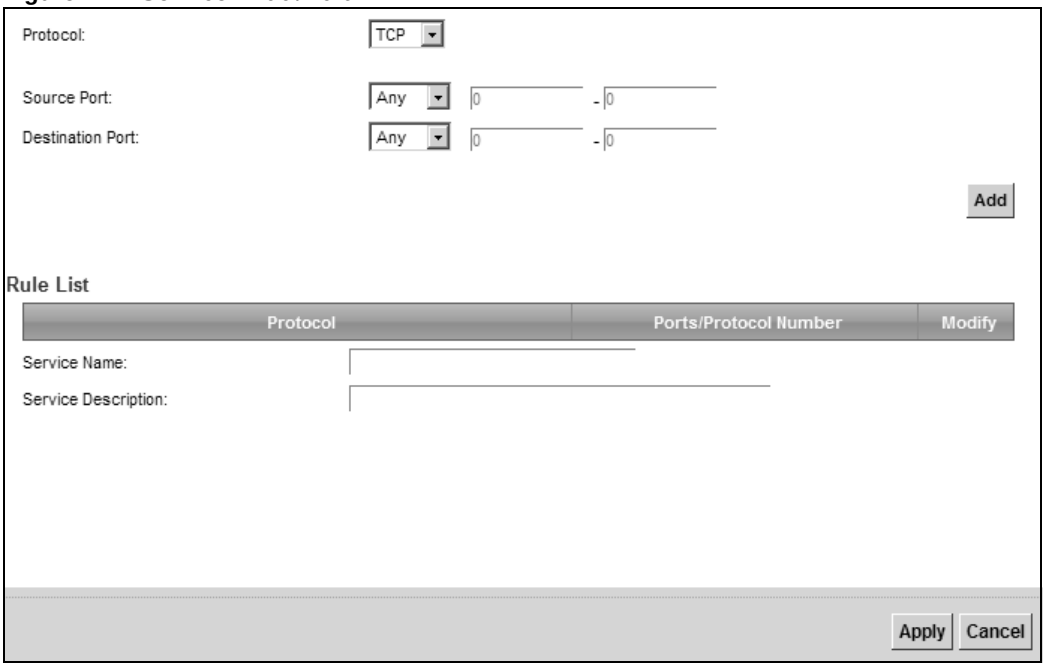
**Table 77** Security > Firewall > Protocol

| LABEL | DESCRIPTION |
|---|---|
| Add new service entry | Click this to add a new service. |
| Name | This is the name of your customized service. |
| Description | This is the description of your customized service. |
| Ports/Protocol Number | This shows the IP protocol (**TCP**, **UDP**, **ICMP**, or **TCP/UDP**) and the port number or range of ports that defines your customized service. **Other** and the protocol number displays if the service uses another IP protocol. |
| Modify | Click the **Edit** icon to edit the entry.<br>Click the **Delete** icon to remove this entry. |

## 13.3.1 Add/Edit a Service

Use this screen to add a customized service rule that you can use in the firewall's ACL rule configuration. Click **Add new service entry** or the edit icon next to an existing service rule in the **Service** screen to display the following screen.

**Figure 111** Service: Add/Edit



The following table describes the labels in this screen.

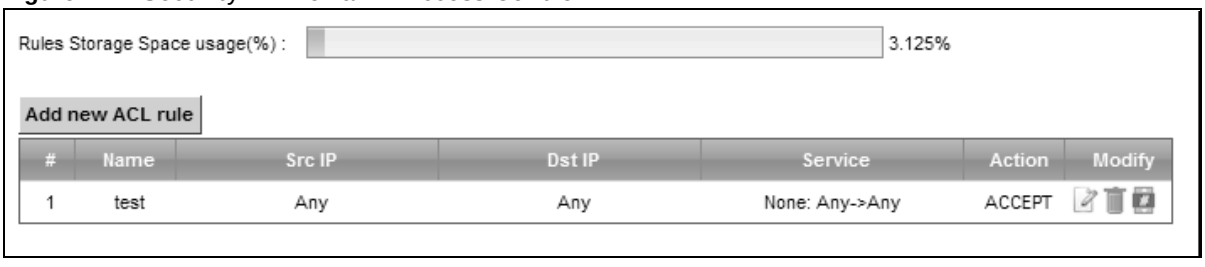
**Table 78** Service: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Protocol | Choose the IP protocol (**TCP**, **UDP**, **ICMP**, or **Other**) that defines your customized port from the drop-down list box. Select **Other** to be able to enter a protocol number. |
| Source/ Destination Port | These fields are displayed if you select **TCP** or **UDP** as the IP port.<br>Select **Single** to specify one port only or **Range** to specify a span of ports that define your customized service. If you select **Any**, the service is applied to all ports.<br>Type a single port number or the range of port numbers that define your customized service. |
| Protocol Number | This field is displayed if you select **Other** as the protocol.<br>Enter the protocol number of your customized port. |
| Add | Click this to add the protocol to the **Rule List** below. |
| Rule List | |
| Protocol | This is the IP port (**TCP**, **UDP**, **ICMP**, or **Other**) that defines your customized port. |
| Ports/Protocol Number | For **TCP**, **UDP**, **ICMP**, or **TCP/UDP** protocol rules this shows the port number or range that defines the custom service. For other IP protocol rules this shows the protocol number. |
| Delete | Click the **Delete** icon to remove the rule. |
| Service Name | Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port. |
| Service Description | Enter a description for your customized port. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 13.4 The Access Control Screen

Click **Security > Firewall > Access Control** to display the following screen. This screen displays a list of the configured incoming or outgoing filtering rules.

**Figure 112** Security > Firewall > Access Control




The following table describes the labels in this screen.

**Table 79** Security > Firewall > Access Control

| LABEL | DESCRIPTION |
|---|---|
| Add new ACL rule | Click this to go to add a filter rule for incoming or outgoing IP traffic. |
| # | This is the index number of the entry. |

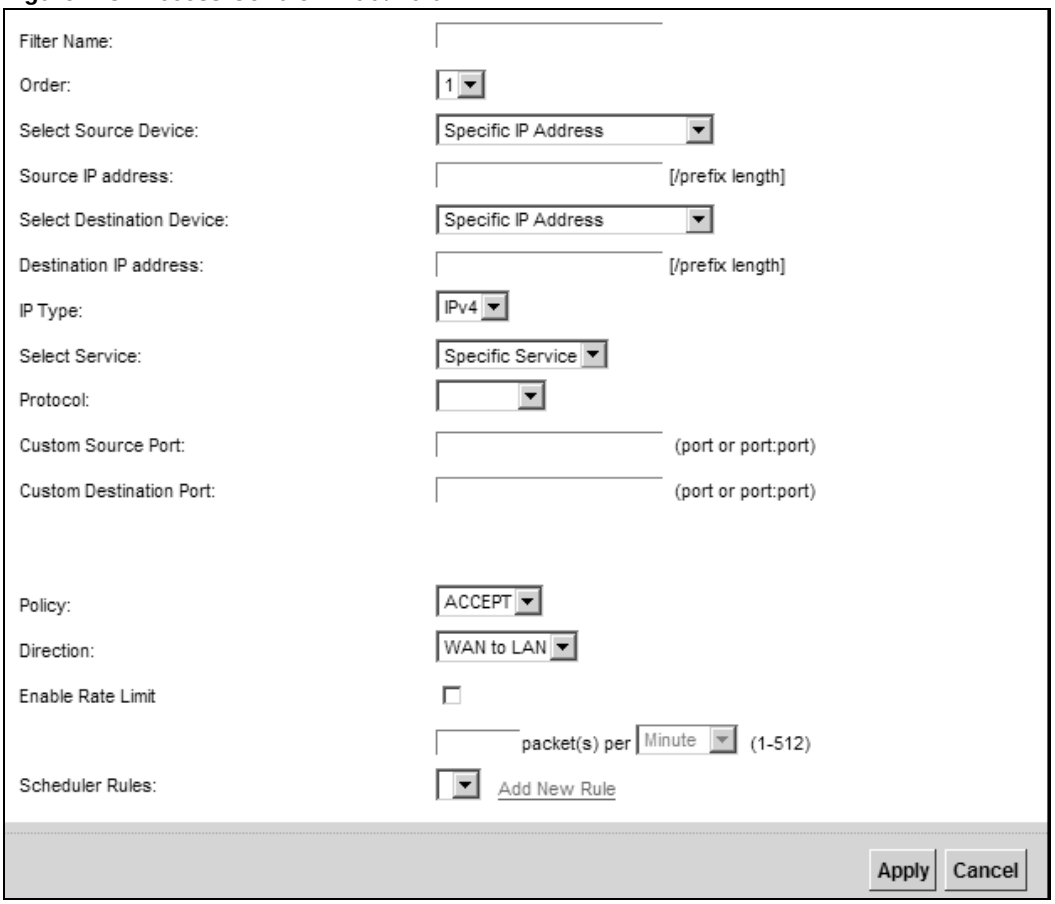
**Table 79** Security > Firewall > Access Control (continued)

| LABEL | DESCRIPTION |
|---|---|
| Name | This displays the name of the rule. |
| Src IP | This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to **Any**. |
| Dst IP | This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to **Any**. |
| Service | This displays the transport layer protocol that defines the service and the direction of traffic to which this rule applies. |
| Action | This field displays whether the rule 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 (**ACCEPT**). |
| Modify | Click the **Edit** icon to edit the rule.<br>Click the **Delete** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.<br>Click the **Move To** icon to change the order of the rule. Enter the number in the # field. |

## 13.4.1 Add/Edit an ACL Rule

Click **Add new ACL rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays.

**Figure 113** Access Control: Add/Edit



The following table describes the labels in this screen.

**Table 80** Access Control: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Filter Name | Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.<br>You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule. |
| Order | Select the order of the ACL rule. |
| Select Source Device | Select the source device to which the ACL rule applies. If you select **Specific IP Address**, enter the source IP address in the field below. |
| Source IP Address | Enter the source IP address. |
| Select Destination Device | Select the destination device to which the ACL rule applies. If you select **Specific IP Address**, enter the destiniation IP address in the field below. |
| Destination IP Address | Enter the destination IP address. |
| IP Type | Select whether your IP type is **IPv4** or **IPv6**. |
| Select Protocol | Select the transport layer protocol that defines your customized port from the drop-down list box. The specific protocol rule sets you add in the **Security > Firewall > Service > Add** screen display in this list.<br>If you want to configure a customized protocol, select **Specific Service**. |
| Protocol | This field is displayed only when you select **Specific Protocol** in **Select Protocol**.<br>Choose the IP port (**TCP/UDP**, **TCP**, **UDP**, **ICMP**, or **ICMPv6**) that defines your customized port from the drop-down list box. |
| Custom Source Port | This field is displayed only when you select **Specific Protocol** in **Select Protocol**.<br>Enter a single port number or the range of port numbers of the source. |
| Custom Destination Port | This field is displayed only when you select **Specific Protocol** in **Select Protocol**.<br>Enter a single port number or the range of port numbers of the destination. |
| Policy | 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 (**ACCEPT**) packets that match this rule. |
| Direction | Use the drop-down list box to select the direction of traffic to which this rule applies. |
| Enable Rate Limit | Select this check box to set a limit on the upstream/downstream transmission rate for the specified protocol.<br>Specify how many packets per minute or second the transmission rate is. |
| Scheduler Rules | Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by click **Add New Rule**. This will bring you to the **Security > Scheduler Rules** screen. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 13.5 The DoS Screen

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Use the **DoS** screen to activate protection against DoS attacks. Click **Security > Firewall > DoS** to display the following screen.

**Figure 114** Security > Firewall > DoS


The following table describes the labels in this screen.

**Table 81** Security > Firewall > DoS

| LABEL | DESCRIPTION |
|---|---|
| DoS Protection Blocking | Select **Enable** to enable protection against DoS attacks. |
| Deny Ping Response | Select Enable to block ping request packets. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 14

# MAC Filter

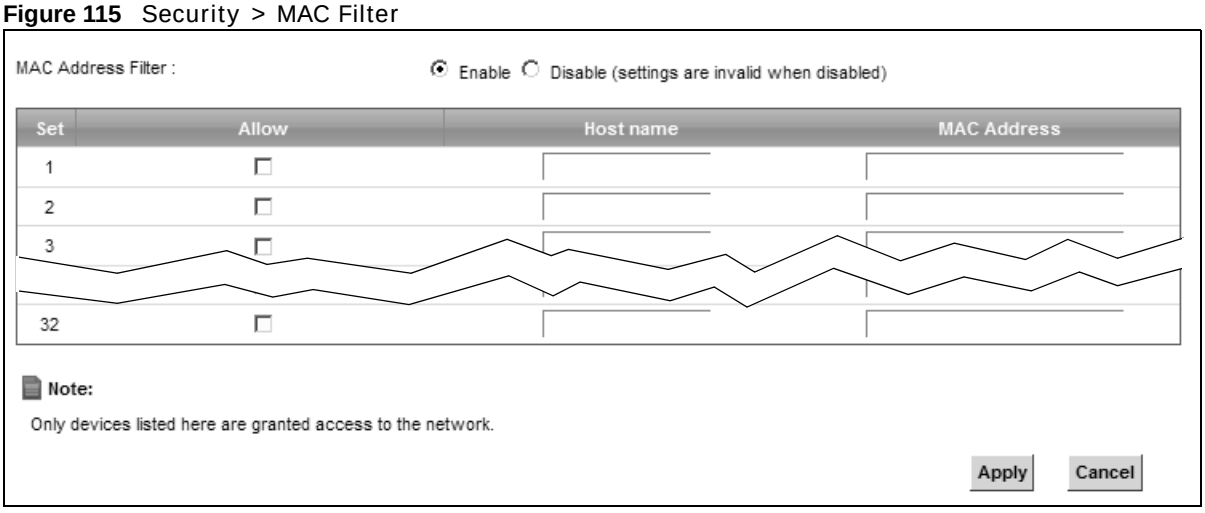
## 14.1 Overview

You can configure the Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. 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.

## 14.2 The MAC Filter Screen

Use this screen to allow wireless and LAN clients access to the Device. Click **Security** > **MAC Filter**. The screen appears as shown.

**Figure 115** Security > MAC Filter




The following table describes the labels in this screen.

**Table 82** Security > MAC Filter

| LABEL | DESCRIPTION |
|---|---|
| MAC Address Filter | Select **Enable** to activate the MAC filter function. |
| Set | This is the index number of the MAC address. |
| Allow | Select **Allow** to permit access to the Device. MAC addresses not listed will be denied access to the Device.<br><br>If you clear this, the MAC Address field for this set clears. |
| Host name | Enter the host name of the wireless or LAN clients that are allowed access to the Device. |

**Table 82** Security > MAC Filter (continued)

| LABEL | DESCRIPTION |
|---|---|
| MAC Address | Enter the MAC addresses of the wireless or LAN clients that are allowed 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. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 15

# Parental Control

## 15.1 Overview

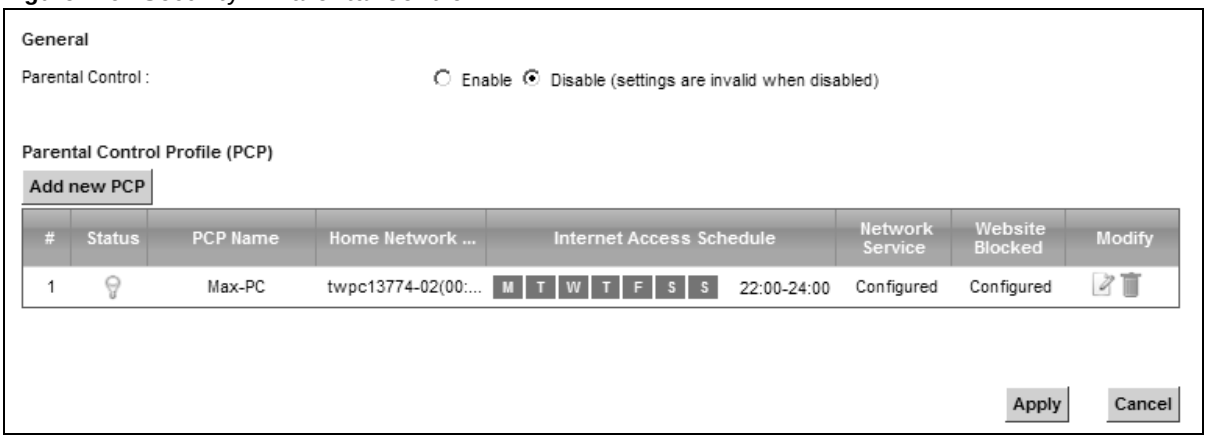
Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the Device performs parental control on a specific user.

## 15.2 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 116** Security > Parental Control




The following table describes the fields in this screen.

**Table 83** Security > Parental Control

| LABEL | DESCRIPTION |
|---|---|
| Parental Control | Select **Enable** to activate parental control. |
| Add new PCP | Click this if you want to configure a new parental control rule. |
| # | This shows the index number of the rule. |
| Status | This indicates whether the rule is active or not.<br>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 (MAC) | This shows the MAC address of the LAN user's computer to which this rule applies. |

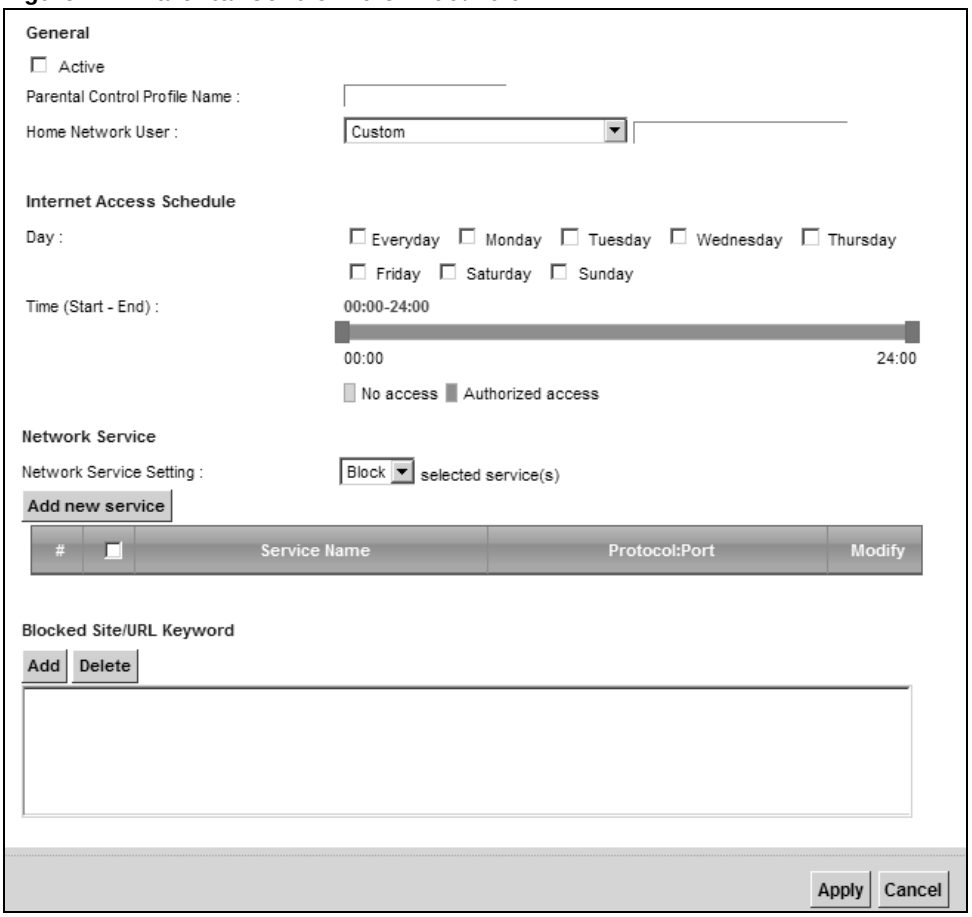
**Table 83** Security > Parental Control (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Website Block | 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.<br>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. |

## 15.2.1 Add/Edit a 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 117** Parental Control Rule: Add/Edit



The following table describes the fields in this screen.

**Table 84** Parental Control Rule: 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 | Drag the time bar to define the 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.<br>If you select **Allow**, 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. |
| # | This shows the index number of the rule. Select the checkbox next to the rule to activate it. |
| Service Name | This shows the name of the rule. |
| Protocol:Port | This shows the protocol and the port of the rule. |
| Modify | Click the **Edit** icon to go to the screen where you can edit the rule.<br>Click the **Delete** icon to delete an existing rule. |
| Blocked Site/ URL Keyword | Click **Add** to show a screen to enter the URL of web site or URL keyword to which the Device blocks access. Click **Delete** to remove it. |
| Apply | Click this button to save your settings back to the Device. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 16

# Scheduler Rule

## 16.1 Overview

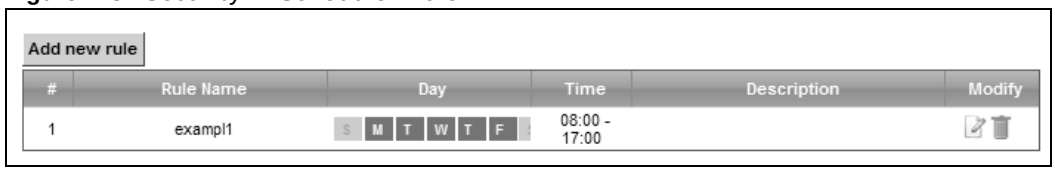
You can define time periods and days during which the Device performs scheduled rules of certain features (such as Firewall Access Control) in the **Scheduler Rule** screen.

## 16.2 The Scheduler Rule Screen

Use this screen to view, add, or edit time schedule rules.

Click **Security > Scheduler Rule** to open the following screen.

**Figure 118** Security > Scheduler Rule




The following table describes the fields in this screen.

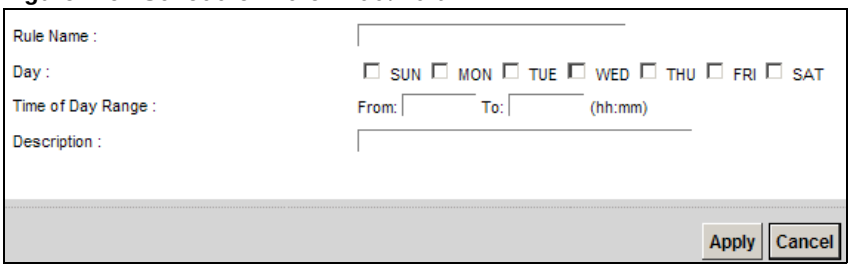
**Table 85** Security > Scheduler Rule

| LABEL | DESCRIPTION |
|---|---|
| Add new rule | Click this to create a new rule. |
| # | This is the index number of the entry. |
| Rule Name | This shows the name of the rule. |
| Day | This shows the day(s) on which this rule is enabled. |
| Time | This shows the period of time on which this rule is enabled. |
| Description | This shows the description of this rule. |
| Modify | Click the **Edit** icon to edit the schedule.<br>Click the **Delete** icon to delete a scheduler rule.<br><br>Note: You cannot delete a scheduler rule once it is applied to a certain feature. |

## 16.2.1 Add/Edit a Schedule

Click the **Add** button in the **Scheduler Rule** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule.

**Figure 119** Scheduler Rule: Add/Edit




The following table describes the fields in this screen.

**Table 86** Scheduler Rule: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Rule Name | Enter a name (up to 31 printable English keyboard characters, not including spaces) for this schedule. |
| Day | Select check boxes for the days that you want the Device to perform this scheduler rule. |
| Time if Day Range | Enter the time period of each day, in 24-hour format, during which the rule will be enforced. |
| Description | Enter a description for this scheduler rule. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 17

# Certificates

## 17.1 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.

### 17.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the Device's CA-signed certificates (Section 17.3 on page 203).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the Device (Section 17.4 on page 206).

## 17.2 What You Need to Know

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

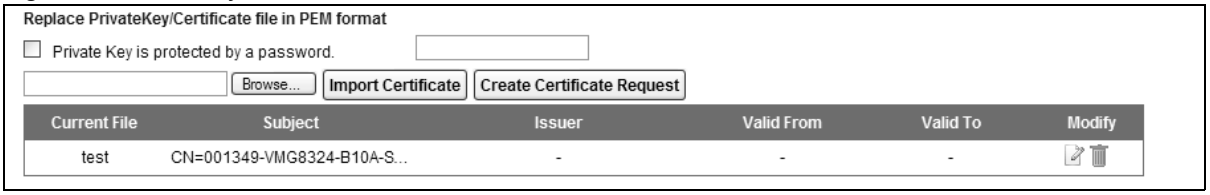
#### Certification Authority

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.

## 17.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. This is the Device's summary list of certificates and certification requests.

**Figure 120** Security > Certificates > Local Certificates



The following table describes the labels in this screen.

**Table 87** Security > Certificates > Local Certificates

| LABEL | DESCRIPTION |
|---|---|
| Private Key is protected by a password? | Select the checkbox and enter the private key into the text box to store it on the Device. The private key should not exceed 63 ASCII characters (not including spaces). |
| Browse... | Click this to find the certificate file you want to upload. |
| Import Certificate | Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Device. |
| Create Certificate Request | Click this button to go to the screen where you can have the Device generate a certification request. |
| 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. |
| Modify | Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request).<br>For a certification request, click **Load Signed** to import the signed certificate.<br>Click the **Remove** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use. |

## 17.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the Device generate a certification request.

**Figure 121** Create Certificate Request

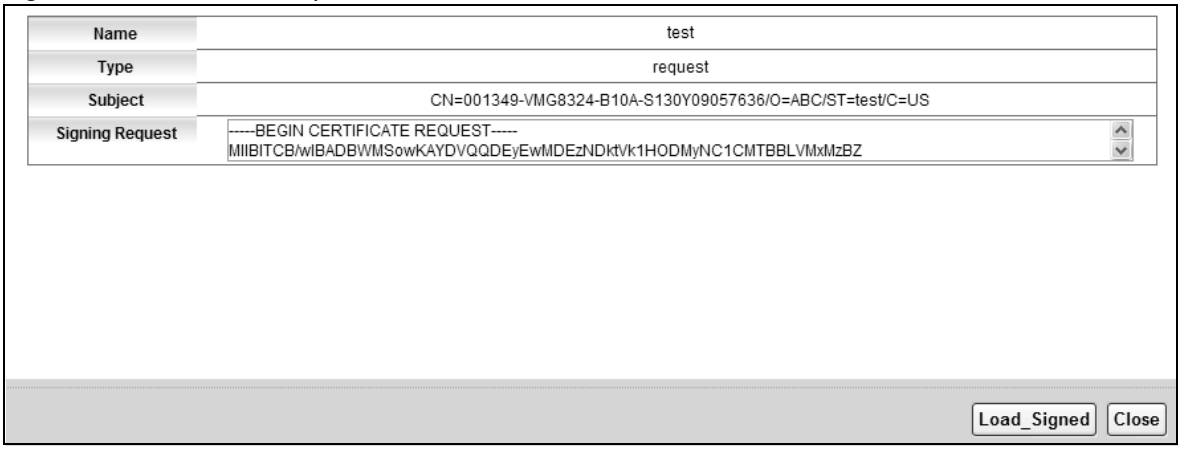
The following table describes the labels in this screen.

**Table 88** Create Certificate Request

| LABEL | DESCRIPTION |
|---|---|
| Certificate Name | Type up to 63 ASCII characters (not including spaces) to identify this certificate. |
| Common Name | Select **Auto** to have the Device configure this field automatically. Or select **Customize** to enter it manually.<br>Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string. |
| Organization Name | Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the Device drops trailing spaces. |
| State/Province Name | Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the Device drops trailing spaces. |
| Country/Region Name | Select a country to identify the nation where the certificate owner is located. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

After you click **Apply**, the following screen displays to notify you that you need to get the certificate request signed by a Certificate Authority. If you already have, click **Load_Signed** to import the signed certificate into the Device. Otherwise click **Back** to return to the **Local Certificates** screen.

**Figure 122** Certificate Request Created

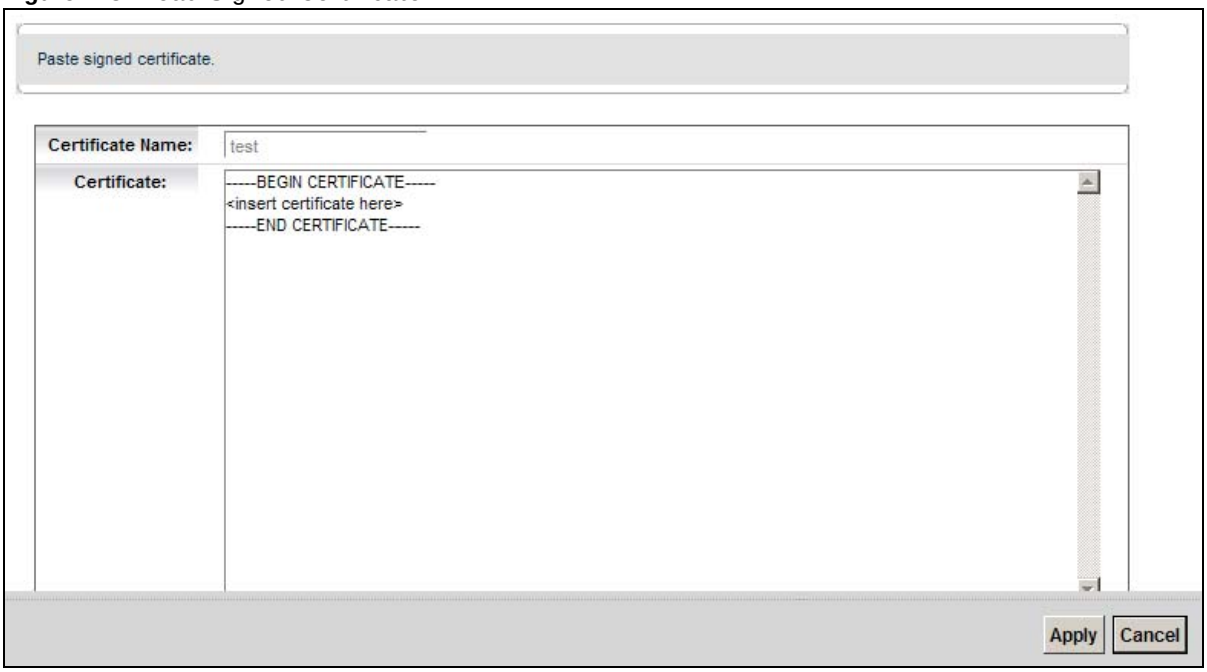



## 17.3.2 Load Signed Certificate

After you create a certificate request and have it signed by a Certificate Authority, in the **Local Certificates** screen click the certificate request's **Load Signed** icon to import the signed certificate into the Device.

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

**Figure 123** Load Signed Certificate




The following table describes the labels in this screen.

**Table 89** Load Signed Certificate

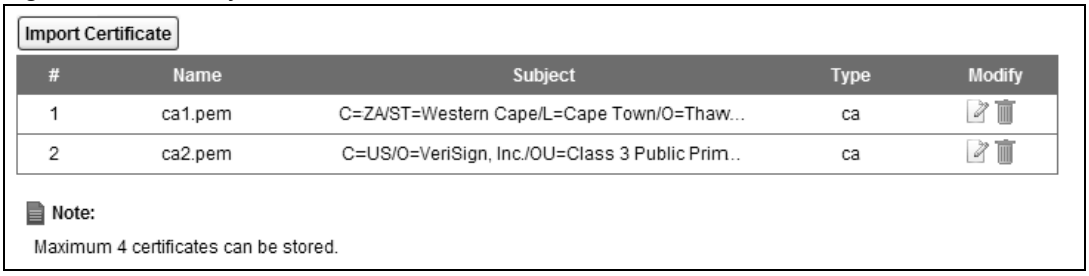
| LABEL | DESCRIPTION |
|---|---|
| Certificate Name | This is the name of the signed certificate. |
| Certificate | Copy and paste the signed certificate into the text box to store it on the Device. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 17.4 The Trusted CA Screen

Click **Security > Certificates > Trusted CA** to open the following screen. This screen displays 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.

**Figure 124** Security > Certificates > Trusted CA




The following table describes the fields in this screen.

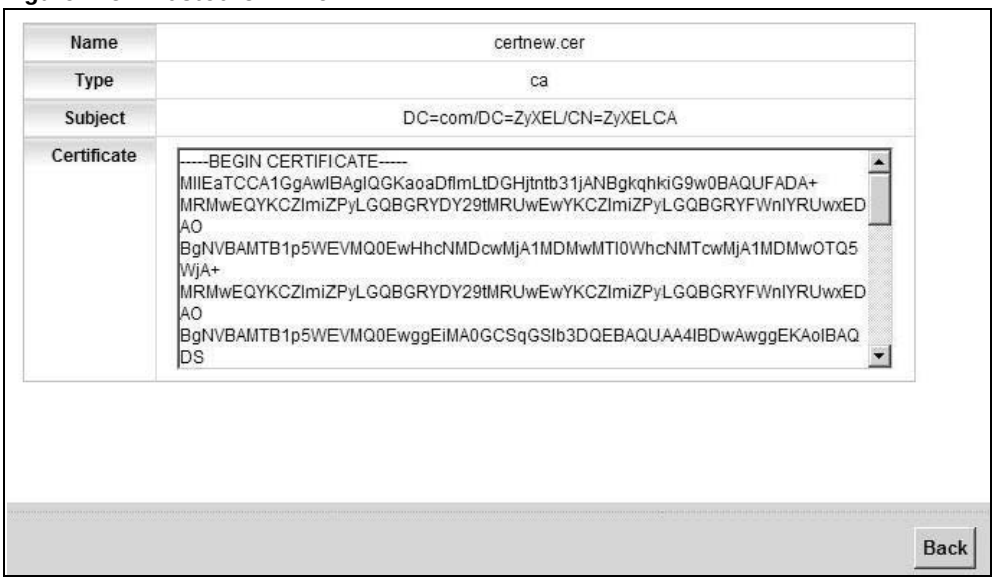
**Table 90** Security > Certificates > Trusted CA

| 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. |
| # | This is the index number of the entry. |
| 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. |
| Modify | Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request).<br>Click the **Delete** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use. |

## 17.4.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate.

**Figure 125** Trusted CA: View




The following table describes the fields in this screen.

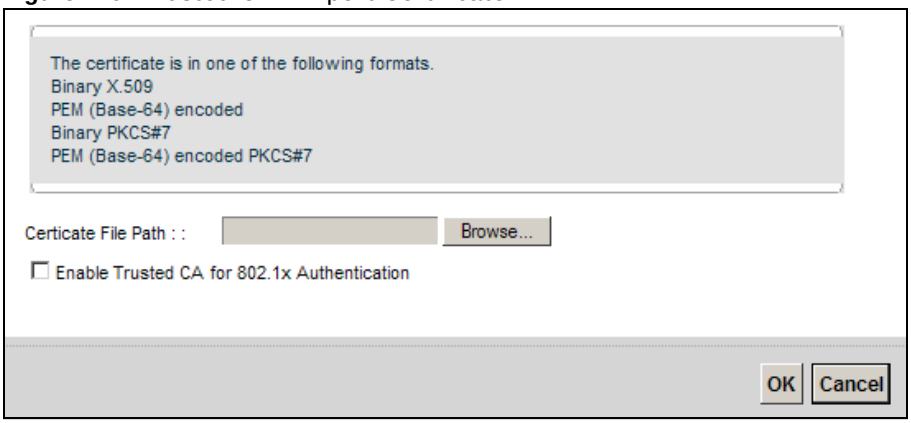
**Table 91** Trusted CA: View

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. |
| Type | This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C). |
| Certificate | This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form.<br>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 **Back** to return to the previous screen. |

## 17.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The Device trusts any valid certificate signed by any of the imported trusted CA certificates.

**Figure 126** Trusted CA: Import Certificate




The following table describes the fields in this screen.

**Table 92** Trusted CA: Import Certificate

| LABEL | DESCRIPTION |
|---|---|
| Certificate File Path | Type in the location of the certificate you want to upload in this field or click **Browse ...** to find it. |
| Enable Trusted CA for 802.1x Authentication | If you select this checkbox, the trusted CA will be used for 802.1x authentication. The selected trusted CA will be displayed in the **Network Setting** > **Broadband** > **802.1x: Edit** screen. |
| Certificate | Copy and paste the certificate into the text box to store it on the Device. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 18 VPN

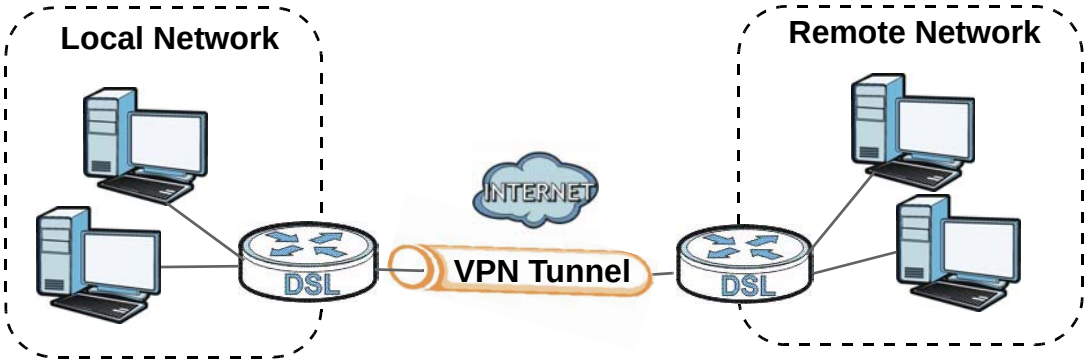
## 18.1 Overview

A virtual private network (VPN) provides secure communications over the the Internet. Internet Protocol Security (IPSec) is a standards-based VPN that provides confidentiality, data integrity, and authentication. This chapter shows you how to configure the Device's VPN settings.

## 18.2 The IPSec VPN General Screen

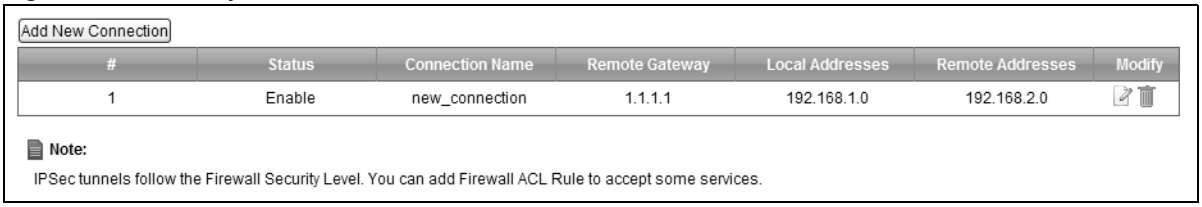
Use this screen to view and manage your VPN tunnel policies. The following figure helps explain the main fields in the web configurator.

**Figure 127** IPSec Fields Summary




Click **Security > IPSec VPN** to open this screen as shown next.

**Figure 128** Security > IPSec VPN



This screen contains the following fields:

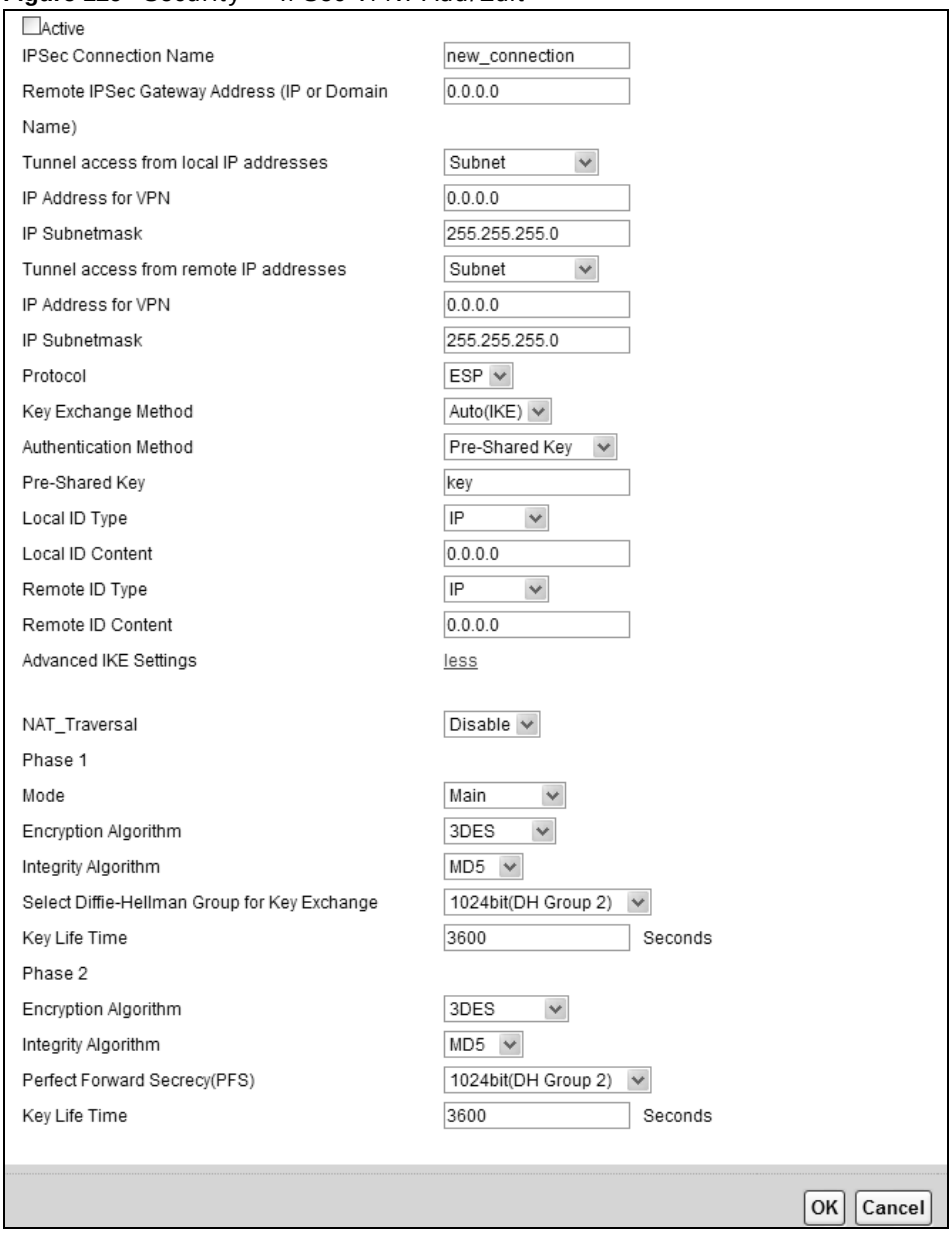
**Table 93** Security > IPSec VPN

| LABEL | DESCRIPTION |
|---|---|
| Add New Connection | Click this button to add an item to the list. |
| # | This displays the index number of an entry. |
| Status | This displays whether the VPN policy is enabled (**Enable**) or not (**Disable**). |
| Connection Name | The name of the VPN policy. |
| Remote Gateway | This is the IP address of the remote IPSec router in the IKE SA. |
| Local Addresses | This displays the IP address(es) on the LAN behind your Device. |
| Remote Addresses | This displays the IP address(es) on the LAN behind the remote IPSec's router. |
| Delete | Click the **Edit** icon to modify the VPN policy.<br>Click the **Delete** icon to delete the VPN policy. |

# 18.3 The IPSec VPN Add/Edit Screen

Use these settings to add or edit VPN policies. Click the **Add New Connection** button in the **Security > VPN** screen to open this screen as shown next.

**Figure 129** Security > IPSec VPN: Add/Edit




This screen contains the following fields:

**Table 94** Security > IPSec VPN: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this to activate this VPN policy. |
| IPSec Connection Name | Enter the name of the VPN policy. |
| Remote IPSec Gateway Address | Enter the IP address of the remote IPSec router in the IKE SA. |
| Tunnel access from local IP addresses | Select **Single Address** to have only one local LAN IP address use the VPN tunnel. Select **Subnet** to specify local LAN IP addresses by their subnet mask. |

**Table 94** Security > IPSec VPN: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| IP Address for VPN | If **Single Address** is selected, enter a (static) IP address on the LAN behind your Device.<br>If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind your Device. Then enter the subnet mask to identify the network address. |
| IP Subnetmask | If **Subnet** is selected, enter the subnet mask to identify the network address. |
| Tunnel access from remote IP addresses | Select **Single Address** to have only one remote LAN IP address use the VPN tunnel. Select **Subnet** to specify remote LAN IP addresses by their subnet mask. |
| IP Address for VPN | If **Single Address** is selected, enter a (static) IP address on the LAN behind the remote IPSec's router.<br>If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind the remote IPSec's router. Then enter the subnet mask to identify the network address. |
| IP Subnetmask | If **Subnet** is selected, enter the subnet mask to identify the network address. |
| Protocol | Select which protocol you want to use in the IPSec SA. Choices are:<br>**AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Integraty Algorithm**.<br>**ESP** (RFC 2406) - provides encryption and the same services offered by **AH**, but its authentication is weaker. If you select **ESP**, you must select an **Encryption Agorithm** and **Integraty Algorithm**.<br>Both **AH** and **ESP** increase processing requirements and latency (delay). The Device and remote IPSec router must use the same active protocol. |
| Key Exchange Method | Select the key exchange method:<br>**Auto(IKE)** - Select this to use automatic IKE key management VPN connection policy.<br>**Manual** - Select this option to configure a VPN connection policy that uses a manual key instead of IKE key management. This may be useful if you have problems with IKE key management.<br>Note: Only use manual key as a temporary solution, because it is not as secure as a regular IPSec SA. |
| Authentication Method | Select **Pre-Shared Key** to use a pre-shared key for authentication, and type in your pre-shared key. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.<br>Select **Certificate (X.509)** to use a certificate for authentication. |
| Pre-Shared Key | Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation.<br>Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. |
| Local ID Type | Select **IP** to identify the Device by its IP address.<br>Select **E-mail** to identify this Device by an e-mail address.<br>Select **DNS** to identify this Device by a domain name.<br>Select **ASN1DN** (Abstract Syntax Notation one - Distinguished Name) to this Device by the subject field in a certificate. This is used only with certificate-based authentication. |

**Table 94** Security > IPSec VPN: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Local ID Content | When you select IP in the **Local ID Type** field, type the IP address of your computer in this field. If you configure this field to 0.0.0.0 or leave it blank, the Device automatically uses the **Pre-Shared Key** (refer to the **Pre-Shared Key** field description).<br><br>It is recommended that you type an IP address other than 0.0.0.0 in this field or use the **DNS** or **E-mail** type in the following situations.<br><br>• When there is a NAT router between the two IPSec routers.<br>• When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.<br><br>When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this Device in this field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. |
| Remote ID Type | Select **IP** to identify the remote IPSec router by its IP address.<br><br>Select **E-mail** to identify the remote IPSec router by an e-mail address.<br><br>Select **DNS** to identify the remote IPSec router by a domain name.<br><br>Select **ASN1DN** to identify the remote IPSec router by the subject field in a certificate. This is used only with certificate-based authentication. |
| Remote ID Content | The configuration of the remote content depends on the remote ID type.<br><br>For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to 0.0.0.0 or leave it blank, the Device will use the address in the **Remote IPSec Gateway Address** field (refer to the **Remote IPSec Gateway Address** field description).<br><br>For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.<br><br>It is recommended that you type an IP address other than 0.0.0.0 or use the **DNS** or **E-mail** ID type in the following situations:<br><br>• When there is a NAT router between the two IPSec routers.<br>• When you want the Device to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses. |
| Advanced IKE Settings | Click **more** to display advanced settings. Click **less** to display basic settings only. |
| NAT_Traversal | Select **Enable** if you want to set up a VPN tunnel when there are NAT routers between the Device and remote IPSec router. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward UDP port 500 packets to the remote IPSec router behind the NAT router. Otherwise, select **Disable**. |
| Phase 1 | |
| Mode | Select the negotiation mode to use to negotiate the IKE SA. Choices are:<br><br>**Main** - this encrypts the Device's and remote IPSec router's identities but takes more time to establish the IKE SA.<br><br>**Aggressive** - this is faster but does not encrypt the identities.<br><br>The Device and the remote IPSec router must use the same negotiation mode. |

**Table 94** Security > IPSec VPN: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Encryption Algorithm | Select which key size and encryption algorithm to use in the IKE SA. Choices are:<br>**DES** - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**AES** - **128** - a 128-bit key with the AES encryption algorithm<br>**AES** - **196** - a 196-bit key with the AES encryption algorithm<br>**AES** - **256** - a 256-bit key with the AES encryption algorithm<br>The Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput. |
| Integrity Algorithm | Select which hash algorithm to use to authenticate packet data. Choices are **MD5**, **SHA1**. **SHA** is generally considered stronger than **MD5**, but it is also slower. |
| Select Diffie-Hellman Group for Key Exchange | Select which Diffie-Hellman key group you want to use for encryption keys. Choices for number of bits in the random number are: 768, 1024, 1536, 2048, 3072, 4096.<br>The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. |
| Key Life Time | Define the length of time before an IPSec SA automatically renegotiates in this field.<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Phase 2 | |
| Encryption Algorithm | Select which key size and encryption algorithm to use in the IKE SA. Choices are:<br>**DES** - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**AES** - **128** - a 128-bit key with the AES encryption algorithm<br>**AES** - **192** - a 196-bit key with the AES encryption algorithm<br>**AES** - **256** - a 256-bit key with the AES encryption algorithm<br>Select **ESP_NULL** to set up a tunnel without encryption. When you select **ESP_NULL**, you do not enter an encryption key.<br>The Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput. |
| Integrity Algorithm | Select which hash algorithm to use to authenticate packet data. Choices are **MD5** and **SHA1**. **SHA** is generally considered stronger than **MD5**, but it is also slower. |

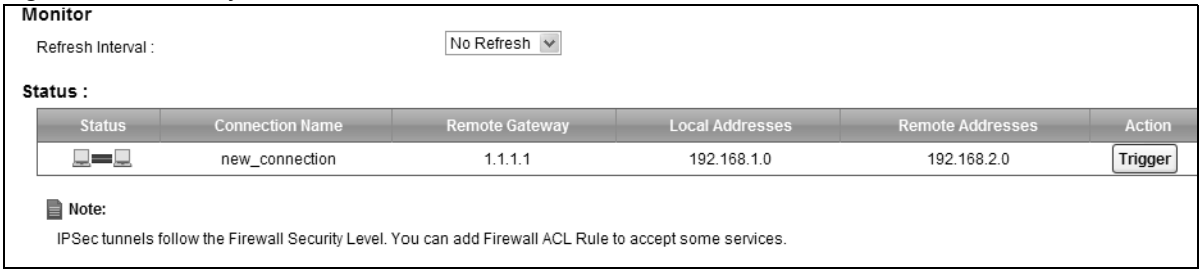
**Table 94** Security > IPSec VPN: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Perfect Forward Secrecy (PFS) | Select whether or not you want to enable Perfect Forward Secrecy (PFS)<br>PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. Choices are:<br>**None** - do not use any random number.<br>**768bit(DH Group1)** - use a 768-bit random number<br>**1024bit(DH Group2)** - use a 1024-bit random number<br>**1536bit(DH Group5)** - use a 1536-bit random number<br>**2048bit(DH Group14)** - use a 2048-bit random number<br>**3072bit(DH Group15)** - use a 3072-bit random number<br>**4096bit(DH Group16)** - use a 4096-bit random number |
| Key Life Time | Define the length of time before an IPSec SA automatically renegotiates in this field.<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| The following fields are available if you select Manual in the Key Exchange Method field. | |
| Encryption Algorithm | Select which key size and encryption algorithm to use in the IKE SA. Choices are:<br>**DES** - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**EPS_NULL** - no encryption key or algorithm |
| Encryption Key | This field is applicable when you select an Encryption Algorithm.<br>Enter the encryption key, which depends on the encryption algorithm.<br>**DES** - type a unique key 16 hexadecimal characters long<br>**3DES** - type a unique key 48 hexadecimal characters long |
| Authentication Algorithm | Select which hash algorithm to use to authenticate packet data. Choices are MD5, SHA1. SHA is generally considered stronger than MD5, but it is also slower. |
| Authentication Key | Enter the authentication key, which depends on the authentication algorithm.<br>**MD5** - type a unique key 32 hexadecimal characters long<br>**SHA1** - type a unique key 40 hexadecimal characters long |
| SPI | Type a unique SPI (Security Parameter Index) in hexadecimal characters.<br>The SPI is used to identify the Device during authentication.<br>The Device and remote IPSec router must use the same SPI. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 18.4 The IPSec VPN Monitor Screen

Use this screen to check your VPN tunnel's current status. You can also manually trigger a VPN tunnel to the remote network. Click **Security > IPSec VPN > Monitor** to open this screen as shown next.

**Figure 130** Security > IPSec VPN > Monitor




This screen contains the following fields:

**Table 95** Security > IPSec VPN > Monitor

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select how often you want the Device to update this screen. Select **No Refresh** to have the Device stop updating the screen. |
| Status | This displays a green line between two hosts if the VPN tunnel has been established successfully. Otherwise, it displays a red line in between. |
| Connection Name | This displays the name of the VPN policy. |
| Remote Gateway | This is the IP address of the remote IPSec router in the IKE SA. |
| Local Addresses | This displays the IP address(es) on the LAN behind your Device. |
| Remote Addresses | This displays the IP address(es) on the LAN behind the remote IPSec router. |
| Action | Click **Trigger** to establish a VPN connection with the remote network. |

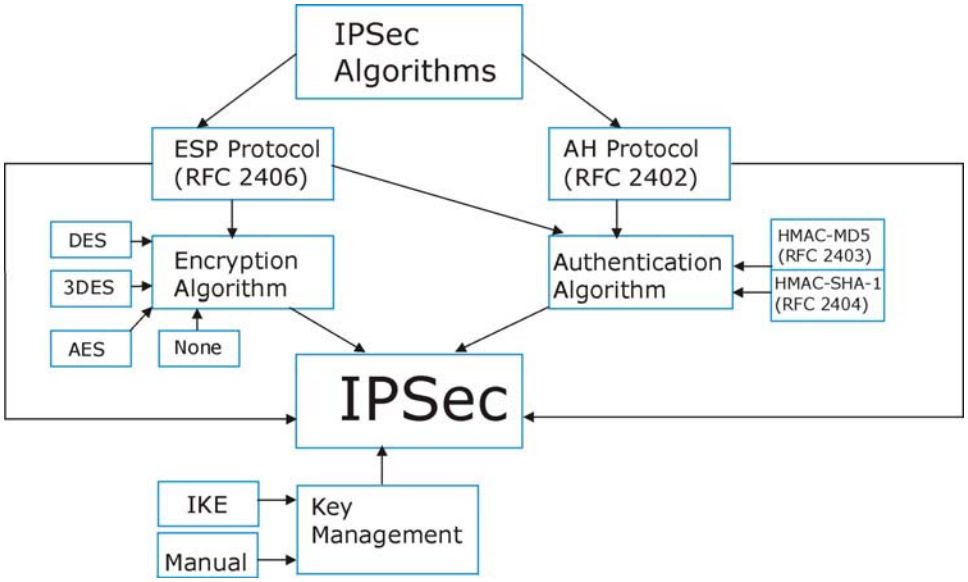
# 18.5 Technical Reference

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

## 18.5.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

**Figure 131** IPSec Architecture




### IPSec Algorithms

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

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

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

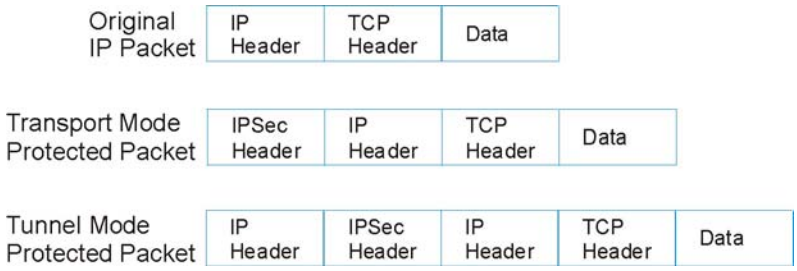
### Key Management

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

## 18.5.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the Device supports **Tunnel** mode only.

**Figure 132** Transport and Tunnel Mode IPSec Encapsulation



### Transport Mode

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

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

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

### Tunnel Mode

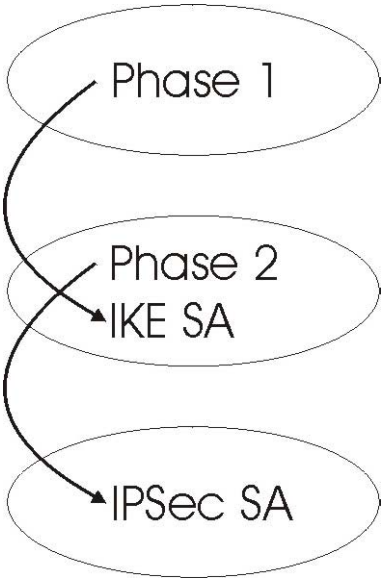
**Tunnel** mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel**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

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

## 18.5.3 IKE Phases

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

**Figure 133** Two Phases to Set Up the IPSec SA




In phase 1 you must:

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

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

## 18.5.4 Negotiation Mode

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

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

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

## 18.5.5 IPSec and NAT

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

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

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

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

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

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

**Table 96** VPN and NAT

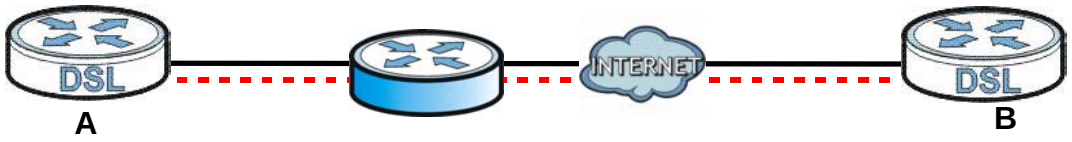
| SECURITY PROTOCOL | MODE | NAT |
|---|---|---|
| AH | Transport | N |
| AH | Tunnel | N |
| ESP | Transport | N |
| ESP | Tunnel | Y |

## 18.5.6 VPN, NAT, and NAT Traversal

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

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

**Figure 134** NAT Router Between IPSec Routers




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

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router **A**.

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

**Table 97** VPN and NAT

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

Y* - This is supported in the Device if you enable NAT traversal.

## 18.5.7 ID Type and Content

With aggressive negotiation mode (see Section 18.5.4 on page 221), the Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.

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

With main mode (see Section 18.5.4 on page 221), the ID type and content are encrypted to provide identity protection. In this case the Device can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The Device can distinguish up to 48 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and eight key groups when you configure a VPN rule (see Section 18.2 on page 211). The ID type and content act as an extra level of identification for incoming SAs.

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

**Table 98** Local ID Type and Content Fields

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

#### 18.5.7.1 ID Type and Content Examples

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

The two Devices in this example can complete negotiation and establish a VPN tunnel.

**Table 99** Matching ID Type and Content Configuration Example

| Device A | Device B |
|---|---|
| Local ID type: E-mail | Local ID type: IP |
| Local ID content: tom@yourcompany.com | Local ID content: 1.1.1.2 |
| Remote ID type: IP | Remote ID type: E-mail |
| Remote ID content: 1.1.1.2 | Remote ID content: tom@yourcompany.com |

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

**Table 100** Mismatching ID Type and Content Configuration Example

| DEVICE A | DEVICE B |
|---|---|
| Local ID type: IP | Local ID type: IP |
| Local ID content: 1.1.1.10 | Local ID content: 1.1.1.2 |
| Remote ID type: E-mail | Remote ID type: IP |
| Remote ID content: aa@yahoo.com | Remote ID content: 1.1.1.0 |

### 18.5.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 18.5.3 on page 220 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

### 18.5.9 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

# 19

# Log

## 19.1 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.

### 19.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 19.2 on page 226).
- Use the **Security Log** screen to see the security-related logs for the categories that you select (Section 19.3 on page 227).

### 19.1.2 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 101** 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. |

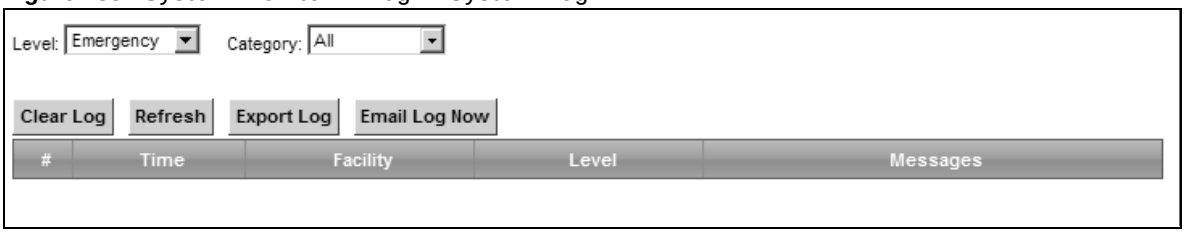
**Table 101** Syslog Severity Levels

| CODE | SEVERITY |
|---|---|
| 5 | Notice: There is a normal but significant condition on the system. |
| 6 | Informational: The syslog contains an informational message. |
| 7 | Debug: The message is intended for debug-level purposes. |

# 19.2 The System Log Screen

Use the **System Log** screen to see the system logs. Click **System Monitor > Log** to open the **System Log** screen.

**Figure 135** System Monitor > Log > System Log




The following table describes the fields in this screen.

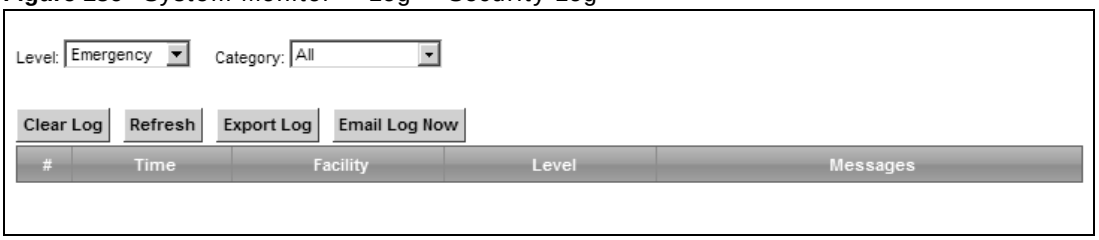
**Table 102** System Monitor > Log > System Log

| 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. |
| Category | Select the type of logs to display. |
| Clear Log | Click this to delete all the logs. |
| Refresh | Click this to renew the log screen. |
| Export Log | Click this to export the selected log(s). |
| Email Log Now | Click this to send the log file(s) to the E-mail address you specify in the **Maintenance > Log Setting** screen. |
| System Log | |
| # | This field is a sequential value and is not associated with a specific entry. |
| Time | This field displays the time the log was recorded. |
| Facility | The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Level | This field displays the severity level of the logs that the device is to send to this syslog server. |
| Messages | This field states the reason for the log. |

# 19.3 The Security Log Screen

Use the **Security Log** screen to see the security-related logs for the categories that you select. Click **System Monitor > Log > Security Log** to open the following screen.

**Figure 136** System Monitor > Log > Security Log




The following table describes the fields in this screen.

**Table 103** System Monitor > Log > Security 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. |
| Category | Select the type of logs to display. |
| Clear Log | Click this to delete all the logs. |
| Refresh | Click this to renew the log screen. |
| Export Log | Click this to export the selected log(s). |
| Email Log Now | Click this to send the log file(s) to the E-mail address you specify in the **Maintenance > Log Setting** screen. |
| # | This field is a sequential value and is not associated with a specific entry. |
| Time | This field displays the time the log was recorded. |
| Facility | The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Level | This field displays the severity level of the logs that the device is to send to this syslog server. |
| Messages | This field states the reason for the log. |

# 20

# Traffic Status

## 20.1 Overview

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

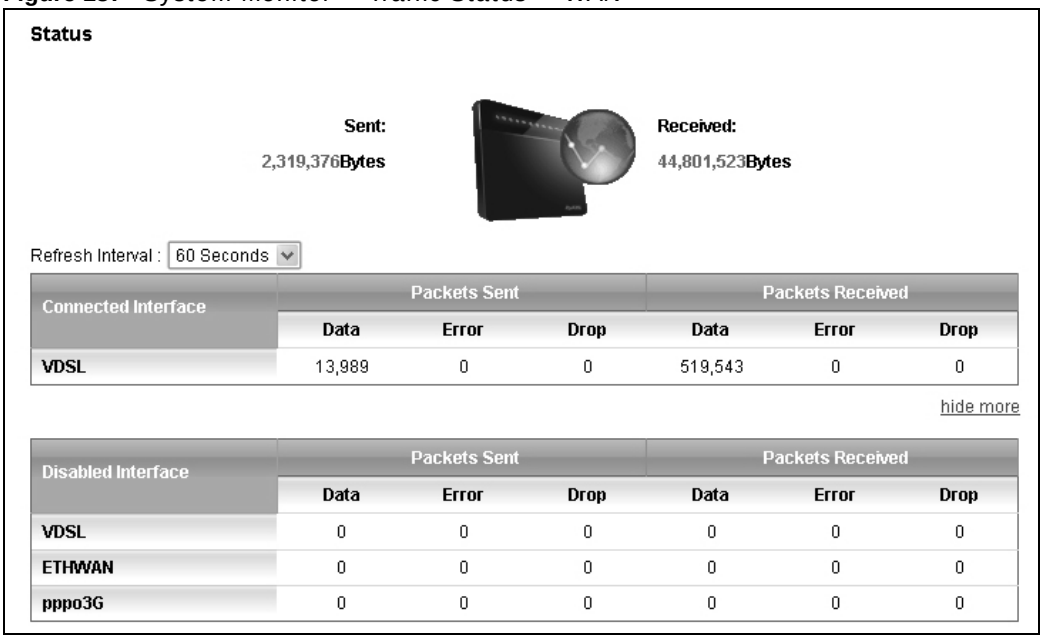
### 20.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 20.2 on page 229).
- Use the **LAN** screen to view the LAN traffic statistics (Section 20.3 on page 231).
- Use the **NAT** screen to view the NAT status of the Device's client(s) (Section 20.4 on page 232)

## 20.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. The figure in this screen shows the number of bytes received and sent on the Device.

**Figure 137** System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

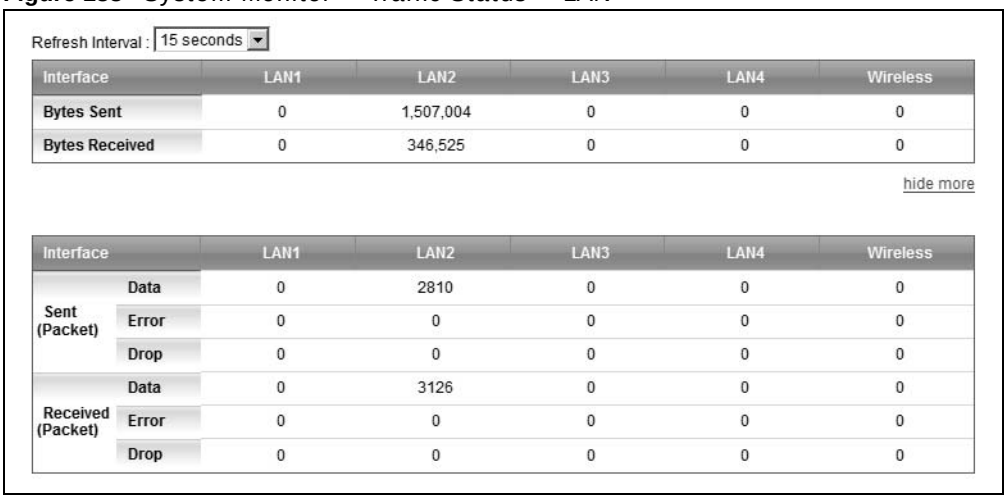
**Table 104** System Monitor > Traffic Status > WAN

| LABEL | DESCRIPTION |
|---|---|
| Connected Interface | This shows the name of the WAN interface that is currently connected. |
| 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. |
| more...hide more | Click **more...** to show more information. Click **hide more** to hide them. |
| Disabled Interface | This shows the name of the WAN interface that is currently disconnected. |
| 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. |

# 20.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. The figure in this screen shows the interface that is currently connected on the Device.

**Figure 138** System Monitor > Traffic Status > LAN




The following table describes the fields in this screen.

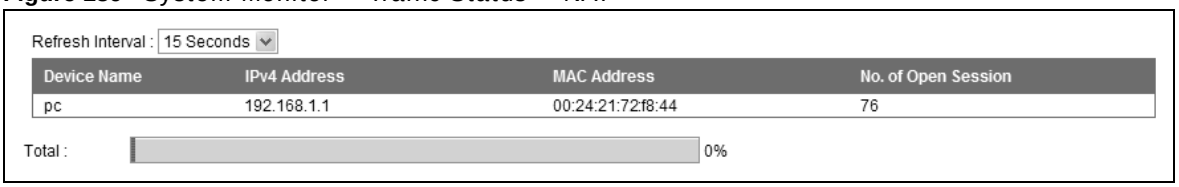
**Table 105** System Monitor > Traffic Status > LAN

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select how often you want the Device to update this screen. |
| 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. |
| more...hide more | Click **more...** to show more information. Click **hide more** to hide them. |
| Interface | This shows the LAN or WLAN interface. |
| Sent (Packets) | |
| 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 (Packets) | |
| 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. |

# 20.4 The NAT Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. The figure in this screen shows the NAT session statistics for hosts currently connected on the Device.

**Figure 139** System Monitor > Traffic Status > NAT




The following table describes the fields in this screen.

**Table 106** System Monitor > Traffic Status > NAT

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select how often you want the Device to update this screen. |
| Device Name | This displays the name of the connected host. |
| IPv4 Address | This displays the IPv4 IP address of the connected host. |
| MAC Address | This displays the MAC address of the connected host. |
| No. of Open Session | This displays the number of NAT sessions currently opened for the connected host. |
| Total | This displays what percentage of NAT sessions the Device can support is currently being used by all connected hosts. |

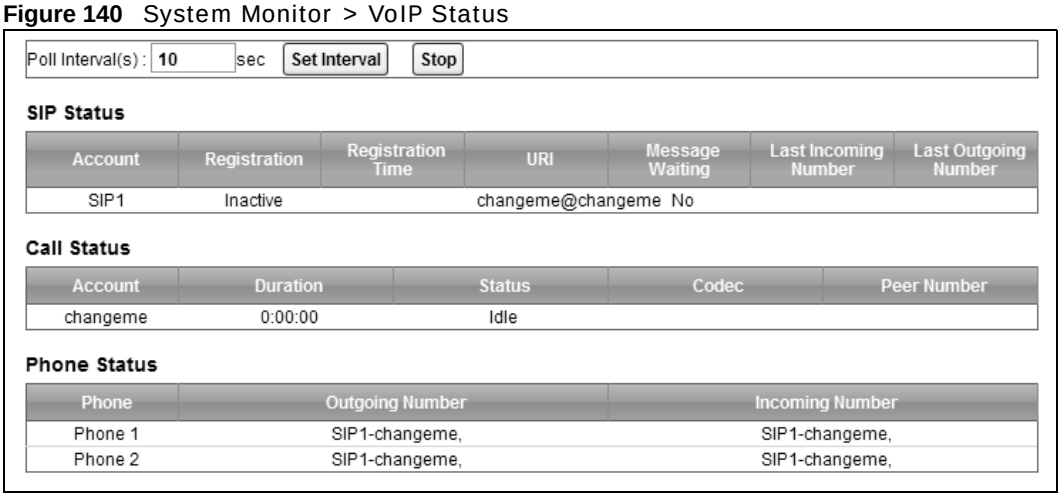
# 21

# VoIP Status

## 21.1 The VoIP Status Screen

Click **System Monitor > VoIP Status** to open the following screen. You can view the VoIP registration, current call status and phone numbers in this screen.

**Figure 140** System Monitor > VoIP Status




The following table describes the fields in this screen.

**Table 107** System Monitor > VoIP Status

| LABEL | DESCRIPTION |
|---|---|
| Poll Interval(s) | Enter the number of seconds the Device needs to wait before updating this screen and then click **Set Interval**. Click **Stop** to have the Device stop updating this screen. |
| SIP Status | |
| Account | This column displays each SIP account in the Device. |
| Registration | This field displays the current registration status of the SIP account. You can change this in the **Status** screen.<br>**Registered** - The SIP account is registered with a SIP server.<br>**Not Registered** - The last time the Device tried to register the SIP account with the SIP server, the attempt failed. The Device automatically tries to register the SIP account when you turn on the Device or when you activate it.<br>**Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Account**. |
| Registration Time | This field displays the last time the Device successfully registered the SIP account. The field is blank if the Device has never successfully registered this account. |
| URI | This field displays the account number and service domain of the SIP account. You can change these in the **VoIP > SIP** screens. |

**Table 107** System Monitor > VoIP Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| Message Waiting | This field indicates whether or not there are any messages waiting for the SIP account. |
| Last Incoming Number | This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account. |
| Last Outgoing Number | This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number. |
| Call Status | |
| Account | This column displays each SIP account in the Device. |
| Duration | This field displays how long the current call has lasted. |
| Status | This field displays the current state of the phone call.<br>**Idle** - There are no current VoIP calls, incoming calls or outgoing calls being made.<br>**Dial** - The callee's phone is ringing.<br>**Ring** - The phone is ringing for an incoming VoIP call.<br>**Process** - There is a VoIP call in progress.<br>**DISC** - The callee's line is busy, the callee hung up or your phone was left off the hook. |
| Codec | This field displays what voice codec is being used for a current VoIP call through a phone port. |
| Peer Number | This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port. |
| Phone Status | |
| Phone | This field displays the name of a phone port on the Device. |
| Outgoing Number | This field displays the SIP number that you use to make calls on this phone port. |
| Incoming Number | This field displays the SIP number that you use to receive calls on this phone port. |

# 22

# ARP Table

## 22.1 Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

### 22.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

## 22.2 ARP Table Screen

Use the ARP table to view IP-to-MAC address mapping(s). To open this screen, click **System Monitor** > **ARP Table**.

**Figure 141** System Monitor > ARP Table

**IPv4 ARP Table**

| # | IPv4 Address | MAC Address | Device |
|---|---|---|---|
| 1 | 192.168.1.74 | 00:02:e3:57:e2:1c | LAN |
| 2 | 192.168.1.2 | 00:24:21:7e:f8:44 | LAN |

**IPv6 Neighbor Table**

| # | IPv6 Address | MAC Address | Device |
|---|---|---|---|

The following table describes the labels in this screen.

**Table 108** System Monitor > ARP Table

| LABEL | DESCRIPTION |
|---|---|
| # | This is the ARP table entry number. |
| IPv4/IPv6 Address | This is the learned IPv4 or IPv6 IP address of a device connected to a port. |
| MAC Address | This is the MAC address of the device with the listed IP address. |
| Device | This is the type of interface used by the device. You can click on the device type to go to its configuration screen. |

# 23

# Routing Table

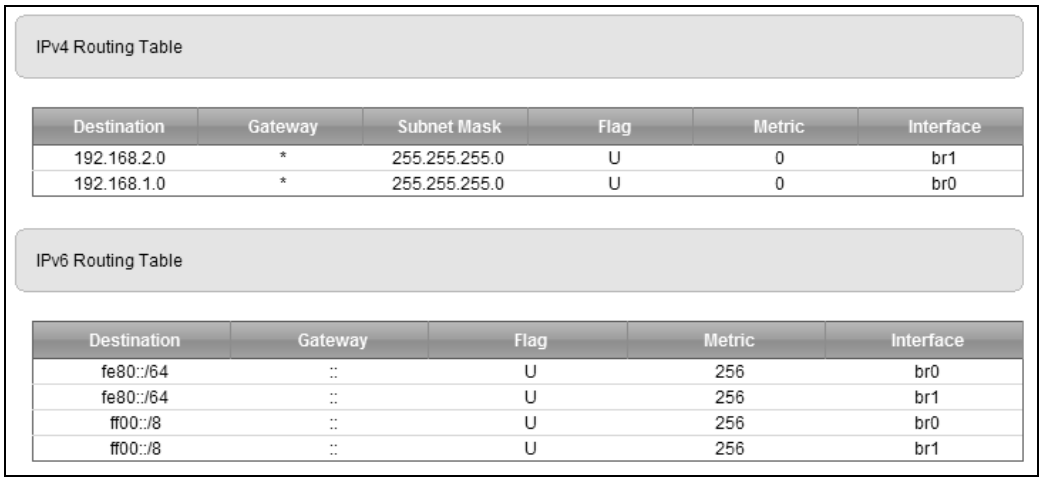
## 23.1 Overview

Routing is based on the destination address only and the Device takes the shortest path to forward a packet.

## 23.2 The Routing Table Screen

Click **System Monitor** > **Routing Table** to open the following screen.

**Figure 142** System Monitor > Routing Table




The following table describes the labels in this screen.

**Table 109** System Monitor > Routing Table

| LABEL | DESCRIPTION |
|---|---|
| IPv4/IPv6 Routing Table | |
| Destination | This indicates the destination IPv4 address or IPv6 address and prefix of this route. |
| Gateway | This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic. |
| Subnet Mask | This indicates the destination subnet mask of the IPv4 route. |

**Table 109** System Monitor > Routing Table (continued)

| LABEL | DESCRIPTION |
|---|---|
| Flag | This indicates the route status.<br>**U-Up:** The route is up.<br>**!-Reject:** The route is blocked and will force a route lookup to fail.<br>**G-Gateway:** The route uses a gateway to forward traffic.<br>**H-Host:** The target of the route is a host.<br>**R-Reinstate:** The route is reinstated for dynamic routing.<br>**D-Dynamic (redirect):** The route is dynamically installed by a routing daemon or redirect.<br>**M-Modified (redirect):** The route is modified from a routing daemon or redirect. |
| Metric | The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost". |
| Service | This indicates the name of the service used to forward the route. |
| Interface | This indicates the name of the interface through which the route is forwarded.<br>**brx** indicates a LAN interface where x can be 0~3 to represent LAN1 to LAN4 respectively.<br>**ptm0** indicates a WAN interface using IPoE or in bridge mode.<br>**ppp0** indicates a WAN interface using PPPoE. |

# 24

# IGMP/MLD Status

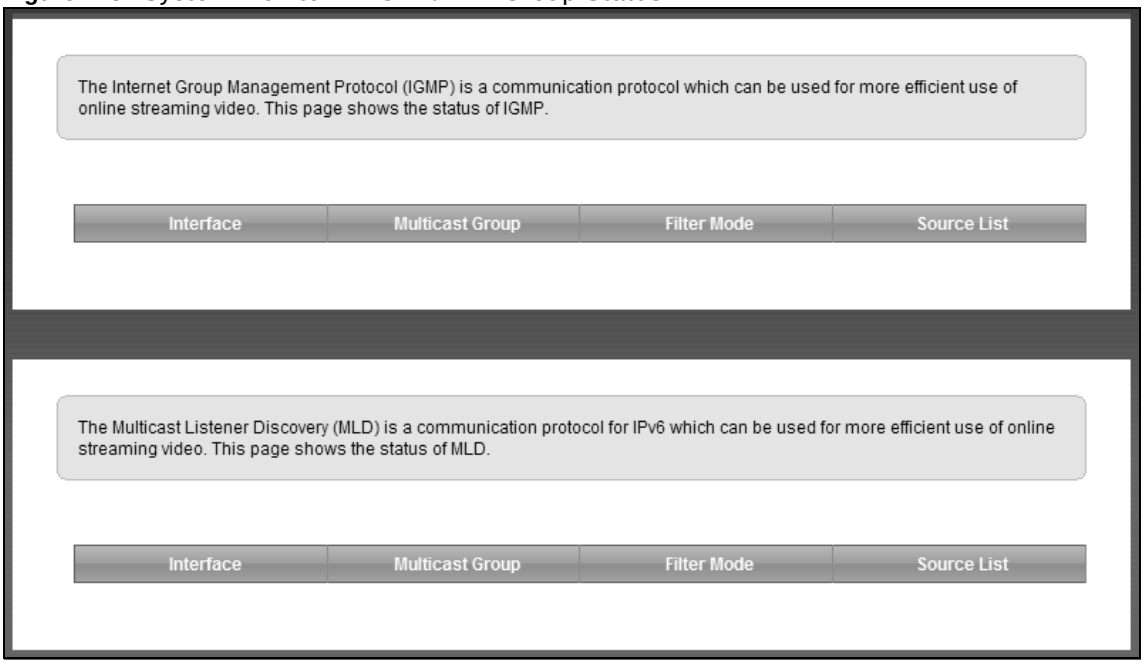
## 24.1 Overview

Use the **IGMP Status** screens to look at IGMP/MLD group status and traffic statistics.

## 24.2 The IGMP/MLD Group Status Screen

Use this screen to look at the current list of multicast groups the Device has joined and which ports have joined it. To open this screen, click **System Monitor > IGMP/MLD Group Status**.

**Figure 143** System Monitor > IGMP/MLD Group Status




The following table describes the labels in this screen.

**Table 110** System Monitor > IGMP/MLD Group Status

| LABEL | DESCRIPTION |
|---|---|
| Interface | This field displays the name of an interface on the Device that belongs to an IGMP or MLD multicast group. |
| Multicast Group | This field displays the name of the IGMP or MLD multicast group to which the interface belongs. |

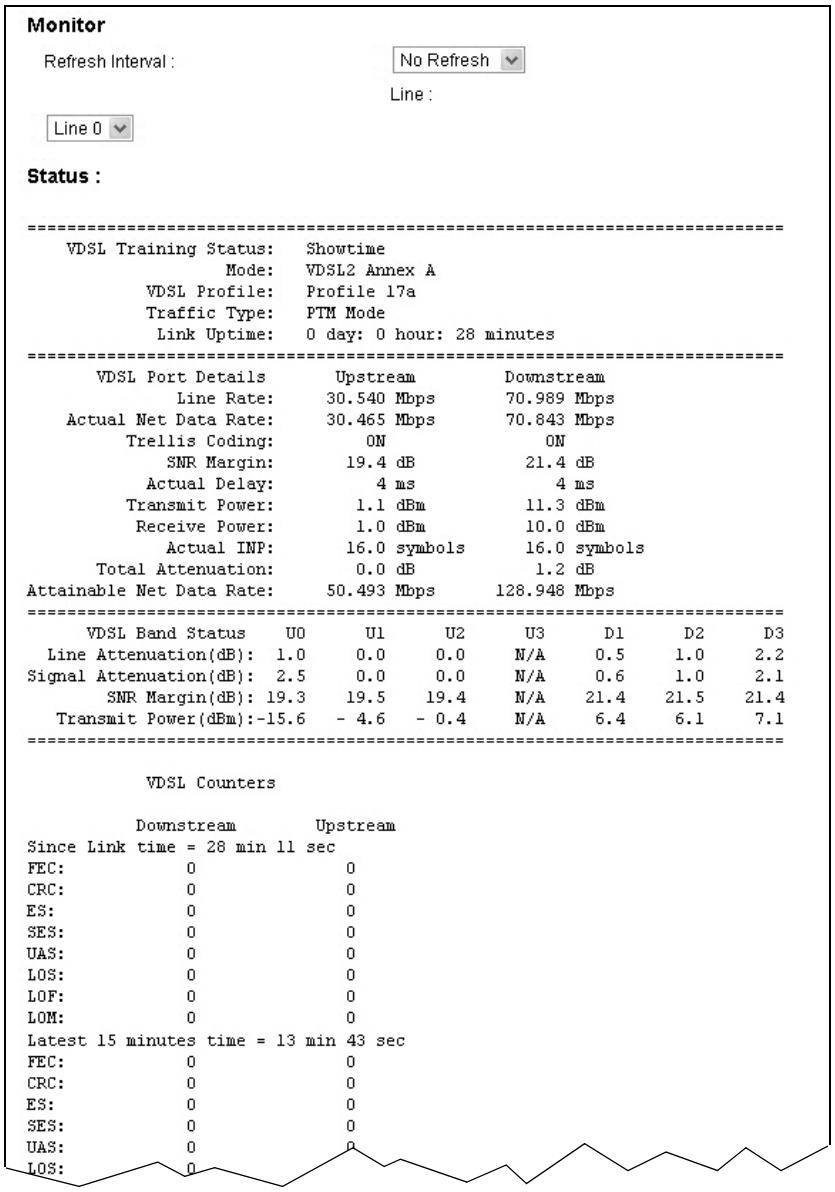
**Table 110** System Monitor > IGMP/MLD Group Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| Filter Mode | **INCLUDE** means that only the IP addresses in the **Source List** get to receive the multicast group's traffic.<br>**EXCLUDE** means that the IP addresses in the **Source List** are not allowed to receive the multicast group's traffic but other IP addresses can. |
| Source List | This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode. |

## 25.1 The xDSL Statistics Screen

Use this screen to view detailed DSL statistics. Click **System Monitor > xDSL Statistics** to open the following screen.

**Figure 144** System Monitor > xDSL Statistics



**Monitor**

Refresh Interval : No Refresh

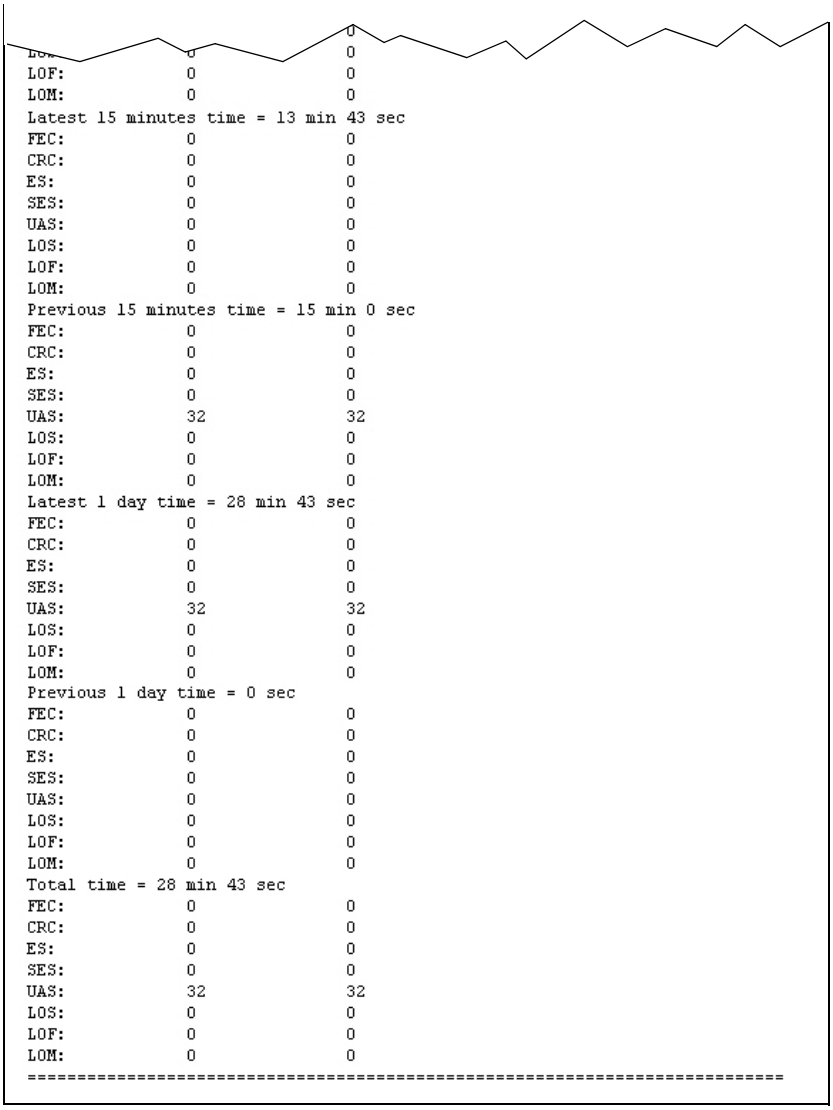
Line : Line 0

**Status :**

```
================================================================================
    VDSL Training Status:   Showtime
                    Mode:   VDSL2 Annex A
            VDSL Profile:   Profile 17a
            Traffic Type:   PTM Mode
             Link Uptime:   0 day: 0 hour: 28 minutes
================================================================================
       VDSL Port Details       Upstream          Downstream
                Line Rate:     30.540 Mbps       70.989 Mbps
    Actual Net Data Rate:      30.465 Mbps       70.843 Mbps
          Trellis Coding:          ON                ON
              SNR Margin:        19.4 dB           21.4 dB
            Actual Delay:           4 ms              4 ms
          Transmit Power:         1.1 dBm           11.3 dBm
           Receive Power:         1.0 dBm           10.0 dBm
              Actual INP:        16.0 symbols      16.0 symbols
       Total Attenuation:         0.0 dB            1.2 dB
Attainable Net Data Rate:      50.493 Mbps      128.948 Mbps
================================================================================
      VDSL Band Status    U0      U1      U2      U3      D1      D2      D3
  Line Attenuation(dB):  1.0     0.0     0.0     N/A     0.5     1.0     2.2
Signal Attenuation(dB):  2.5     0.0     0.0     N/A     0.6     1.0     2.1
       SNR Margin(dB): 19.3    19.5    19.4     N/A    21.4    21.5    21.4
   Transmit Power(dBm):-15.6   - 4.6   - 0.4     N/A     6.4     6.1     7.1
================================================================================

            VDSL Counters

           Downstream        Upstream
Since Link time = 28 min 11 sec
FEC:              0                 0
CRC:              0                 0
ES:               0                 0
SES:              0                 0
UAS:              0                 0
LOS:              0                 0
LOF:              0                 0
LOM:              0                 0
Latest 15 minutes time = 13 min 43 sec
FEC:              0                 0
CRC:              0                 0
ES:               0                 0
SES:              0                 0
UAS:              0                 0
LOS:              0
```




The following table describes the labels in this screen.

**Table 111** Status > xDSL Statistics

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select the time interval for refreshing statistics. |
| Line | Select which DSL line's statistics you want to display. |
| xDSL Training Status | This displays the current state of setting up the DSL connection. |
| Mode | This displays the ITU standard used for this connection. |
| Traffic Type | This displays the type of traffic the DSL port is sending and receiving. **Inactive** displays if the DSL port is not currently sending or receiving traffic. |
| Link Uptime | This displays how long the port has been running (or connected) since the last time it was started. |
| xDSL Port Details | |
| Upstream | These are the statistics for the traffic direction going out from the port to the service provider. |

**Table 111** Status > xDSL Statistics (continued)

| LABEL | DESCRIPTION |
|---|---|
| Downstream | These are the statistics for the traffic direction coming into the port from the service provider. |
| Line Rate | These are the data transfer rates at which the port is sending and receiving data. |
| Actual Net Data Rate | These are the rates at which the port is sending and receiving the payload data without transport layer protocol headers and traffic. |
| Trellis Coding | This displays whether or not the port is using Trellis coding for traffic it is sending and receiving. Trellis coding helps to reduce the noise in ADSL transmissions. Trellis may reduce throughput but it makes the connection more stable. |
| SNR Margin | This is the upstream and downstream Signal-to-Noise Ratio margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the system still being able to meet its transmission targets. |
| Actual Delay | This is the upstream and downstream interleave delay. It is the wait (in milliseconds) that determines the size of a single block of data to be interleaved (assembled) and then transmitted. Interleave delay is used when transmission error correction (Reed- Solomon) is necessary due to a less than ideal telephone line. The bigger the delay, the bigger the data block size, allowing better error correction to be performed. |
| Transmit Power | This is the upstream and downstream far end actual aggregate transmit power (in dBm).<br><br>Upstream is how much power the port is using to transmit to the service provider. Downstream is how much port the service provider is using to transmit to the port. |
| Receive Power | Upstream is how much power the service provider is receiving from the port. Downstream is how much power the port is receiving from the service provider. |
| Actual INP | Sudden spikes in the line's level of external noise (impulse noise) can cause errors and result in lost packets. This could especially impact the quality of multimedia traffic such as voice or video. Impulse noise protection (INP) provides a buffer to allow for correction of errors caused by error correction to deal with this. The number of DMT (Discrete Multi-Tone) symbols shows the level of impulse noise protection for the upstream and downstream traffic. A higher symbol value provides higher error correction capability, but it causes overhead and higher delay which may increase error rates in received multimedia data. |
| Total Attenuation | This is the upstream and downstream line attenuation, measured in decibels (dB). This attenuation is the difference between the power transmitted at the near-end and the power received at the far-end. Attenuation is affected by the channel characteristics (wire gauge, quality, condition and length of the physical line). |
| Attainable Net Data Rate | These are the highest theoretically possible transfer rates at which the port could send and receive payload data without transport layer protocol headers and traffic. |
| xDSL Counters | |
| Downstream | These are the statistics for the traffic direction coming into the port from the service provider. |
| Upstream | These are the statistics for the traffic direction going out from the port to the service provider. |
| FEC | This is the number of Far End Corrected blocks. |
| CRC | This is the number of Cyclic Redundancy Checks. |
| ES | This is the number of Errored Seconds meaning the number of seconds containing at least one errored block or at least one defect. |
| SES | This is the number of Severely Errored Seconds meaning the number of seconds containing 30% or more errored blocks or at least one defect. This is a subset of ES. |
| UAS | This is the number of UnAvailable Seconds. |
| LOS | This is the number of Loss Of Signal seconds. |

**Table 111** Status > xDSL Statistics (continued)

| LABEL | DESCRIPTION |
|---|---|
| LOF | This is the number of Loss Of Frame seconds. |
| LOM | This is the number of Loss of Margin seconds. |

# 26

# 3G Statistics

## 26.1 Overview

Use the **3G Statistics** screens to look at 3G Internet connection status.

## 26.2 The 3G Statistics Screen

To open this screen, click **System Monitor > 3G Statistics**. The 3G status is available on this screen only when you insert a compatible 3G dongle in a USB port on the Device.

**Figure 145** System Monitor > 3G Statistics


The following table describes the labels in this screen.

**Table 112** System Monitor > 3G Statistics

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select how often you want the Device to update this screen. Select **No Refresh** to stop refreshing. |
| 3G Status | This field displays the status of the 3G Internet connection. This field can display:<br>**GSM** - Global System for Mobile Communications, 2G<br>**GPRS** - General Packet Radio Service, 2.5G<br>**EDGE** - Enhanced Data rates for GSM Evolution, 2.75G<br>**WCDMA** - Wideband Code Division Multiple Access, 3G<br>**HSDPA** - High-Speed Downlink Packet Access, 3.5G<br>**HSUPA** - High-Speed Uplink Packet Access, 3.75G<br>**HSPA** - HSDPA+HSUPA, 3.75G |

**Table 112** System Monitor > 3G Statistics (continued)

| LABEL | DESCRIPTION |
|---|---|
| Service Provider | This field displays the name of the service provider. |
| Signal Strength | This field displays the strength of the signal in dBm. |
| Connection Uptime | This field displays the time the connection has been up. |
| 3G Card Manufacturer | This field displays the manufacturer of the 3G card. |
| 3G Card Model | This field displays the model name of the 3G card. |
| 3G Card F/W Version | This field displays the firmware version of the 3G card. |
| SIM Card IMSI | The International Mobile Subscriber Identity or IMSI is a unique identification number associated with all cellular networks. This number is provisioned in the SIM card. |

# 27

# User Account

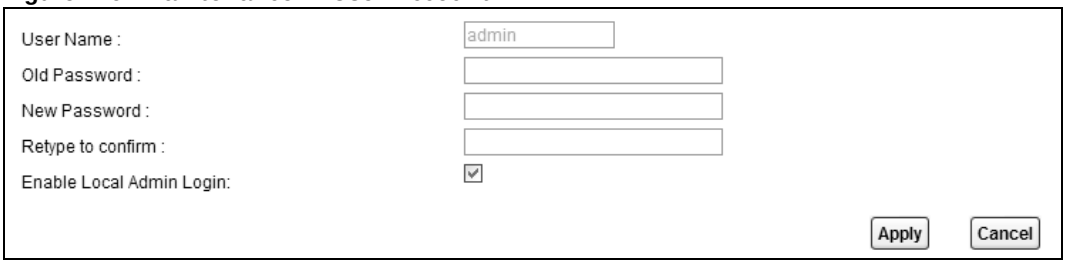
## 27.1 Overview

In the **Users Account** screen, you can change the password of the “admin” user account that you used to log in the Device.

## 27.2 The User Account Screen

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

**Figure 146** Maintenance > User Account




The following table describes the labels in this screen.

**Table 113** Maintenance > User Account

| LABEL | DESCRIPTION |
|---|---|
| User Name | This field displays the name of the account that you used to log in the system. |
| 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 (6 to 256 characters). At least one numeric character and one letter are required. 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 force LAN and wireless LAN users to pass the user authentication before they can access the Web Configurator. Clear this to let any LAN and wireless LAN users access the Web Configurator directly without user authentication. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 28

# Remote Management

## 28.1 Overview

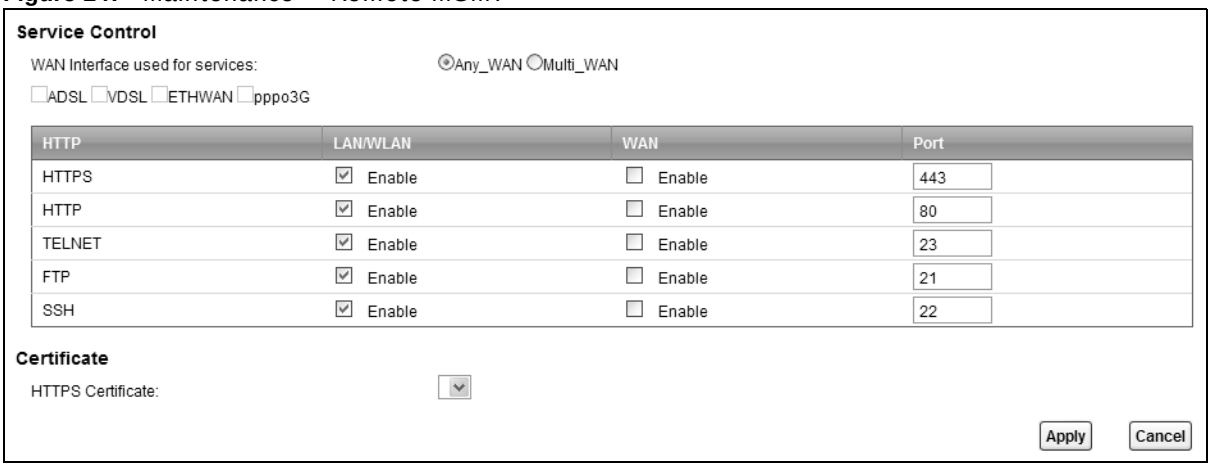
Remote management controls through which interface(s), which services can access the Device.

Note: The Device is managed using the Web Configurator.

## 28.2 The Remote MGMT Screen

Use this screen to configure through which interface(s), which services can access the Device. You can also specify the port numbers the services must use to connect to the Device. Click **Maintenance > Remote MGMT** to open the following screen.

**Figure 147** Maintenance > Remote MGMT




The following table describes the fields in this screen.

**Table 114** Maintenance > Remote MGMT

| LABEL | DESCRIPTION |
|---|---|
| WAN Interface used for services | Select **Any WAN** to have the Device automatically activate the remote management service when any WAN connection is up.<br>Select **Multi WAN** and then select one or more WAN connections to have the Device activate the remote management service when the selected WAN connections are up. |
| HTTP | This is the service you may use to access the Device. |
| LAN/WLAN | Select the **Enable** check box for the corresponding services that you want to allow access to the Device from the LAN/WLAN. |
| WAN | Select the **Enable** check box for the corresponding services that you want to allow access to the Device from the WAN. |

**Table 114** Maintenance > Remote MGMT (continued)

| LABEL | DESCRIPTION |
|---|---|
| Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Certificate | |
| HTTPS Certificate | Select a certificate the HTTPS server (the Device) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **Certificates** screen. |
| Apply | Click **Apply** to save your changes back to the Device. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 28.3 The Trust Domain Screen

Use this screen to view a list of public IP addresses which are allowed to access the Device through the services configured in the **Maintenance > Remote MGMT** screen. Click **Maintenance > Remote MGMT > Turst Domain** to open the following screen.

Note: If this list is empty, all public IP addresses can access the Device from the WAN through the specified services.

**Figure 148** Maintenance > Remote MGMT > Trust Domain


The following table describes the fields in this screen.

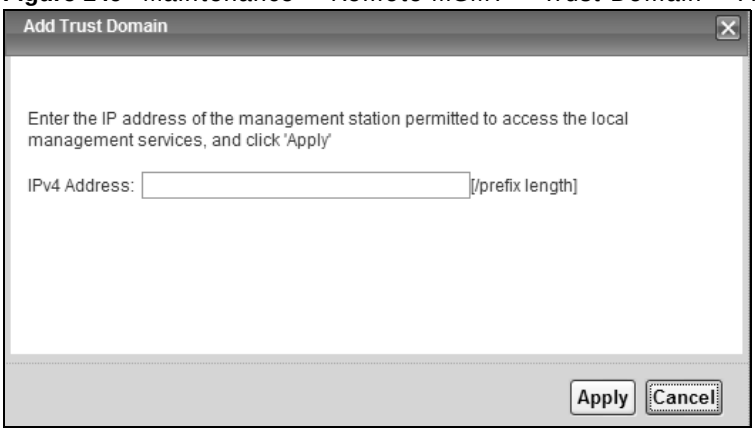
**Table 115** Maintenance > Remote MGMT > Trust Domain

| LABEL | DESCRIPTION |
|---|---|
| Add Trust Domain | Click this to add a trusted host IP address. |
| IPv4 Address | This field shows a trusted host IP address. |
| Delete | Click the **Delete** icon to remove the trust IP address. |

# 28.4 The Add Trust Domain Screen

Use this screen to configure a public IP address which is allowed to access the Device. Click the **Add Trust Domain** button in the **Maintenance > Remote MGMT > Turst Domain** screen to open the following screen.

**Figure 149** Maintenance > Remote MGMT > Trust Domain > Add Trust Domain




The following table describes the fields in this screen.

**Table 116** Maintenance > Remote MGMT > Trust Domain > Add Trust Domain

| LABEL | DESCRIPTION |
|---|---|
| IPv4 Address | Enter a public IPv4 IP address which is allowed to access the service on the Device from the WAN. |
| Apply | Click **Apply** to save your changes back to the Device. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 29

# TR-064

## 29.1 Overview

This chapter explains how to configure the Device's TR-064 auto-configuration settings.

## 29.2 The TR-064 Screen

TR-064 is a LAN-Side DSL CPE Configuration protocol defined by the DSL Forum. TR-064 is built on top of UPnP. It allows the users to use a TR-064 compliant CPE management application on their computers from the LAN to discover the CPE and configure user-specific parameters, such as the username and password.

Click **Maintenance > TR-064** to open the following screen.

**Figure 150** Maintenance > TR-064


The following table describes the fields in this screen.

**Table 117** Maintenance > TR-064

| LABEL | DESCRIPTION |
|---|---|
| State | Select **Enable** to activate management via TR-064 on the LAN. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 30

# SNMP

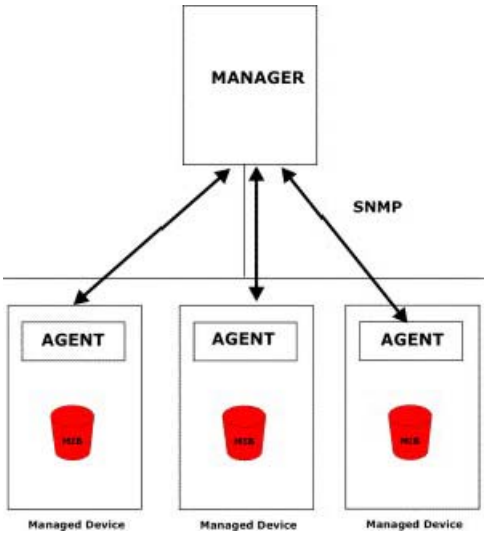
## 30.1 Overview

This chapter explains how to configure the SNMP settings on the Device.

## 30.2 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 151** 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

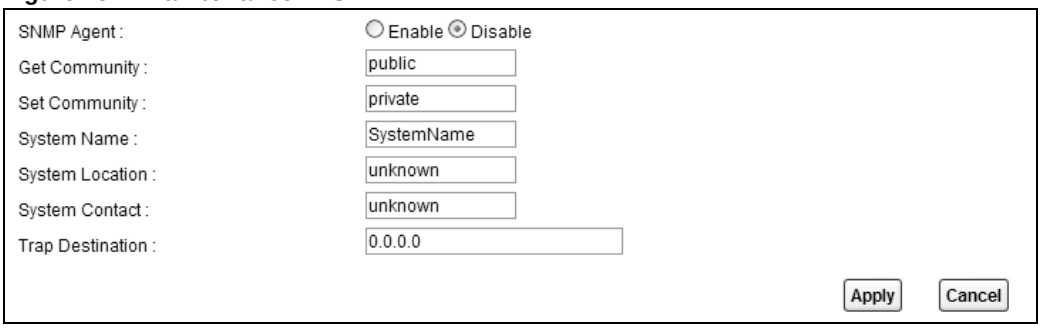
managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

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

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

Click **Maintenance > SNMP** to open the following screen. Use this screen to configure the Device SNMP settings.

**Figure 152** Maintenance > SNMP




The following table describes the fields in this screen.

**Table 118** Maintenance > SNMP

| LABEL | DESCRIPTION |
|---|---|
| SNMP Agent | Select **Enable** to let the Device act as an SNMP agent, which allows a manager station to manage and monitor the Device through the network. Select **Disable** to turn this feature off. |
| Get Community | Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. |
| Set Community | Enter the **Set community**, which is the password for incoming Set requests from the management station. |
| System Name | Enter the SNMP system name. |
| System Location | Enter the SNMP system location. |
| System Contact | Enter the SNMP system contact. |
| Trap Destination | Type the IP address of the station to send your SNMP traps to. |
| Apply | Click this to save your changes back to the Device. |
| Cancel | Click this to restore your previously saved settings. |

# 31

# Time Settings

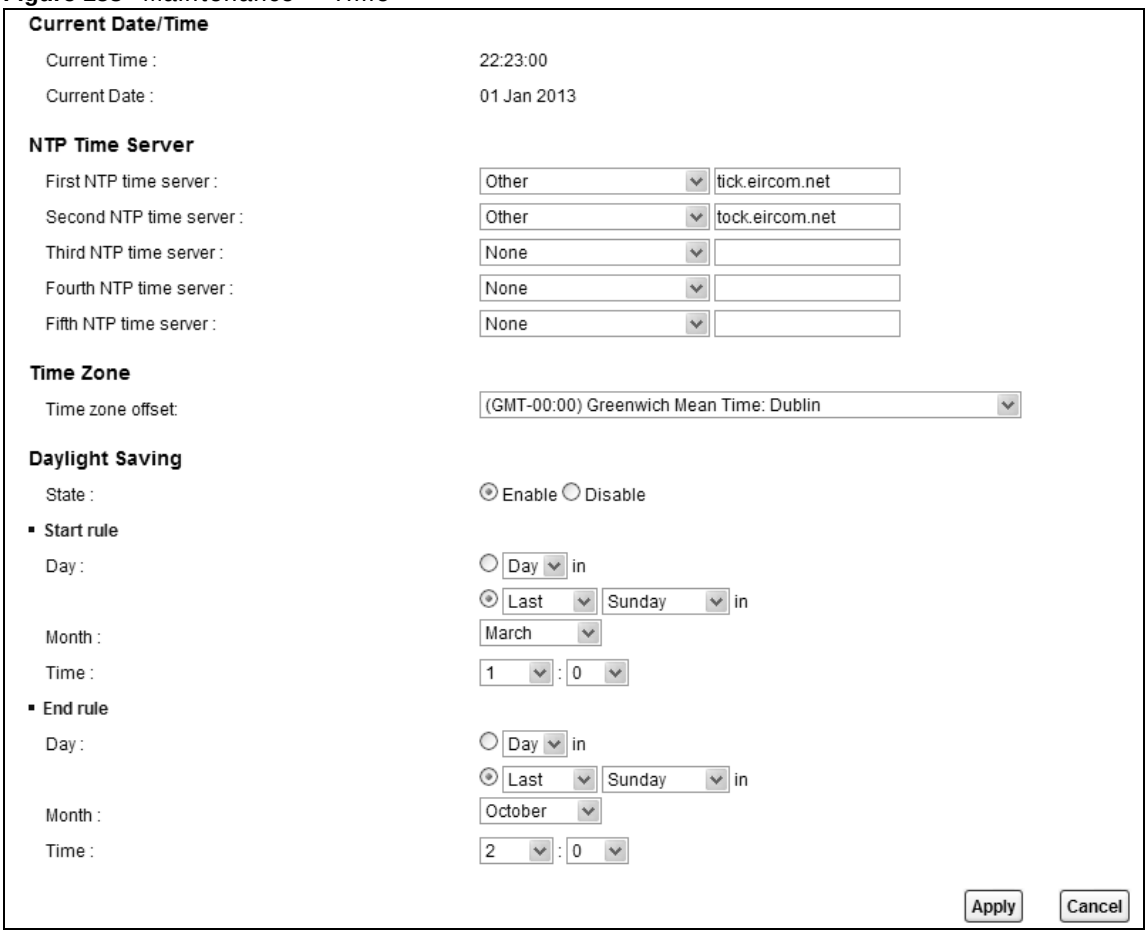
## 31.1 Overview

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

## 31.2 The Time Screen

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

**Figure 153** Maintenance > Time



The following table describes the fields in this screen.

**Table 119** Maintenance > Time

| LABEL | DESCRIPTION |
|---|---|
| Current Date/Time | |
| Current Time | This field displays the time of your Device.<br>Each time you reload this page, the Device synchronizes the time with the time server. |
| Current Date | This field displays the date of your Device.<br>Each time you reload this page, the Device synchronizes the date with the time server. |
| NTP Time Server | |
| First ~ Fifth NTP time server | Select an NTP time server from the drop-down list box.<br>Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server.<br>Select **None** if you don't want to configure the time server.<br>Check with your ISP/network administrator if you are unsure of this information. |
| Time Zone | |
| Time zone offset | Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). |
| Daylight Saving | Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. |
| State | Select **Enable** if you use Daylight Saving Time. |
| Start rule: | Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples:<br>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, set the day to **Second**, **Sunday**, the month to **March** and the time to **2** in the **Hour** field.<br>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 set the day to **Last**, **Sunday** and the month to **March**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| End rule | Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples:<br>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 set the day to **First**, **Sunday**, the month to **November** and the time to **2** in the **Hour** field.<br>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 set the day to **Last**, **Sunday**, and the month to **October**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |

**Table 119** Maintenance > Time (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 32

# E-mail Notification

## 32.1 Overview

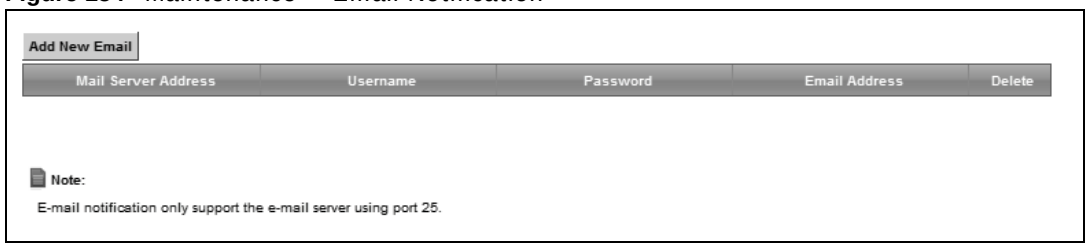
A mail server is an application or a computer that runs such an application to receive, forward and deliver e-mail messages.

To have the Device send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

## 32.2 The Email Notification Screen

Click **Maintenance > Email Notification** to open the **Email Notification** screen. Use this screen to view, remove and add mail server information on the Device.

**Figure 154** Maintenance > Email Notification




The following table describes the labels in this screen.

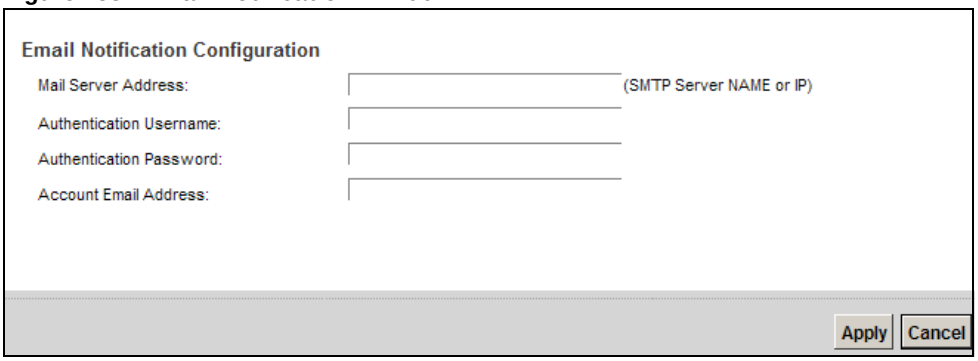
**Table 120** Maintenance > Email Notification

| LABEL | DESCRIPTION |
|---|---|
| Add New Email | Click this button to create a new entry. |
| Mail Server Address | This field displays the server name or the IP address of the mail server. |
| Username | This field displays the user name of the sender's mail account. |
| Password | This field displays the password of the sender's mail account. |
| Email Address | This field displays the e-mail address that you want to be in the from/sender line of the e-mail that the Device sends. |
| Delete | Click this button to delete the selected entry(ies). |

## 32.2.1 Email Notification Edit

Click the **Add** button in the **Email Notification** screen. Use this screen to configure the required information for sending e-mail via a mail server.

**Figure 155** Email Notification > Add




The following table describes the labels in this screen.

**Table 121** Email Notification > Add

| LABEL | DESCRIPTION |
|---|---|
| Mail Server Address | Enter the server name or the IP address of the mail server for the e-mail address specified in the **Account Email Address** field.<br>If this field is left blank, reports, logs or notifications will not be sent via e-mail. |
| Authentication Username | Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the **Account Email Address** field. |
| Authentication Password | Enter the password associated with the user name above. |
| Account Email Address | Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the Device sends.<br>If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well. |
| Apply | Click this button to save your changes and return to the previous screen. |
| Cancel | Click this button to begin configuring this screen afresh. |

# 33

# Log Setting

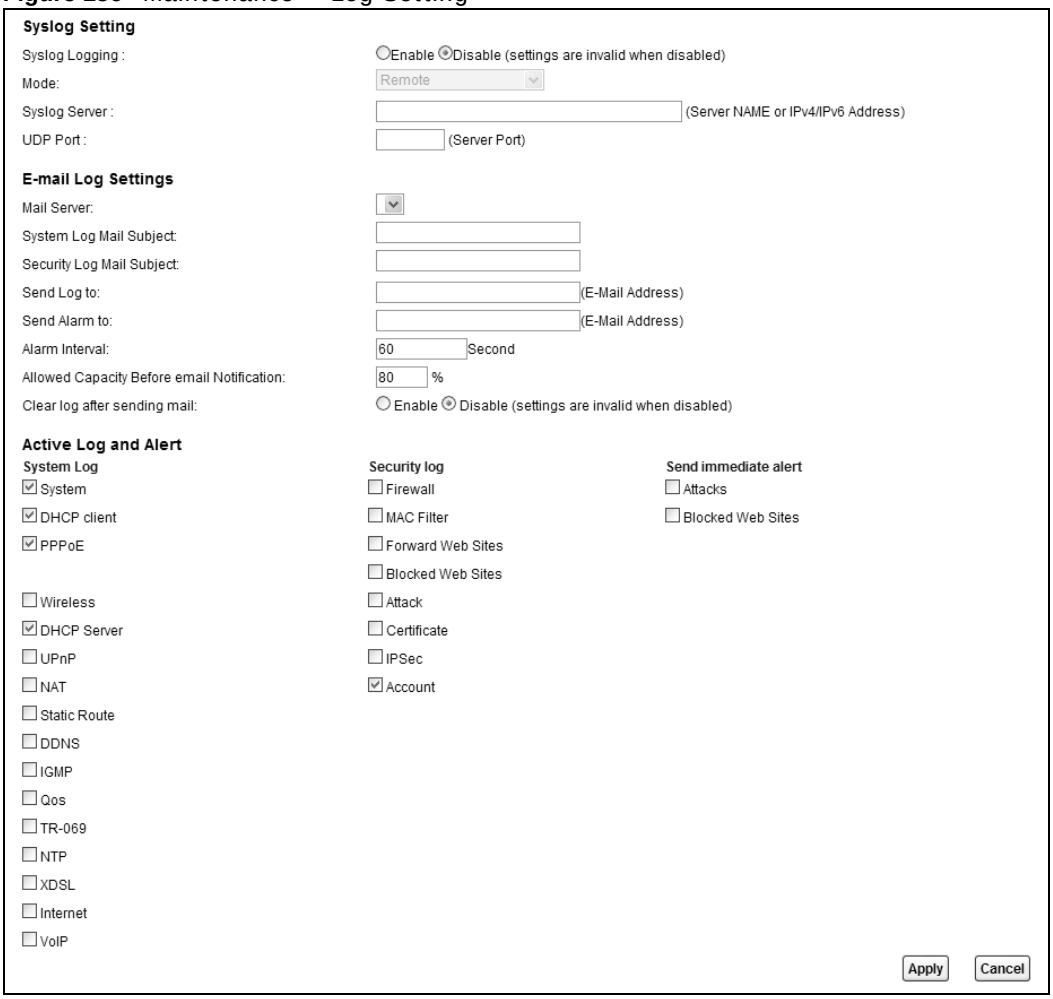
## 33.1 Overview

You can configure where the Device sends logs and which logs and/or immediate alerts the Device records in the **Log Setting** screen.

## 33.2 The Log Settings Screen

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

**Figure 156** Maintenance > Log Setting



The following table describes the fields in this screen.

**Table 122** Maintenance > Log Setting

| LABEL | DESCRIPTION |
|---|---|
| Syslog Setting | |
| Syslog Logging | The Device sends a log to an external syslog server. Select **Enable** to enable syslog logging. |
| Mode | Select the syslog destination from the drop-down list box.<br>If you select **Remote**, the log(s) will be sent to a remote syslog server. 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**. |
| Syslog Server | Enter the server name or IP address of the syslog server that will log the selected categories of logs. |
| UDP Port | Enter the port number used by the syslog server. |
| E-mail Log Settings | |
| Mail Server | Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail. |
| System Log 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. |
| Security Log Mail Subject | Type a title that you want to be in the subject line of the security log e-mail message that the Device sends. |
| Send Log 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. |
| Send Alarm to | Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail. |
| Alarm Interval | Specify how often the alarm should be updated. |
| Allowed Capacity Before Email | Set what percent of the Device's log storage space can be filled before the Device sends a log e-mail. |
| Clear log after sending mail | Select this to delete all the logs after the Device sends an E-mail of the logs. |
| Active Log and Alert | |
| System Log | Select the categories of system logs that you want to record. |
| Security Log | Select the categories of security logs that you want to record. |
| Send immediate alert | Select log categories for which you want the Device to send E-mail alerts immediately. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

## 33.2.1 Example E-mail Log

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

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.

- "End of Log" message shows that a complete log has been sent.

**Figure 157** E-mail Log Example

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

End of Firewall Log
```

# 34

# Firmware Upgrade

## 34.1 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.

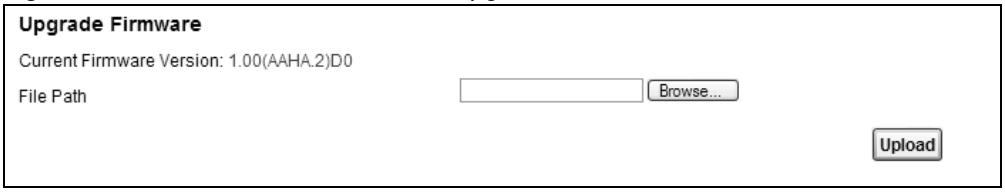
**Only use firmware for your device's specific model. Refer to the label on the bottom of your Device.**

## 34.2 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 158** Maintenance > Firmware Upgrade



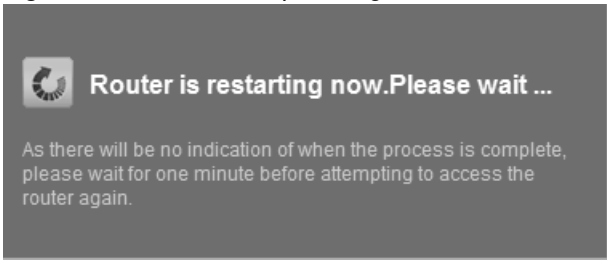

The following table describes the labels in this screen.

**Table 123** 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. |

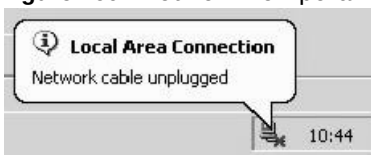
After you see the firmware updating screen, wait two minutes before logging into the Device again.

**Figure 159** 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.

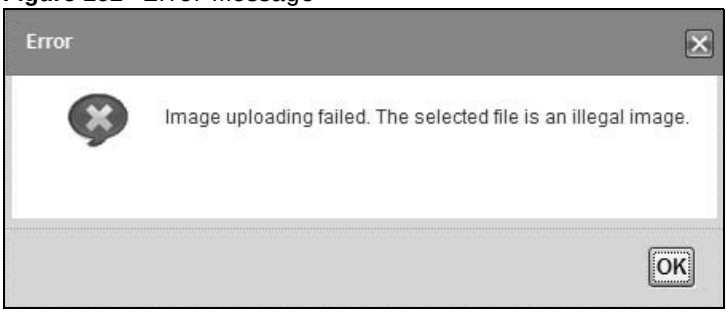
**Figure 160** Network Temporarily Disconnected




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 161** Error Message



# 35

# Configuration

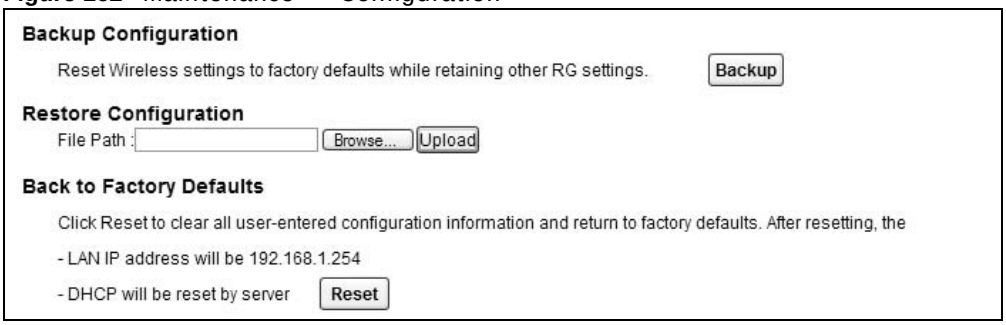
## 35.1 Overview

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

## 35.2 The Configuration Screen

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

**Figure 162** Maintenance > Configuration




### 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 124** Restore Configuration

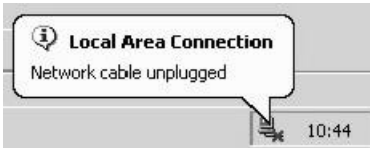
| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse ...** to find it. |
| Browse... | Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them. |
| Upload | Click this to begin the upload process. |

**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.

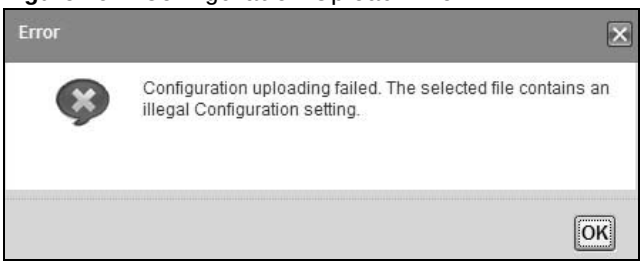
**Figure 163** Network Temporarily Disconnected




If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.254). See Appendix A on page 285 for details on how to set up your computer's IP address.

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

**Figure 164** Configuration Upload Error



### 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 165** Reset Warning Message

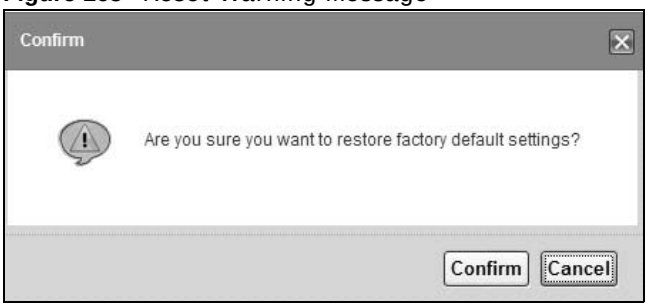
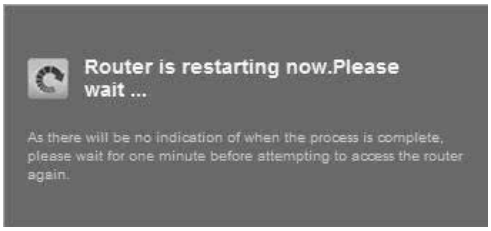



**Figure 166** Reset In Process Message




You can also press the **RESET** button on the rear panel to reset the factory defaults of your Device. Refer to Section 1.6 on page 22 for more information on the **RESET** button.

## 35.3 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 **Reboot** to have the Device reboot. This does not affect the Device's configuration.

**Figure 167** Maintenance > Reboot

# 36

# Diagnostic

## 36.1 Overview

The **Diagnostic** screens display information to help you identify problems with the Device.

The route between a CO VDSL switch and one of its CPE may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

### 36.1.1 What You Can Do in this Chapter

- The **Ping & TraceRoute & NsLookup** screen lets you ping an IP address or trace the route packets take to a host (Section 36.3 on page 274).
- The **802.1ag** screen lets you perform CFM actions (Section 36.5 on page 276).
- The **OAM Ping** screen lets you send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC. (Section 36.5 on page 276).

## 36.2 What You Need to Know

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

#### How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

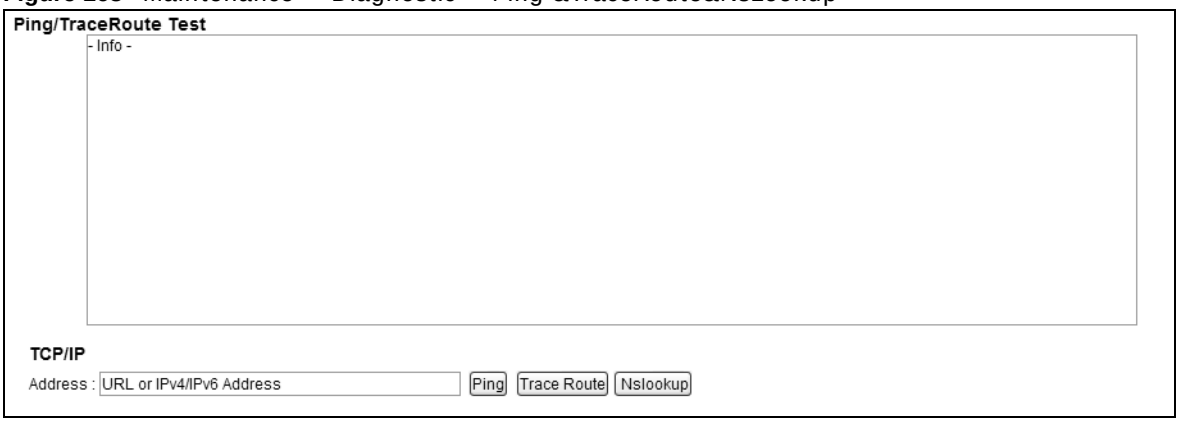
CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

# 36.3 Ping & TraceRoute & NsLookup

Use this screen to ping, traceroute, or nslookup an IP address. Click **Maintenance > Diagnostic > Ping&TraceRoute&NsLookup** to open the screen shown next.

**Figure 168** Maintenance > Diagnostic > Ping &TraceRoute&NsLookup




The following table describes the fields in this screen.

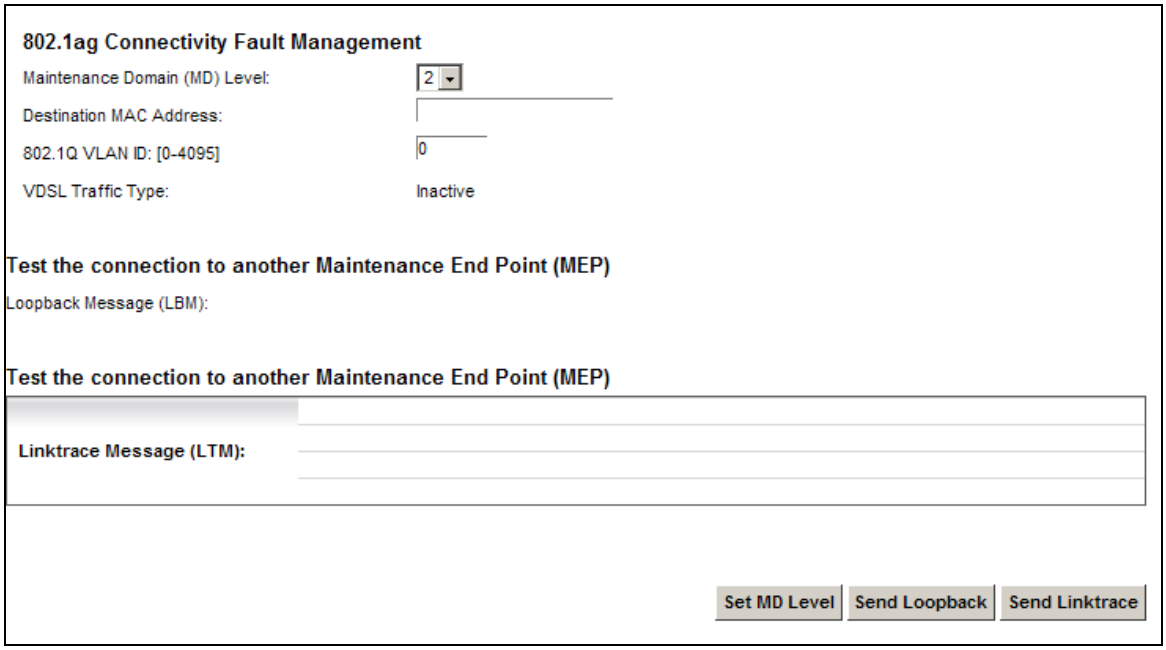
**Table 125** Maintenance > Diagnostic > Ping & TraceRoute & NsLookup

| LABEL | DESCRIPTION |
|---|---|
| URL or IP Address | Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection. |
| Ping | Click this to ping the IP address that you entered. |
| TraceRoute | Click this button to perform the traceroute function. This determines the path a packet takes to the specified computer. |
| Nslookup | Click this button to perform a DNS lookup on the IP address of a computer you enter. |

# 36.4 802.1ag

Click **Maintenance > Diagnostic** > **8.2.1ag** to open the following screen. Use this screen to perform CFM actions.

**Figure 169** Maintenance > Diagnostic > 802.1ag




The following table describes the fields in this screen.

**Table 126** Maintenance > Diagnostic > 802.1ag

| LABEL | DESCRIPTION |
|---|---|
| 802.1ag Connectivity Fault Management | |
| Maintenance Domain (MD) Level | Select a level (0-7) under which you want to create an MA. |
| Destination MAC Address | Enter the target device's MAC address to which the Device performs a CFM loopback test. |
| 802.1Q VLAN ID | Type a VLAN ID (0-4095) for this MA. |
| VDSL Traffic Type | This shows whether the VDSL traffic is activated. |
| Loopback Message (LBM) | This shows how many Loop Back Messages (LBMs) are sent and if there is any inorder or outorder Loop Back Response (LBR) received from a remote MEP. |
| Linktrace Message (LTM) | This shows the destination MAC address in the Link Trace Response (LTR). |
| Set MD Level | Click this button to configure the MD (Maintenance Domain) level. |
| Send Loopback | Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point. |
| Send Linktrace | Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point. |

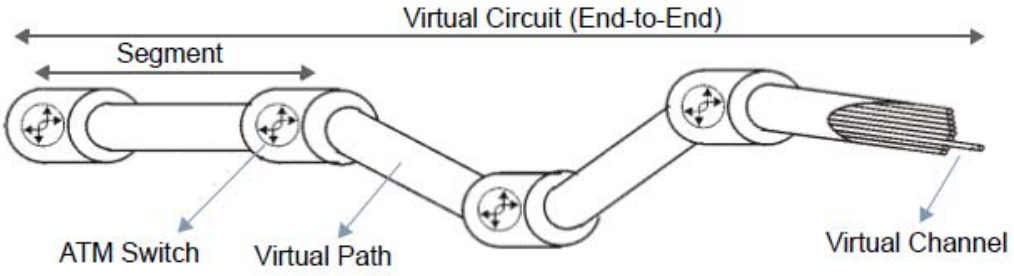
# 36.5 OAM Ping

Click **Maintenance > Diagnostic > OAM Ping** to open the screen shown next. Use this screen to perform an OAM (Operation, Administration and Maintenance) F4 or F5 loopback test on a PVC. The Device sends an OAM F4 or F5 packet to the DSLAM or ATM switch and then returns it to the Device. The test result then displays in the text box.

ATM sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel (VC) Logical connections between ATM devices
- Virtual Path (VP) A bundle of virtual channels
- Virtual Circuits A series of virtual paths between circuit end points

**Figure 170** Virtual Circuit Topology




Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path. A series of virtual paths make up a virtual circuit.

F4 cells operate at the virtual path (VP) level, while F5 cells operate at the virtual channel (VC) level. F4 cells use the same VPI as the user data cells on VP connections, but use different predefined VCI values. F5 cells use the same VPI and VCI as the user data cells on the VC connections, and are distinguished from data cells by a predefinded Payload Type Identifier (PTI) in the cell header. Both F4 flows and F5 flows are bidirectional and have two types.

- segment F4 flows (VCI=3)
- end-to-end F4 flows (VCI=4)
- segment F5 flows (PTI=100)
- end-to-end F5 flows (PTI=101)

OAM F4 or F5 tests are used to check virtual path or virtual channel availability between two DSL devices. Segment flows are terminated at the connecting point which terminates a VP or VC segment. End-to-end flows are terminated at the end point of a VP or VC connection, where an ATM link is terminated. Segment loopback tests allow you to verify integrity of a PVC to the nearest neighboring ATM device. End-to-end loopback tests allow you to verify integrity of an end-to-end PVC.

Note: The DSLAM to which the Device is connected must also support ATM F4 and/or F5 to use this test.

Note: This screen is available only when you configure an ATM layer-2 interface.

**Figure 171** Maintenance > Diagnostic > OAM Ping


The following table describes the fields in this screen.

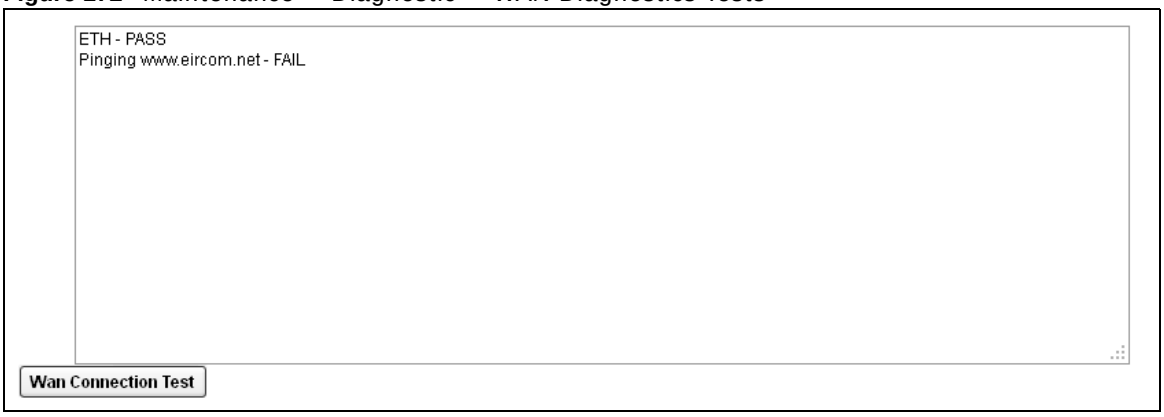
**Table 127** Maintenance > Diagnostic > OAM Ping

| LABEL | DESCRIPTION |
|---|---|
| | Select a PVC on which you want to perform the loopback test. |
| F4 segment | Press this to perform an OAM F4 segment loopback test. |
| F4 end-end | Press this to perform an OAM F4 end-to-end loopback test. |
| F5 segment | Press this to perform an OAM F5 segment loopback test. |
| F5 end-end | Press this to perform an OAM F5 end-to-end loopback test. |

# 36.6 WAN Diagnostics Tests

Click **Maintenance > Diagnostic > WAN Diagnostics Tests** to open the screen shown next. Use this screen to perform a test on the current WAN connection by clicking the **Wan Connection Test** button. The test result then displays in the text box.

**Figure 172** Maintenance > Diagnostic > WAN Diagnostics Tests



# 37

# 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
- Wireless Internet Access
- USB Device Connection
- UPnP

## 37.1 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 1.5 on page 20.
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.

## 37.2 Device Access and Login

### I forgot the IP address for the Device.

1 The default LAN 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 1.6 on page 22.

### I forgot the password.

1 The default admin password is the wireless key printed on the back of the Device.

2 If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 22.

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

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.254.
- If you changed the IP address (Section 6.2 on page 105), 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. See Section 1.5 on page 20.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix C on page 315.

4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote MGMT**).

5 Reset the device to its factory defaults, and try to access the Device with the default IP address. See Section 1.6 on page 22.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- 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.

## 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 admin password is the wireless key printed on the back of the Device. 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 37.1 on page 279.

## I cannot Telnet to the Device.

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

## I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

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

# 37.3 Internet Access

## I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Section 1.5 on page 20.
2. Make sure you entered your ISP account information correctly in the **Network Setting > Broadband** screen. 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 that you enabled the wireless LAN in the Device and your wireless client and that the wireless settings in the wireless client are the same as the settings in the Device.
4. Disconnect all the cables from your device and reconnect them.
5. If the problem continues, contact your ISP.

## I cannot access the Internet through a DSL connection.

1. Make sure you have the **DSL WAN** port connected to a telephone jack (or the DSL or modem jack on a splitter if you have one).
2. Make sure you configured a proper DSL WAN interface (**Network Setting > Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.
3. Check that the LAN interface you are connected to is in the same interface group as the DSL connection (**Network Setting > Interface Group**).
4. If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

## I cannot connect to the Internet using a second DSL connection.

ADSL and VDSL connections cannot work at the same time. You can only use one type of DSL connection, either ADSL or VDSL connection at one time.

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

1. Your session with the Device may have expired. Try logging into the Device again.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Section 1.5 on page 20.

3 Turn the Device off and on.

4 If the problem continues, contact your ISP.

## 37.4 Wireless Internet Access

### What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

### What is a Server Set ID (SSID)?

An SSID is a name that uniquely identifies a wireless network. The AP and all the clients within a wireless network must use the same SSID.

# 37.5 USB Device Connection

The Device fails to detect my USB device.

1. Disconnect the USB device.
2. Reboot the Device.
3. 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.
4. Re-connect your USB device to the Device.

# 37.6 UPnP

When using UPnP and the Device reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1. Disconnect the Ethernet cable from the Device's LAN port or from your computer.
2. Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

1. Wait more than three minutes.
2. Restart the applications.

A

# Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

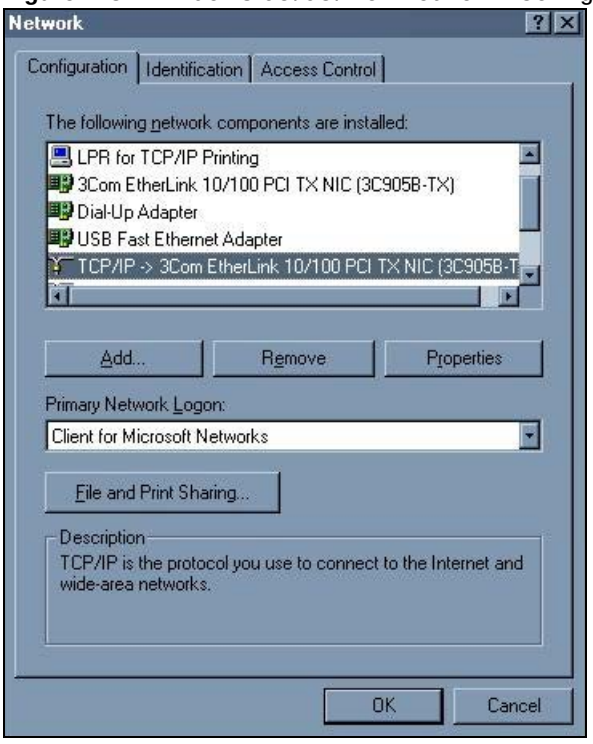
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Device's LAN port.

## Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 173** WIndows 95/98/Me: Network: Configuration



## Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.

2 Select **Adapter** and then click **Add**.

3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.

2 Select **Protocol** and then click **Add**.

3 Select **Microsoft** from the list of **manufacturers**.

4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

## Configuring

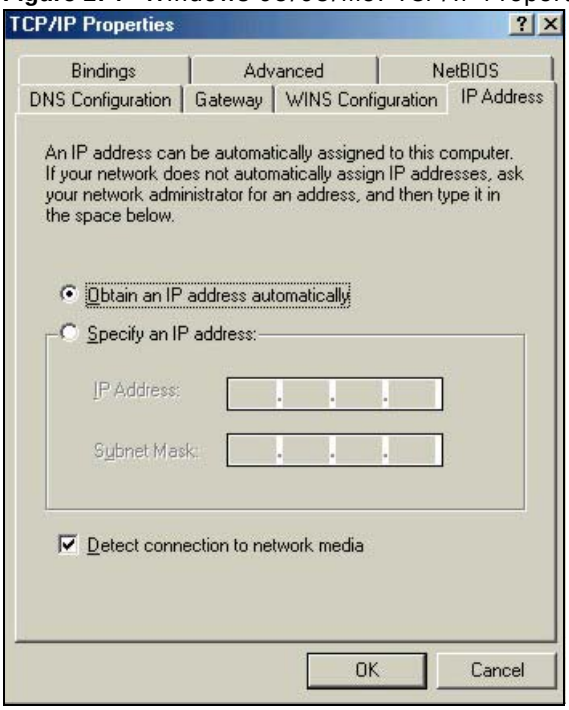
1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.

- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

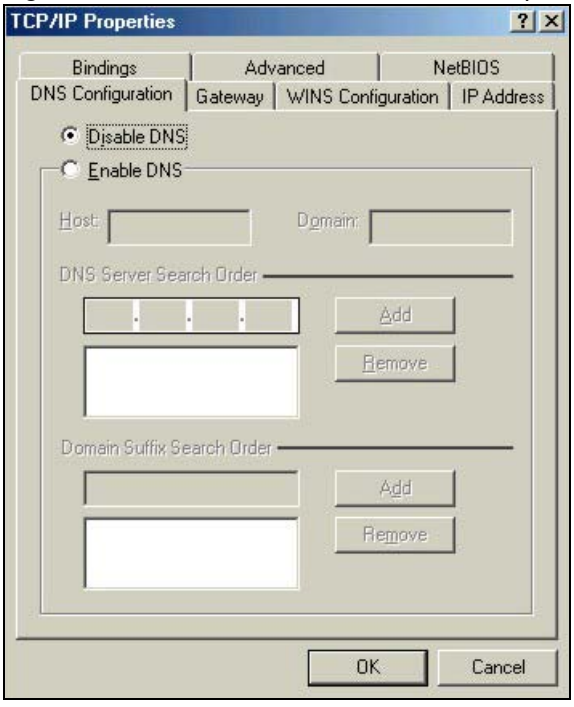
**Figure 174** Windows 95/98/Me: TCP/IP Properties: IP Address




**3** Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 175** Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.
   - If you do not know your gateway's IP address, remove previously installed gateways.
   - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your Device and restart your computer when prompted.

## Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

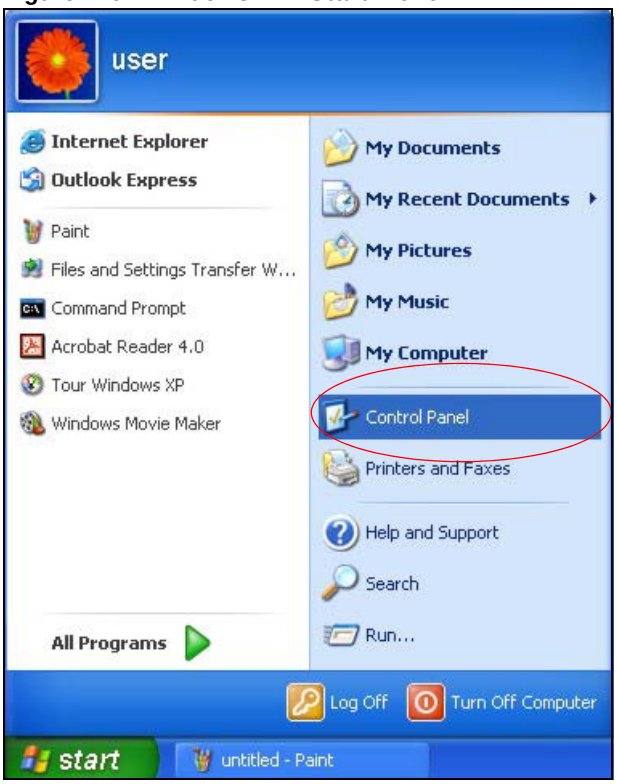
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

**Figure 176** Windows XP: Start Menu



2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

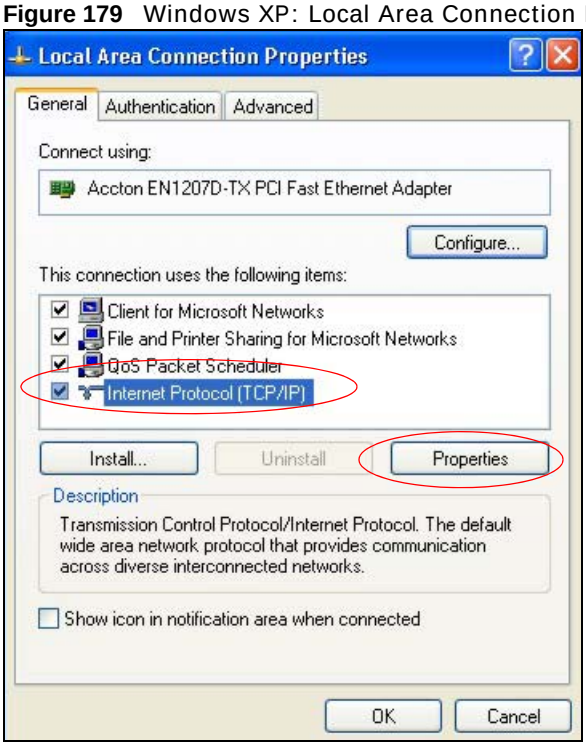
**Figure 177** Windows XP: Control Panel


3 Right-click **Local Area Connection** and then click **Properties**.

**Figure 178** Windows XP: Control Panel: Network Connections: Properties

4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

**Figure 179** Windows XP: Local Area Connection Properties

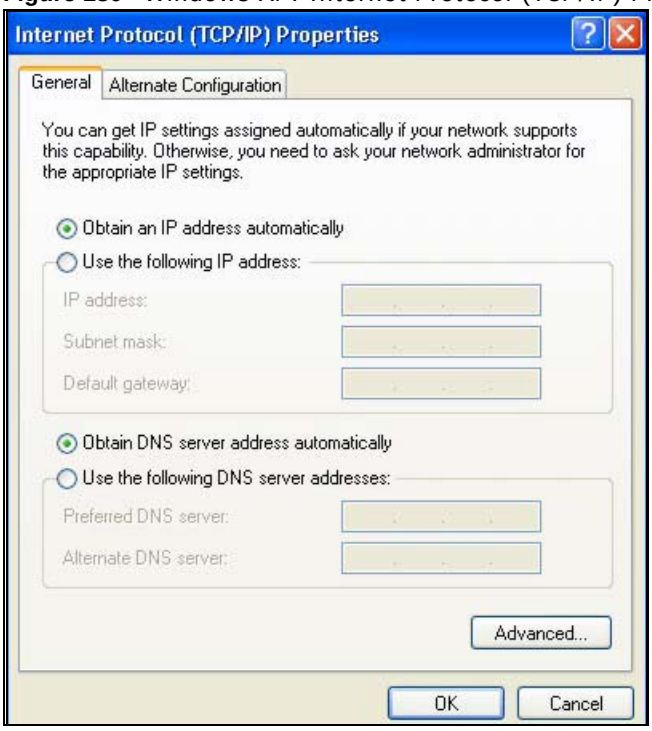



5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

- Click **Advanced**.

**Figure 180** Windows XP: Internet Protocol (TCP/IP) Properties



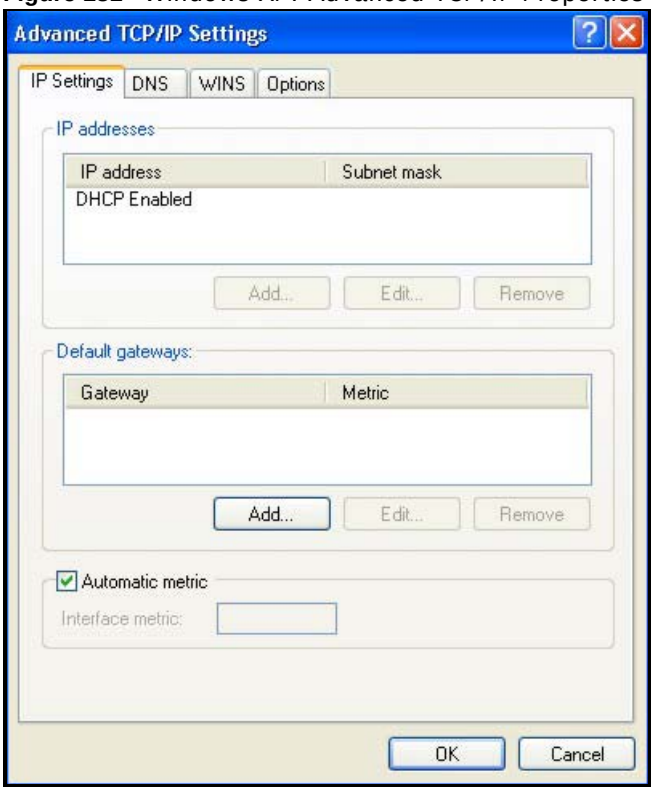

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

**Figure 181** Windows XP: Advanced TCP/IP Properties

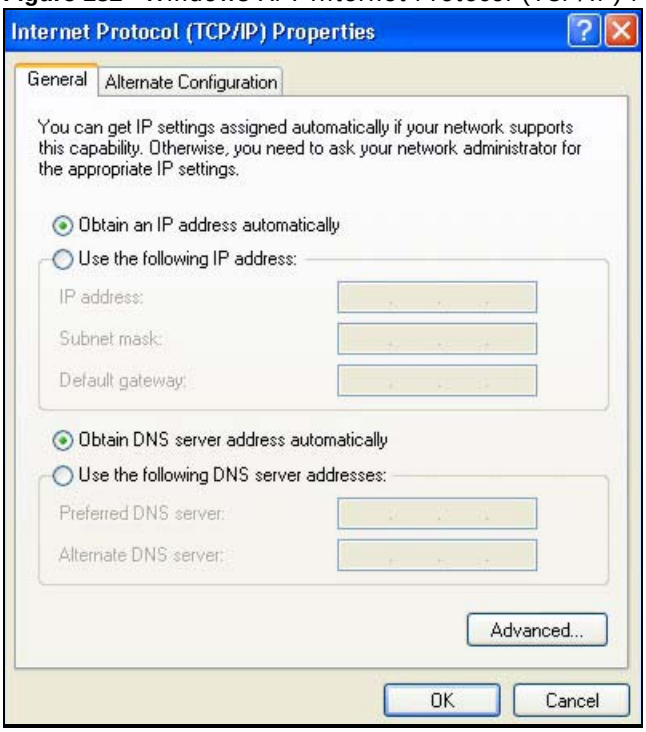



7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 182** Windows XP: Internet Protocol (TCP/IP) Properties




8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your Device and restart your computer (if prompted).

## Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Windows Vista

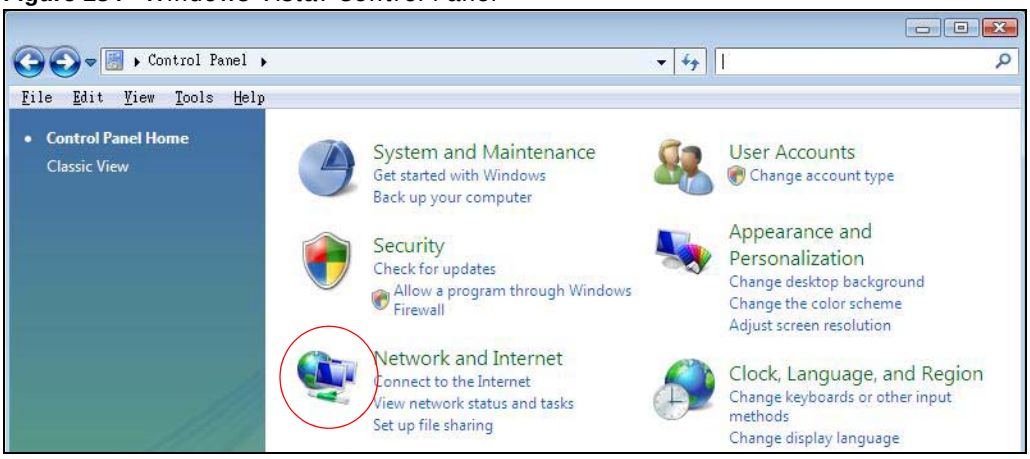
This section shows screens from Windows Vista Enterprise Version 6.0.

1 Click the **Start** icon, **Control Panel**.

**Figure 183** Windows Vista: Start Menu

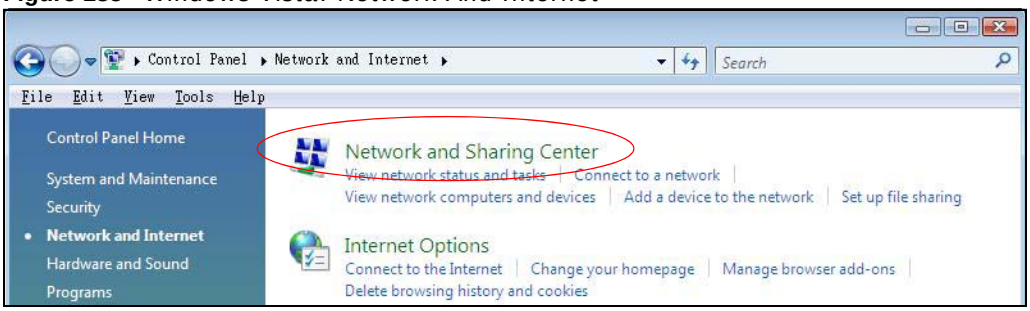

2 In the **Control Panel**, double-click **Network and Internet**.

**Figure 184** Windows Vista: Control Panel



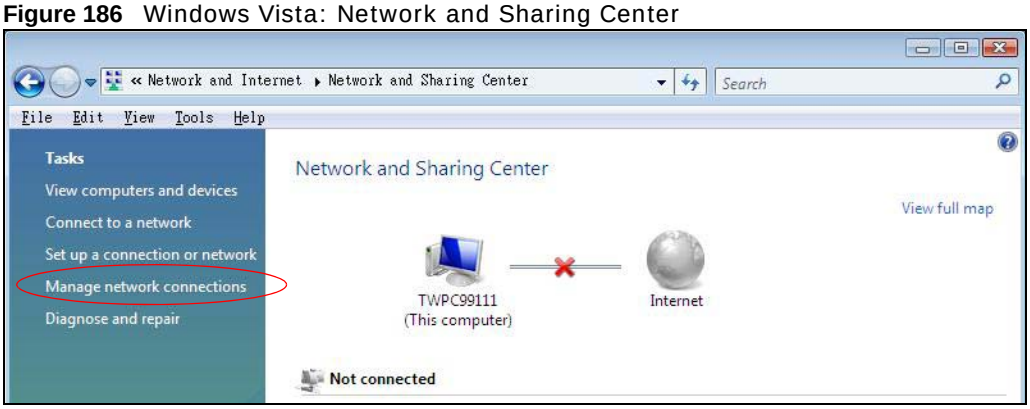

3 Click **Network and Sharing Center**.

**Figure 185** Windows Vista: Network And Internet



4 Click **Manage network connections**.

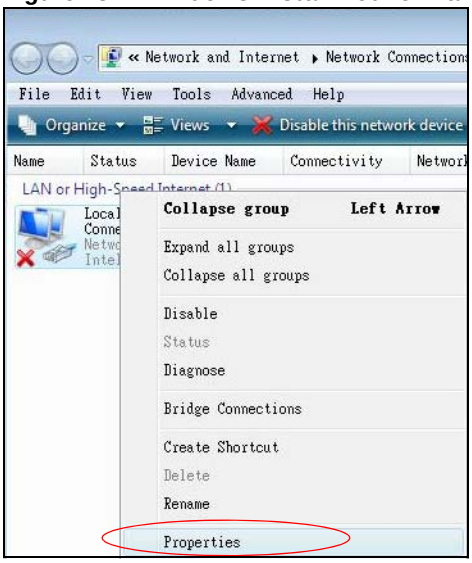
**Figure 186** Windows Vista: Network and Sharing Center




5 Right-click **Local Area Connection** and then click **Properties**.

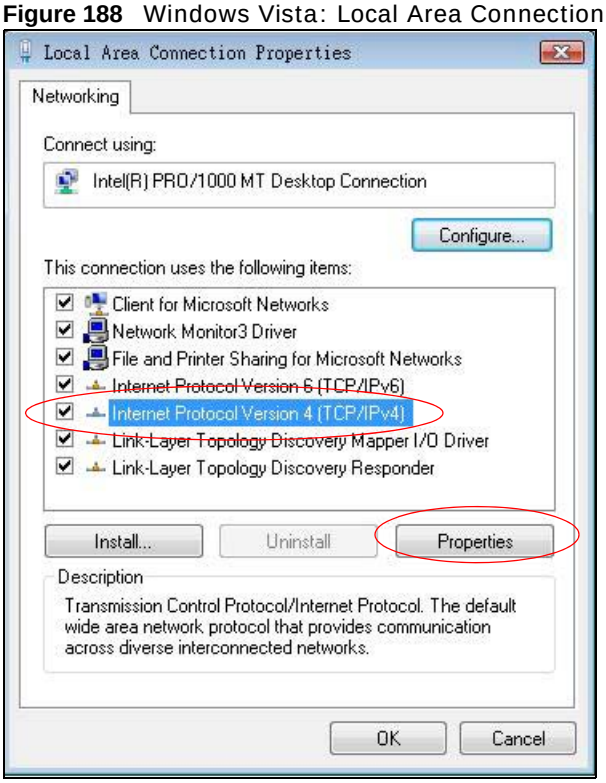
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

**Figure 187** Windows Vista: Network and Sharing Center



6 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

**Figure 188** Windows Vista: Local Area Connection Properties

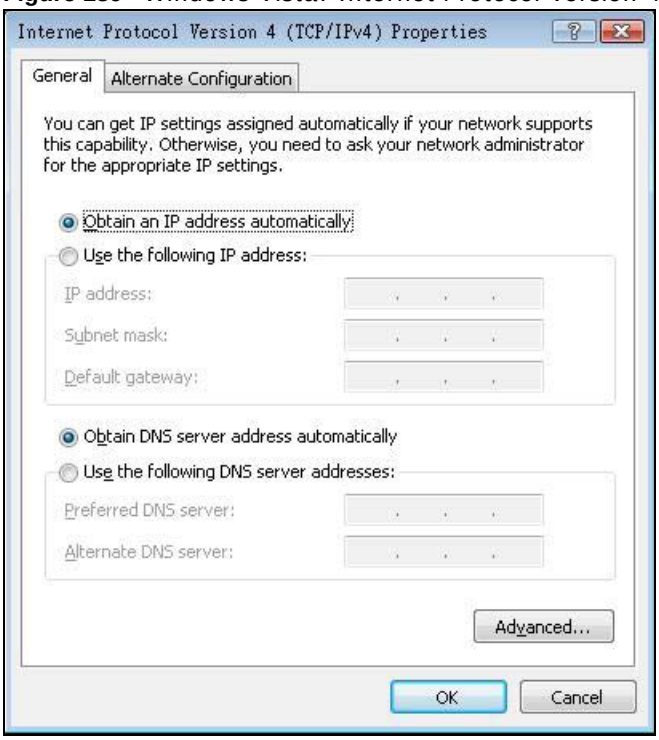



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General tab**).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

- Click **Advanced**.

**Figure 189** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



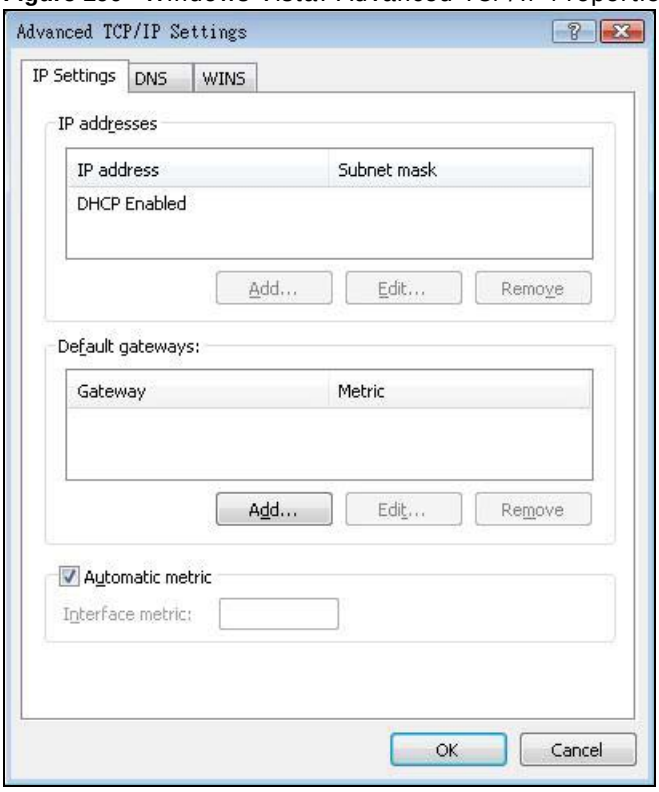

8 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

**Figure 190** Windows Vista: Advanced TCP/IP Properties

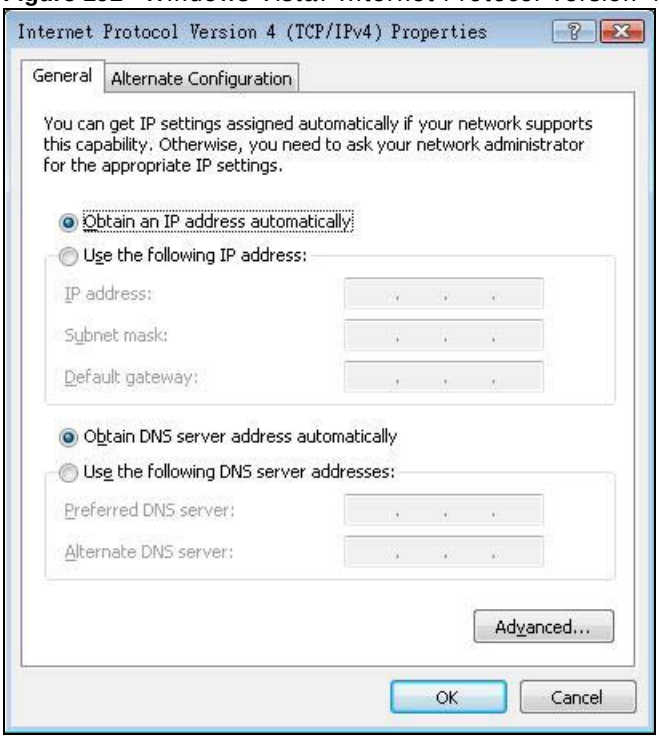



9 In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General tab**):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 191** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties




10 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

11 Click **Close** to close the **Local Area Connection Properties** window.

12 Close the **Network Connections** window.

13 Turn on your Device and restart your computer (if prompted).

## Verifying Settings

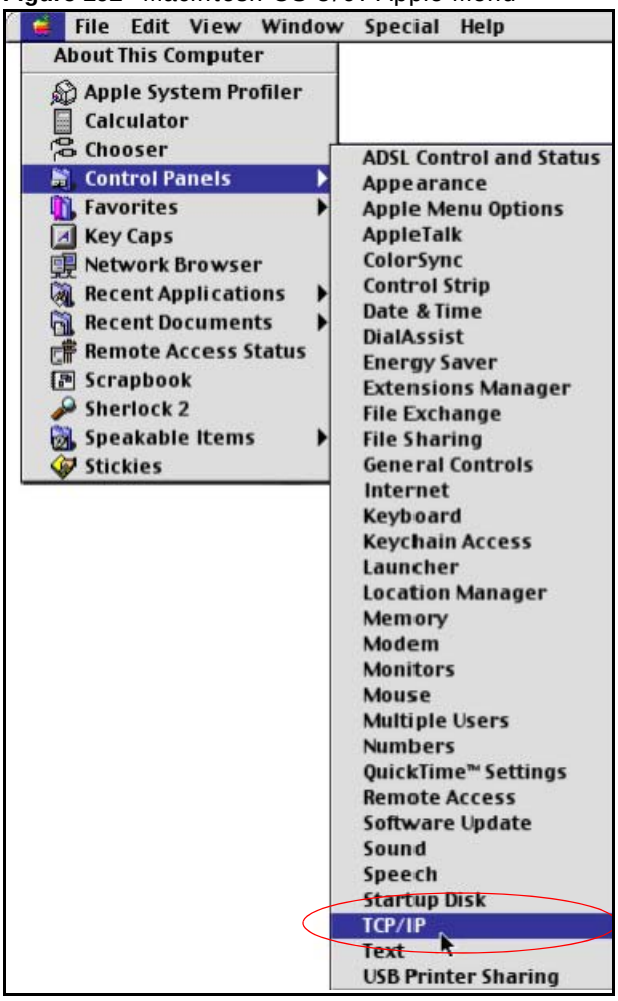
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

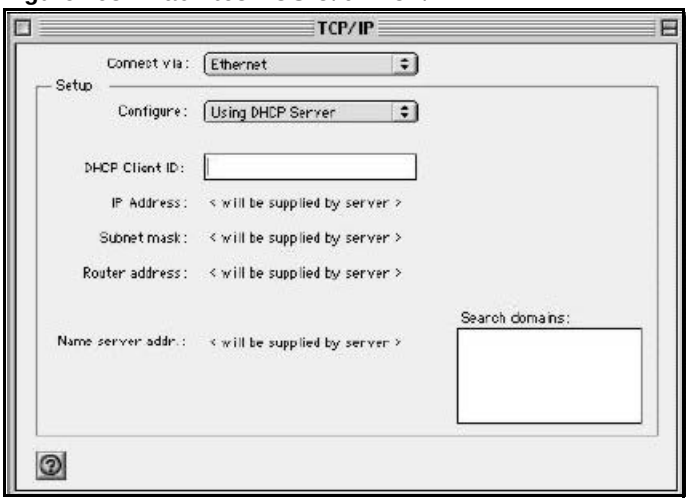
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 192** Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

**Figure 193** Macintosh OS 8/9: TCP/IP




3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Device in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your Device and restart your computer (if prompted).

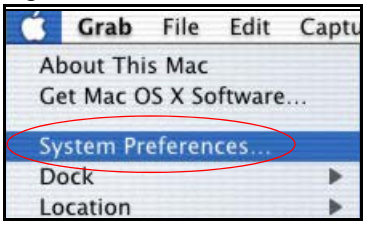
## Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

## Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 194** Macintosh OS X: Apple Menu



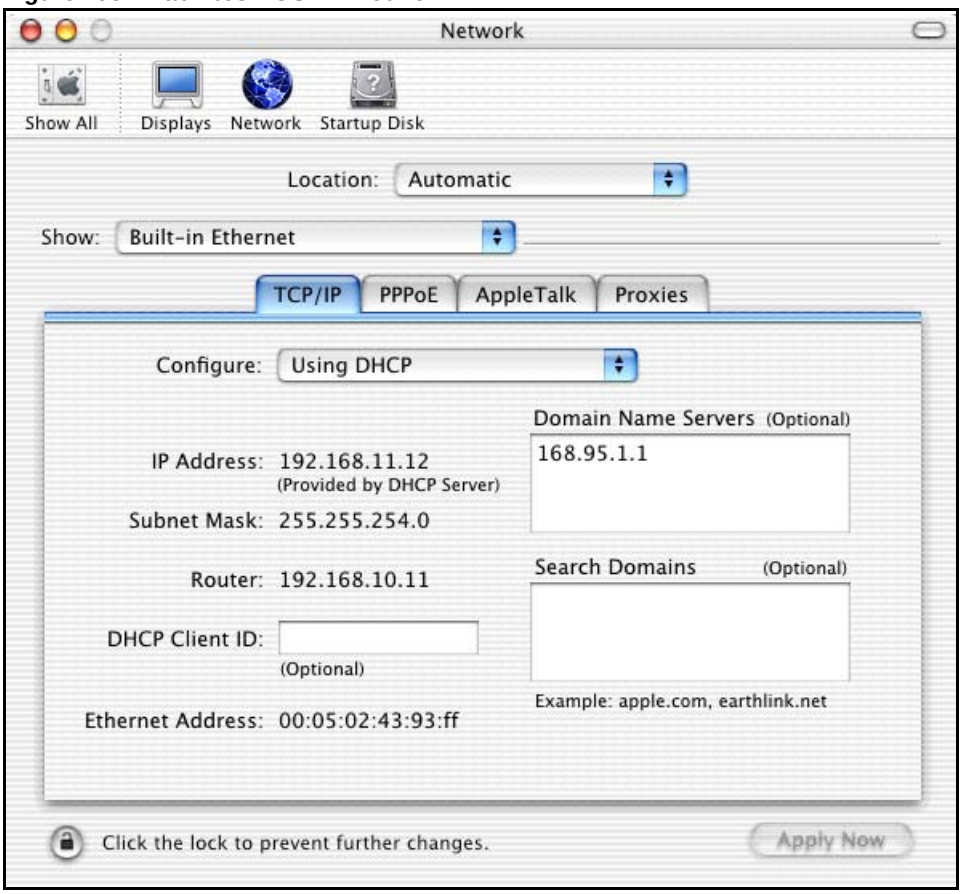

2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.

- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 195** Macintosh OS X: Network




4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Device in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your Device and restart your computer (if prompted).

## Verifying Settings

Check your TCP/IP properties in the **Network** window.

## Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

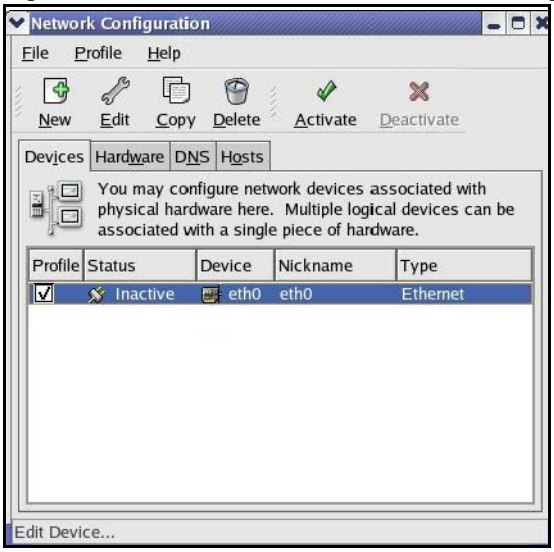
Note: Make sure you are logged in as the root administrator.

## Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 196** Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

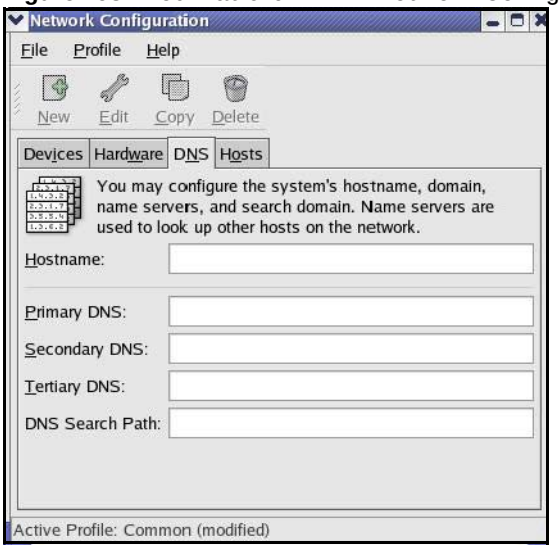
**Figure 197** Red Hat 9.0: KDE: Ethernet Device: General


- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

**Figure 198** Red Hat 9.0: KDE: Network Configuration: DNS




5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

**Figure 199** Red Hat 9.0: KDE: Network Configuration: Activate


7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

## Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

**Figure 200** Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

**Figure 201** Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

**Figure 202** Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

**Figure 203** Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                  [OK]
Shutting down loopback interface:              [OK]
Setting network parameters:                    [OK]
Bringing up loopback interface:                [OK]
Bringing up interface eth0:                    [OK]
```

## Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

**Figure 204** Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

B

# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

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

## Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

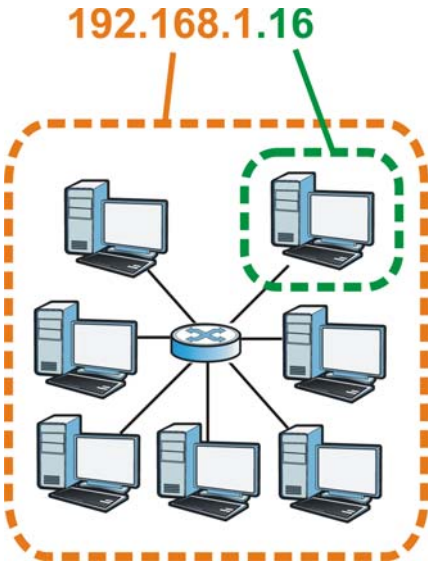
## Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 205** Network Number and Host ID




How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 128** Subnet Masks

| | 1ST OCTET: (192) | 2ND OCTET: (168) | 3RD OCTET: (1) | 4TH OCTET (2) |
|---|---|---|---|---|
| IP Address (Binary) | 11000000 | 10101000 | 00000001 | 00000010 |
| Subnet Mask (Binary) | **11111111** | **11111111** | **11111111** | 00000000 |
| Network Number | **11000000** | **10101000** | **00000001** | |
| Host ID | | | | 00000010 |

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 129** Subnet Masks

| | BINARY | | | | DECIMAL |
|---|---|---|---|---|---|
| | 1ST OCTET | 2ND OCTET | 3RD OCTET | 4TH OCTET | |
| 8-bit mask | 11111111 | 00000000 | 00000000 | 00000000 | 255.0.0.0 |
| 16-bit mask | 11111111 | 11111111 | 00000000 | 00000000 | 255.255.0.0 |
| 24-bit mask | 11111111 | 11111111 | 11111111 | 00000000 | 255.255.255.0 |
| 29-bit mask | 11111111 | 11111111 | 11111111 | 11111000 | 255.255.255.248 |

## Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 130** Maximum Host Numbers

| SUBNET MASK | | HOST ID SIZE | | MAXIMUM NUMBER OF HOSTS |
|---|---|---|---|---|
| 8 bits | 255.0.0.0 | 24 bits | $2^{24} – 2$ | 16777214 |
| 16 bits | 255.255.0.0 | 16 bits | $2^{16} – 2$ | 65534 |
| 24 bits | 255.255.255.0 | 8 bits | $2^{8} – 2$ | 254 |
| 29 bits | 255.255.255.248 | 3 bits | $2^{3} – 2$ | 6 |

## Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 131** Alternative Subnet Mask Notation

| SUBNET MASK | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|---|---|---|---|
| 255.255.255.0 | /24 | 0000 0000 | 0 |
| 255.255.255.128 | /25 | 1000 0000 | 128 |
| 255.255.255.192 | /26 | 1100 0000 | 192 |
| 255.255.255.224 | /27 | 1110 0000 | 224 |
| 255.255.255.240 | /28 | 1111 0000 | 240 |
| 255.255.255.248 | /29 | 1111 1000 | 248 |
| 255.255.255.252 | /30 | 1111 1100 | 252 |

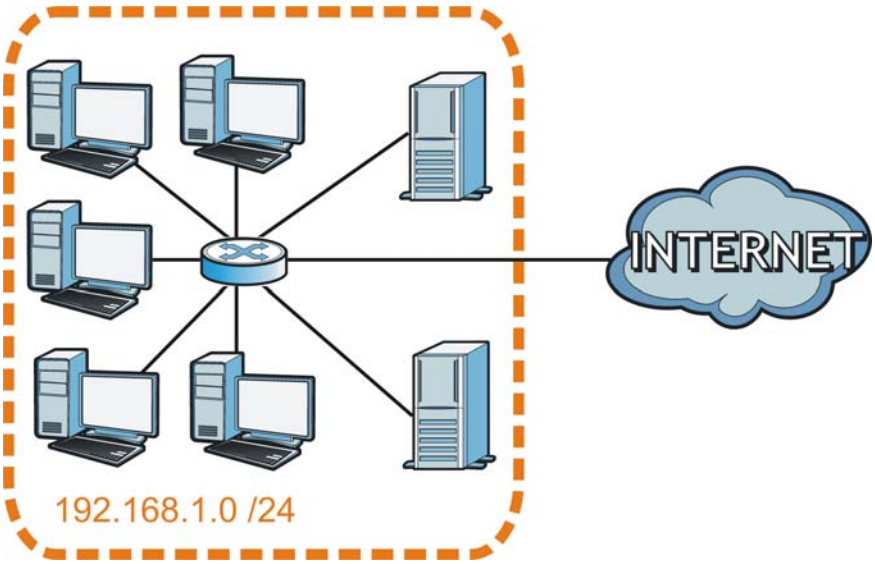
## Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8$ – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

**Figure 206** Subnetting Example: Before Subnetting

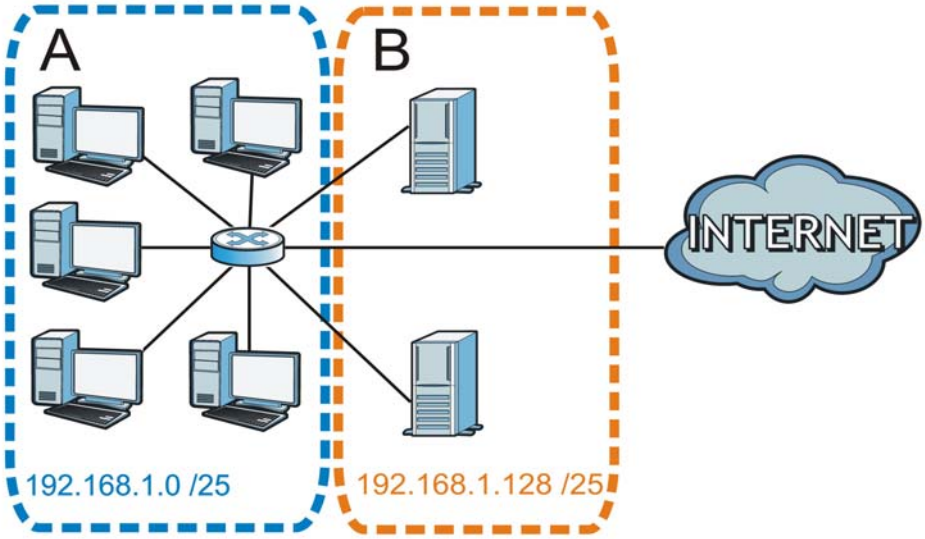



You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

**Figure 207** Subnetting Example: After Subnetting




In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7$ – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6$ - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 132** Subnet 1

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address (Decimal) | 192.168.1. | 0 |
| IP Address (Binary) | 11000000.10101000.00000001. | **00**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |

**Table 132** Subnet 1 (continued)

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| Subnet Address: 192.168.1.0 | Lowest Host ID: 192.168.1.1 | |
| Broadcast Address: 192.168.1.63 | Highest Host ID: 192.168.1.62 | |

**Table 133** Subnet 2

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 64 |
| IP Address (Binary) | 11000000.10101000.00000001. | **01**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.64 | Lowest Host ID: 192.168.1.65 | |
| Broadcast Address: 192.168.1.127 | Highest Host ID: 192.168.1.126 | |

**Table 134** Subnet 3

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 128 |
| IP Address (Binary) | 11000000.10101000.00000001. | **10**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.128 | Lowest Host ID: 192.168.1.129 | |
| Broadcast Address: 192.168.1.191 | Highest Host ID: 192.168.1.190 | |

**Table 135** Subnet 4

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 192 |
| IP Address (Binary) | 11000000.10101000.00000001. | **11**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.192 | Lowest Host ID: 192.168.1.193 | |
| Broadcast Address: 192.168.1.255 | Highest Host ID: 192.168.1.254 | |

## Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

**Table 136** Eight Subnets

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|---|---|---|---|---|
| 1 | 0 | 1 | 30 | 31 |
| 2 | 32 | 33 | 62 | 63 |

**Table 136** Eight Subnets (continued)

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|---|---|---|---|---|
| 3 | 64 | 65 | 94 | 95 |
| 4 | 96 | 97 | 126 | 127 |
| 5 | 128 | 129 | 158 | 159 |
| 6 | 160 | 161 | 190 | 191 |
| 7 | 192 | 193 | 222 | 223 |
| 8 | 224 | 225 | 254 | 255 |

## Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 137** 24-bit Network Number Subnet Planning

| NO. "BORROWED" HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.255.128 (/25) | 2 | 126 |
| 2 | 255.255.255.192 (/26) | 4 | 62 |
| 3 | 255.255.255.224 (/27) | 8 | 30 |
| 4 | 255.255.255.240 (/28) | 16 | 14 |
| 5 | 255.255.255.248 (/29) | 32 | 6 |
| 6 | 255.255.255.252 (/30) | 64 | 2 |
| 7 | 255.255.255.254 (/31) | 128 | 1 |

The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 138** 16-bit Network Number Subnet Planning

| NO. "BORROWED" HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.128.0 (/17) | 2 | 32766 |
| 2 | 255.255.192.0 (/18) | 4 | 16382 |
| 3 | 255.255.224.0 (/19) | 8 | 8190 |
| 4 | 255.255.240.0 (/20) | 16 | 4094 |
| 5 | 255.255.248.0 (/21) | 32 | 2046 |
| 6 | 255.255.252.0 (/22) | 64 | 1022 |
| 7 | 255.255.254.0 (/23) | 128 | 510 |
| 8 | 255.255.255.0 (/24) | 256 | 254 |
| 9 | 255.255.255.128 (/25) | 512 | 126 |
| 10 | 255.255.255.192 (/26) | 1024 | 62 |
| 11 | 255.255.255.224 (/27) | 2048 | 30 |
| 12 | 255.255.255.240 (/28) | 4096 | 14 |
| 13 | 255.255.255.248 (/29) | 8192 | 6 |
| 14 | 255.255.255.252 (/30) | 16384 | 2 |
| 15 | 255.255.255.254 (/31) | 32768 | 1 |

## Configuring IP Addresses

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the Device.

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

The subnet mask specifies the network number portion of an IP address. Your 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 (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

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

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

C

# Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

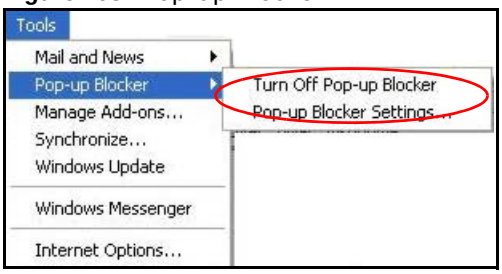
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

## Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

**Figure 208** Pop-up Blocker

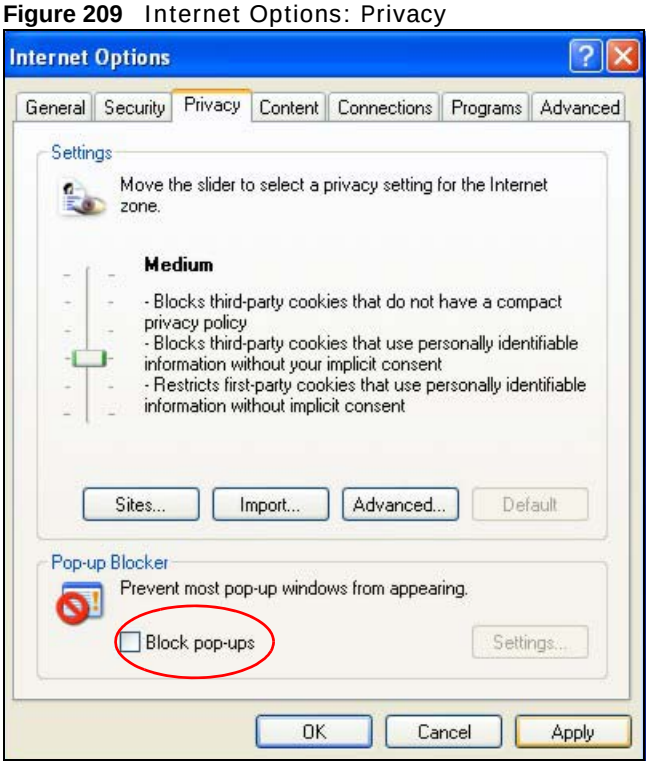



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 209** Internet Options: Privacy




3 Click **Apply** to save this setting.

## Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

**Figure 210** Internet Options: Privacy


3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 211** Pop-up Blocker Settings


5 Click **Close** to return to the **Privacy** screen.

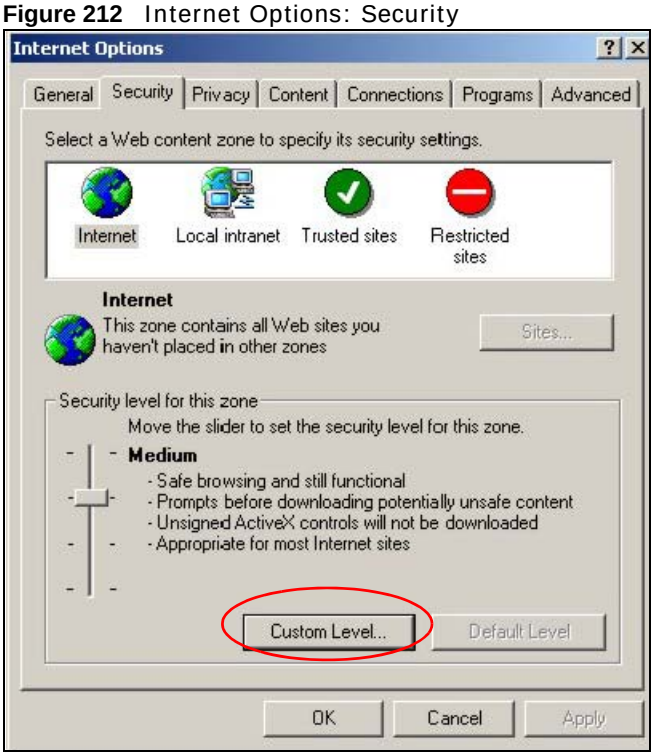
6 Click **Apply** to save this setting.

## JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

**Figure 212** Internet Options: Security




2 Click the **Custom Level...** button.

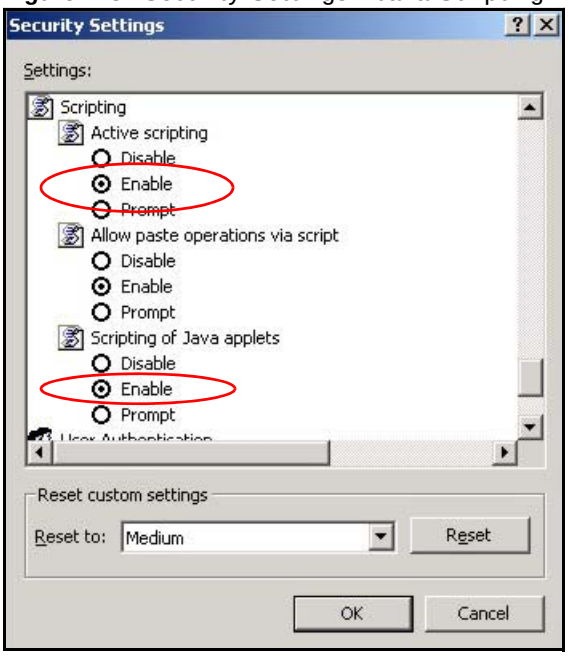
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

**Figure 213** Security Settings - Java Scripting




## Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

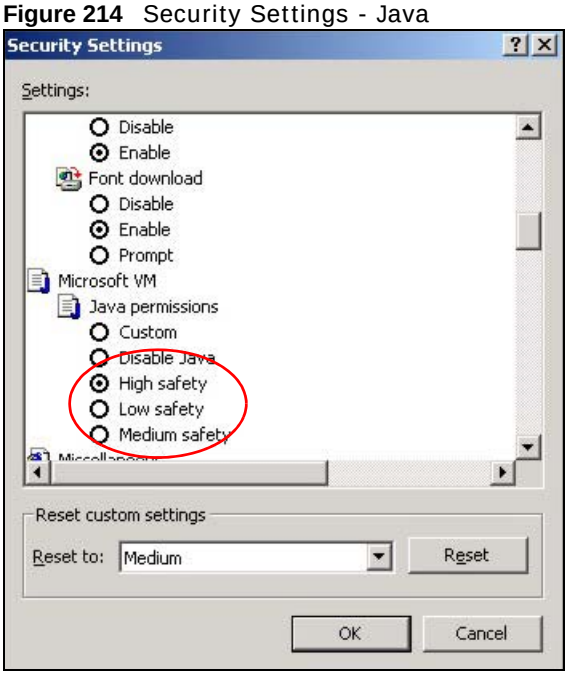
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

**Figure 214** Security Settings - Java



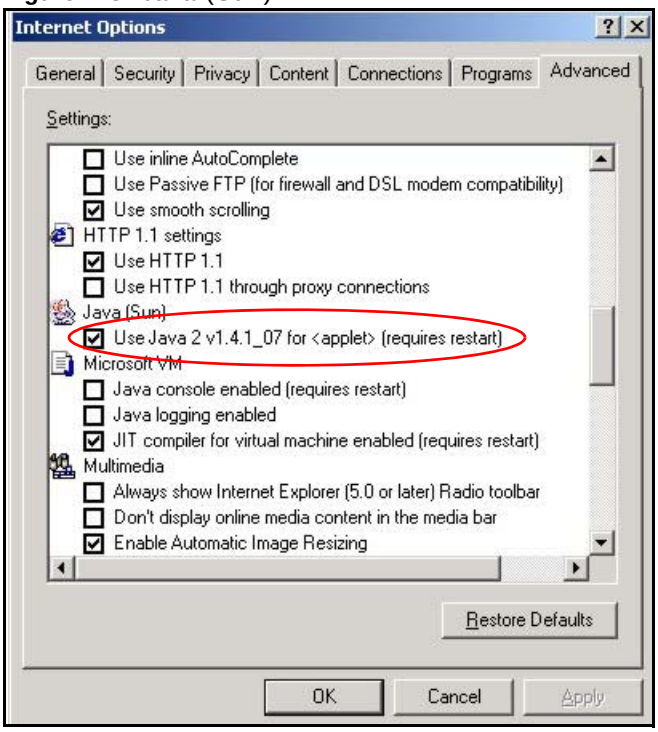

## JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

**Figure 215** Java (Sun)

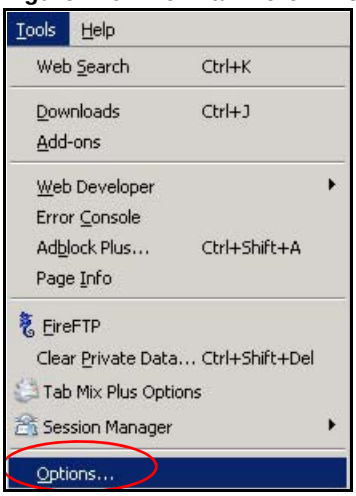



## Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

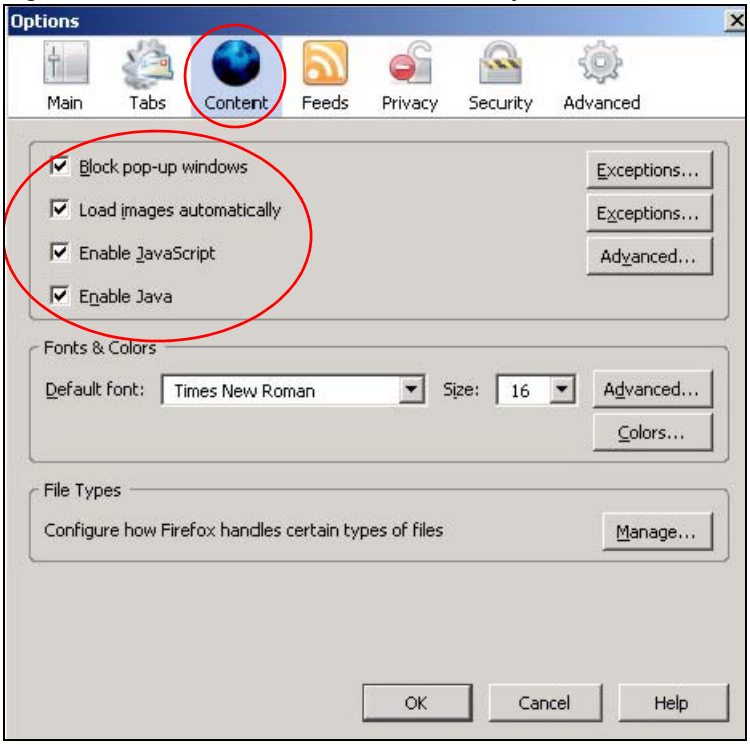
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

**Figure 216** Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

**Figure 217** Mozilla Firefox Content Security



# D

# Wireless LANs

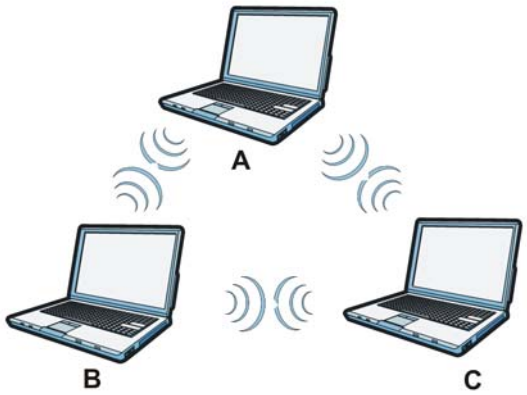
## Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

## Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

**Figure 218** Peer-to-Peer Communication in an Ad-hoc Network



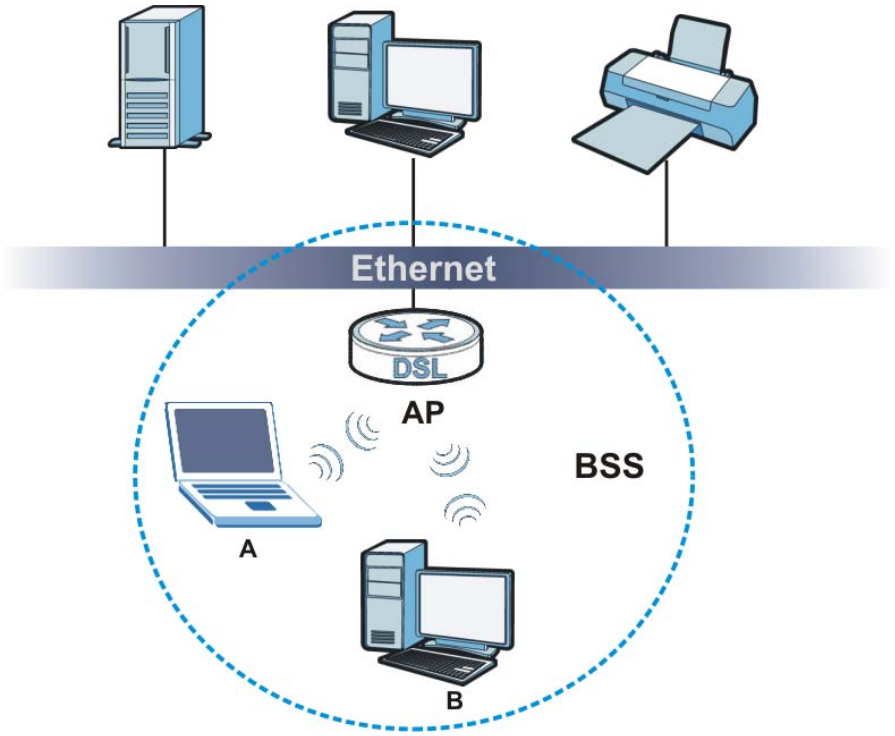

## BSS

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

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is

disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

**Figure 219** Basic Service Set



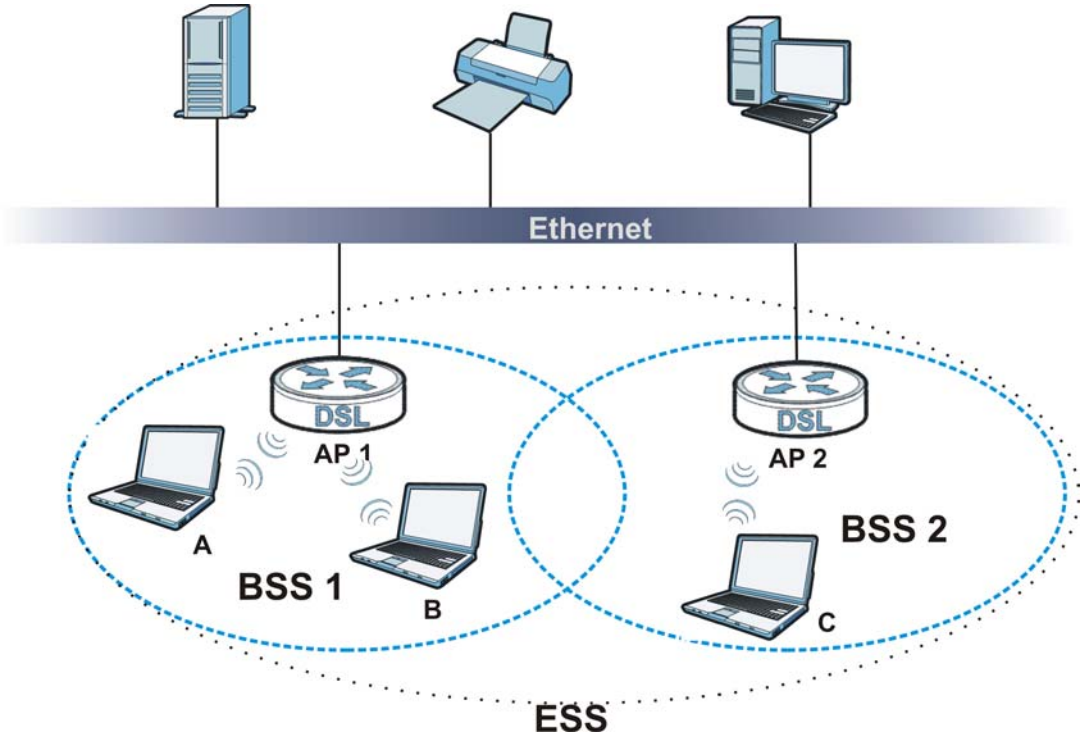

## ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

**Figure 220** Infrastructure WLAN




## Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

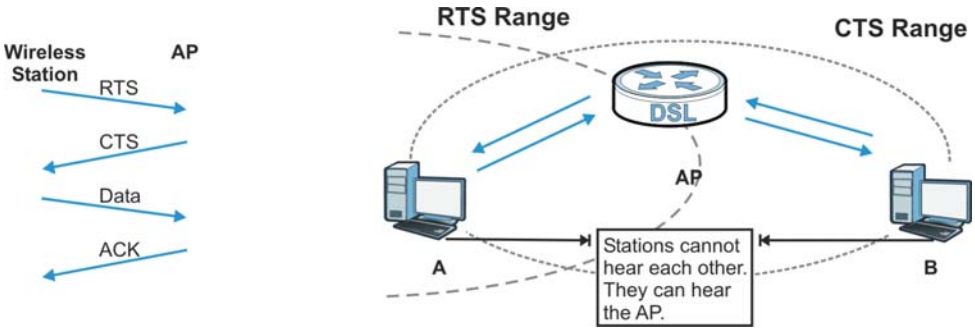
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

## RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they

cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

**Figure 221** RTS/CTS




When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

**RTS/CTS** is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

## Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 139** IEEE 802.11g

| DATA RATE (MBPS) | MODULATION |
|---|---|
| 1 | DBPSK (Differential Binary Phase Shift Keyed) |
| 2 | DQPSK (Differential Quadrature Phase Shift Keying) |
| 5.5 / 11 | CCK (Complementary Code Keying) |
| 6/9/12/18/24/36/48/54 | OFDM (Orthogonal Frequency Division Multiplexing) |

## Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your Device.

**Table 140** Wireless Security Levels

| SECURITY LEVEL | SECURITY TYPE |
|---|---|
| Least Secure | Unique SSID (Default) |
| | Unique SSID with Hide SSID Enabled |
| | MAC Address Filtering |
| | WEP Encryption |
| | IEEE802.1x EAP with RADIUS Server Authentication |
| | Wi-Fi Protected Access (WPA) |
| Most Secure | WPA2 |

Note: You must enable the same wireless security settings on the Device and on all wireless clients that you want to associate with it.

## IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

## RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

## Types of RADIUS Messages

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

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

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

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

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

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

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

## Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

## EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

## EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

## EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

## PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

## LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

## Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

**Table 141** Comparison of EAP Authentication Types

| | EAP-MD5 | EAP-TLS | EAP-TTLS | PEAP | LEAP |
|---|---|---|---|---|---|
| Mutual Authentication | No | Yes | Yes | Yes | Yes |
| Certificate – Client | No | Yes | Optional | Optional | No |
| Certificate – Server | No | Yes | Yes | Yes | No |
| Dynamic Key Exchange | No | Yes | Yes | Yes | Yes |
| Credential Integrity | None | Strong | Strong | Strong | Moderate |
| Deployment Difficulty | Easy | Hard | Moderate | Moderate | Moderate |
| Client Identity Protection | No | No | Yes | Yes | No |

## WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

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. The common-password approach makes WPA(2)-PSK susceptible to brute-force

password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

## User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

## Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

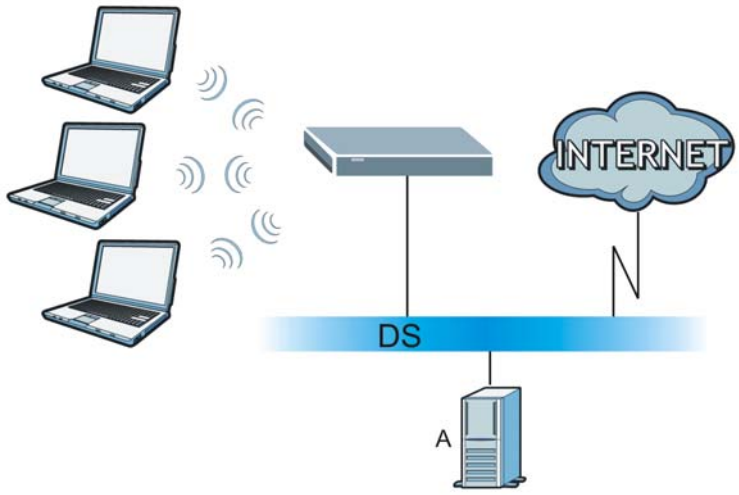
## WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

**Figure 222** WPA(2) with RADIUS Application Example




## WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

**Figure 223** WPA(2)-PSK Authentication

## Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

**Table 142** Wireless Security Relational Matrix

| AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL | ENCRYPTION METHOD | ENTER MANUAL KEY | IEEE 802.1X |
|---|---|---|---|
| Open | None | No | Disable |
| | | | Enable without Dynamic WEP Key |
| Open | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| Shared | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| WPA | TKIP/AES | No | Enable |
| WPA-PSK | TKIP/AES | Yes | Disable |
| WPA2 | TKIP/AES | No | Enable |
| WPA2-PSK | TKIP/AES | Yes | Disable |

## Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

## Antenna Characteristics

## Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

## Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

## Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately

2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

## Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

## Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

# E

# IPv6

## Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x $10^{38}$ IP addresses.

## IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

## Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as “/x” where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

## Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a “private IP address” in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

**Table 143** Link-local Unicast Address Format

| | | |
|---|---|---|
| 1111 1110 10 | 0 | Interface ID |
| 10 bits | 54 bits | 64 bits |

## Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

## Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

## Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

## Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

**Table 144** Predefined Multicast Address

| MULTICAST ADDRESS | DESCRIPTION |
|---|---|
| FF01:0:0:0:0:0:0:1 | All hosts on a local node. |
| FF01:0:0:0:0:0:0:2 | All routers on a local node. |
| FF02:0:0:0:0:0:0:1 | All hosts on a local connected link. |
| FF02:0:0:0:0:0:0:2 | All routers on a local connected link. |
| FF05:0:0:0:0:0:0:2 | All routers on a local site. |
| FF05:0:0:0:0:0:1:3 | All DHCP severs on a local site. |

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

**Table 145** Reserved Multicast Address

| MULTICAST ADDRESS |
|---|
| FF00:0:0:0:0:0:0:0 |
| FF01:0:0:0:0:0:0:0 |
| FF02:0:0:0:0:0:0:0 |
| FF03:0:0:0:0:0:0:0 |
| FF04:0:0:0:0:0:0:0 |
| FF05:0:0:0:0:0:0:0 |
| FF06:0:0:0:0:0:0:0 |
| FF07:0:0:0:0:0:0:0 |

**Table 145** Reserved Multicast Address (continued)

| MULTICAST ADDRESS |
|---|
| FF08:0:0:0:0:0:0:0 |
| FF09:0:0:0:0:0:0:0 |
| FF0A:0:0:0:0:0:0:0 |
| FF0B:0:0:0:0:0:0:0 |
| FF0C:0:0:0:0:0:0:0 |
| FF0D:0:0:0:0:0:0:0 |
| FF0E:0:0:0:0:0:0:0 |
| FF0F:0:0:0:0:0:0:0 |

## Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

## Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

## EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

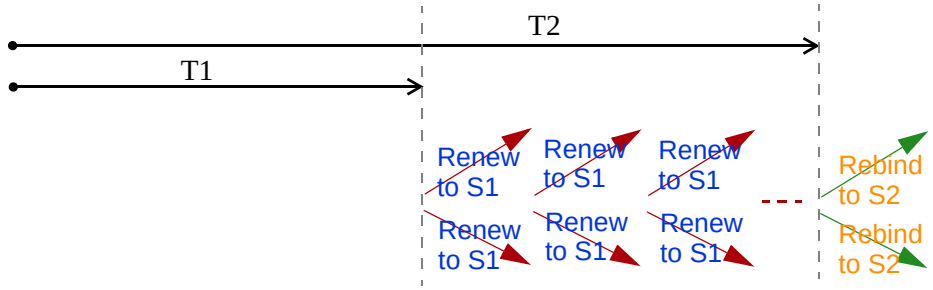
| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **MAC** | 00 | : | 13 | : | 49 | : | 12 | : | 34 | : | 56 | | | | |
| **EUI-64** | 02 | : | 13 | : | 49 | : | FF | : | FE | : | 12 | : | 34 | : | 56 |

## Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If

the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.




## DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

## Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

## ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

## Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.

- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

## IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Device also sends out a neighbor solicitation message. When the Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Device creates an entry in the default router list cache if the router can be used as a default router.

When the Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

## Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

## MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

## Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

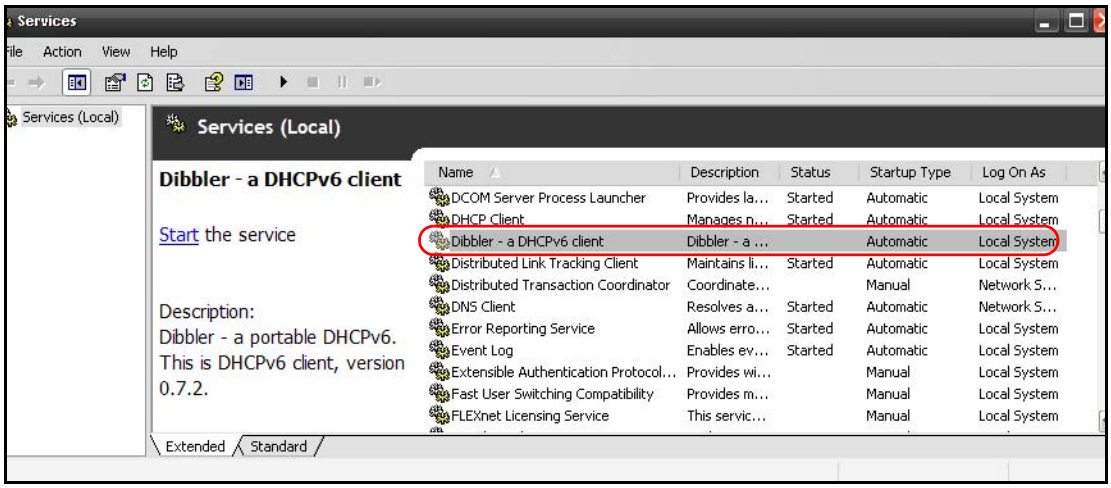
## Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

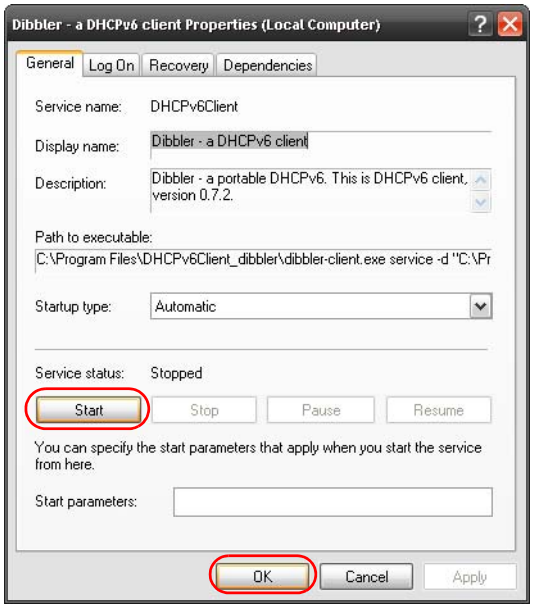
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1. Install Dibbler and select the DHCPv6 client option on your computer.
2. After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.
3. Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.




5 Click **Start** and then **OK**.




6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

## Example - Enabling IPv6 on Windows 7

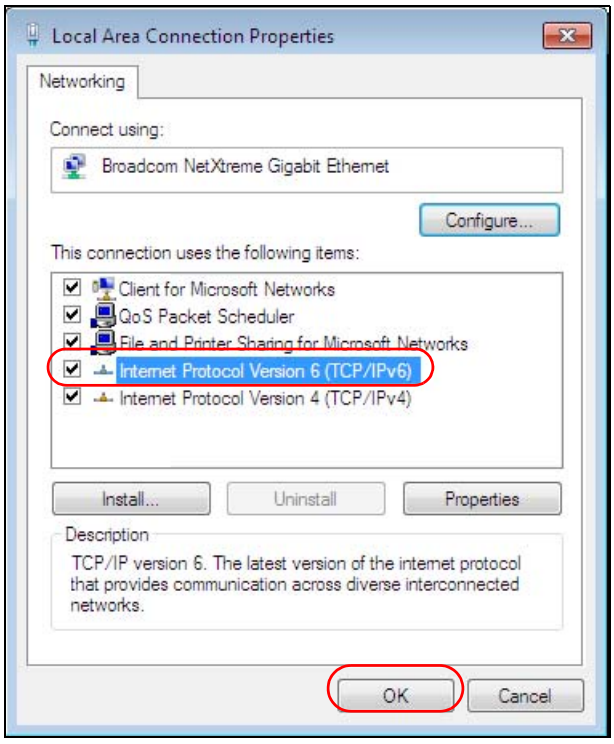
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

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




4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (`2001:b021:2d::1000`) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

F

# Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 146** Examples of Services

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| AH (IPSEC_TUNNEL) | User-Defined | 51 | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| AIM | TCP | 5190 | AOL's Internet Messenger service. |
| AUTH | TCP | 113 | Authentication protocol used by some servers. |
| BGP | TCP | 179 | Border Gateway Protocol. |
| BOOTP_CLIENT | UDP | 68 | DHCP Client. |
| BOOTP_SERVER | UDP | 67 | DHCP Server. |
| CU-SEEME | TCP/UDP<br>TCP/UDP | 7648<br>24032 | A popular videoconferencing solution from White Pines Software. |
| DNS | TCP/UDP | 53 | Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers. |
| ESP (IPSEC_TUNNEL) | User-Defined | 50 | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| FINGER | TCP | 79 | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |
| FTP | TCP<br>TCP | 20<br>21 | File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail. |
| H.323 | TCP | 1720 | NetMeeting uses this protocol. |
| HTTP | TCP | 80 | Hyper Text Transfer Protocol - a client/ server protocol for the world wide web. |
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |
| ICMP | User-Defined | 1 | Internet Control Message Protocol is often used for diagnostic purposes. |
| ICQ | UDP | 4000 | This is a popular Internet chat program. |
| IGMP (MULTICAST) | User-Defined | 2 | Internet Group Multicast Protocol is used when sending packets to a specific group of hosts. |
| IKE | UDP | 500 | The Internet Key Exchange algorithm is used for key distribution and management. |
| IMAP4 | TCP | 143 | The Internet Message Access Protocol is used for e-mail. |
| IMAP4S | TCP | 993 | This is a more secure version of IMAP4 that runs over SSL. |
| IRC | TCP/UDP | 6667 | This is another popular Internet chat program. |
| MSN Messenger | TCP | 1863 | Microsoft Networks' messenger service uses this protocol. |
| NetBIOS | TCP/UDP<br>TCP/UDP<br>TCP/UDP<br>TCP/UDP | 137<br>138<br>139<br>445 | The Network Basic Input/Output System is used for communication between computers in a LAN. |

**Table 146** Examples of Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| NEW-ICQ | TCP | 5190 | An Internet chat program. |
| NEWS | TCP | 144 | A protocol for news groups. |
| NFS | UDP | 2049 | Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments. |
| NNTP | TCP | 119 | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING | User-Defined | 1 | Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3 | TCP | 110 | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |
| POP3S | TCP | 995 | This is a more secure version of POP3 that runs over SSL. |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL (GRE) | User-Defined | 47 | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel. |
| RCMD | TCP | 512 | Remote Command Service. |
| REAL_AUDIO | TCP | 7070 | A streaming audio service that enables real time sound over the web. |
| REXEC | TCP | 514 | Remote Execution Daemon. |
| RLOGIN | TCP | 513 | Remote Login. |
| ROADRUNNER | TCP/UDP | 1026 | This is an ISP that provides services mainly for cable modems. |
| RTELNET | TCP | 107 | Remote Telnet. |
| RTSP | TCP/UDP | 554 | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| SFTP | TCP | 115 | The Simple File Transfer Protocol is an old way of transferring files between computers. |
| SMTP | TCP | 25 | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. |
| SMTPS | TCP | 465 | This is a more secure version of SMTP that runs over SSL. |
| SNMP | TCP/UDP | 161 | Simple Network Management Program. |
| SNMP-TRAPS | TCP/UDP | 162 | Traps for use with the SNMP (RFC:1215). |

**Table 146** Examples of Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| SQL-NET | TCP | 1521 | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSDP | UDP | 1900 | The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP). |
| SSH | TCP/UDP | 22 | Secure Shell Remote Login Program. |
| STRM WORKS | UDP | 1558 | Stream Works Protocol. |
| SYSLOG | UDP | 514 | Syslog allows you to send system logs to a UNIX server. |
| TACACS | UDP | 49 | Login Host Protocol used for (Terminal Access Controller Access Control System). |
| TELNET | TCP | 23 | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. |
| VDOLIVE | TCP<br>UDP | 7000<br>user-defined | A videoconferencing solution. The UDP port number is specified in the application. |

G

# Legal Information

## Copyright



### Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. 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 ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the

corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

### 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.

## 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 the power adaptor or cord 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.

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

## A



## B



## C

## D



## E



## F



## G

## H



## I



## L

## M



## N



## O



## P

## Q



## R



## S

## T



## U



## V



## W