P-870HN-51D

802.11n Wireless VDSL2 4-port Gateway

User's Guide

Default Login Details

IP Address	https://192.168.1.1
User Name	admin
Password	1234

Firmware Version 1.01
Edition 1, 07/2010

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the P-870HN-51D using the web configurator.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Support Disc

  Refer to the included CD for support documents.
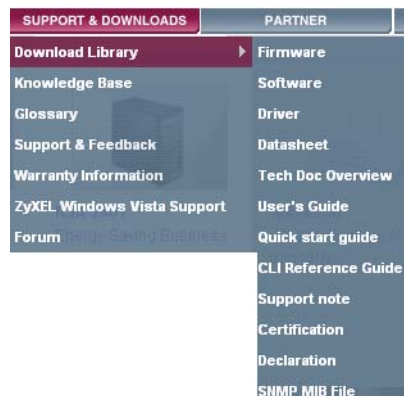
Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.

- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

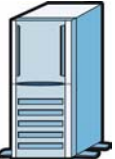**Warnings tell you about things that could harm you or your device.**
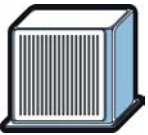
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

• The P-2812HNU-51c may be referred to as the "P-870HN-51D", the "device", the "system" or the "product" in this User's Guide.

• Product labels, screen names, field labels and field choices are all in **bold** font.

• A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.

• "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.

• A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.

• Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.

• "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The P-870HN-51D icon is not an exact representation of your device.

P-870HN-51D	Computer	Notebook computer
Server	DSLAM	Firewall
Telephone	Switch	Router

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.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

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.

Contents Overview

Table of Contents

16

PART I
User's Guide

Introducing the P-870HN-51D

1.1 Overview

The P-870HN-51D is a VDSL2 device that allows super-fast, secure Internet access. It extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices. A range of services such as a firewall and content filtering are also available for secure Internet computing. The P-870HN-51D supports Quality of Service (QoS) to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers.

Please refer to the following description of the product name format.

• "H" denotes an integrated 4-port hub (switch).
• "N" denotes IEEE 802.11n wireless functionality. There is an embedded mini-PCI module for IEEE 802.11b/g/n wireless LAN connectivity.

> **Only use firmware for your P-870HN-51D's specific model. Refer to the label on the bottom of your P-870HN-51D.**

Models ending in "1", for example P-870HN-51D, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service).

See for a full list of features.

1.2 P-870HN-51D for Internet Access

Your P-870HN-51D 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 up to seven WAN services over one VDSL WAN line.

Computers can connect to the P-870HN-51D's LAN ports (or wirelessly).

Figure 1 P-870HN-51D's Internet Access Application
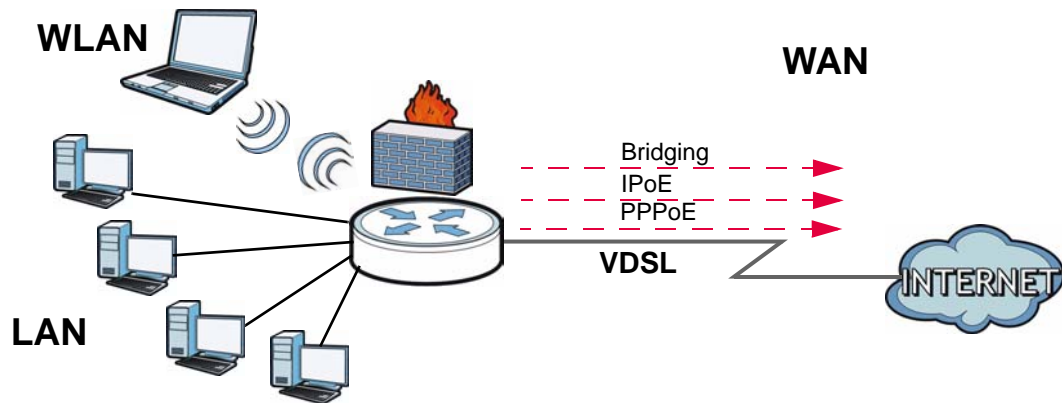
You can also configure the firewall on the P-870HN-51D for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

1.3 Ways to Manage the P-870HN-51D

Use any of the following methods to manage the P-870HN-51D.

• Web Configurator. This is recommended for everyday management of the P-870HN-51D using a (supported) web browser.

• TR-069. This is an auto-configuration server used to remotely configure your device.

1.4 Good Habits for Managing the P-870HN-51D

Do the following things regularly to make the P-870HN-51D more secure and to manage the P-870HN-51D more effectively.

• Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.

• Write down the password and put it in a safe place.

• Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the P-870HN-51D to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the P-870HN-51D. You could simply restore your last configuration.

1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 2   LEDs on the Device
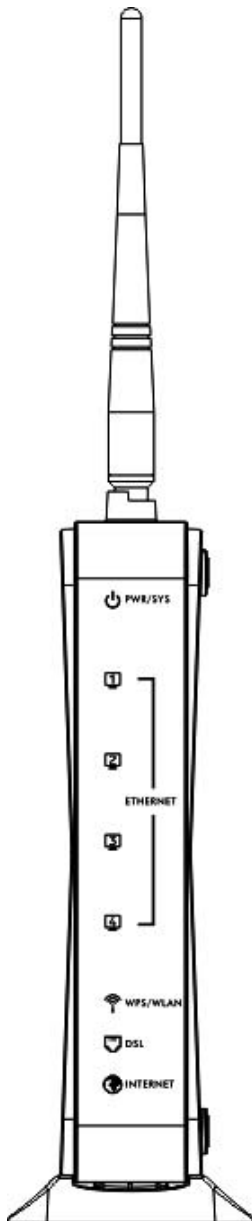
None of the LEDs are on if the P-870HN-51D is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Green	On	The P-870HN-51D is receiving power and ready for use.
		Blinking	The P-870HN-51D is self-testing.
	Red	On	The P-870HN-51D detected an error while self-testing, or there is a device malfunction.
		Off	The P-870HN-51D is not receiving power.
ETHERNET 1-4	Green	On	The P-870HN-51D has a successful 10 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The P-870HN-51D is sending or receiving data to/from the LAN at 10 Mbps.
	Orange	On	The P-870HN-51D has a successful 100 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The P-870HN-51D is sending or receiving data to/from the LAN at 100 Mbps.
		Off	The P-870HN-51D does not have an Ethernet connection with the LAN.
WLAN/ WPS	Green	On	The wireless network is activated and is operating in IEEE 802.11b/g/n mode.
		Blinking	The P-870HN-51D is communicating with other wireless clients at 2 Hz/s.
	Orange	Blinking	The P-870HN-51D is setting up a WPS connection.
		Off	The wireless network is not activated.
DSL	Green	On	The VDSL line is up.
		Blinking	The P-870HN-51D is initializing the VDSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The P-870HN-51D has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The P-870HN-51D is sending or receiving IP traffic.
	Red	On	The P-870HN-51D attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The P-870HN-51D does not have an IP connection.

Refer to the Quick Start Guide for information on hardware connections.

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 "1234".

1.6.1 Using the Reset Button

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

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

1.7 The WPS Button

You can use the **WPS** button on the rear panel of the device to turn the wireless LAN off or on. You can also use it to activate WPS in order to quickly set up a wireless network with strong security. Refer to Section 7.9.4 on page 121 for more information on WPS.

1.7.1 Turn the Wireless LAN Off or On

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

2   Press the **WPS** button for one second and release it. The **WLAN/WPS** LED should change from on to off or vice versa.

1.7.2 Activate WPS

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

2   Select **Active Wireless LAN** and configure the SSID and security settings in the **Network > Wireless LAN** screen. Click **Apply** then.

3   Make sure the **WLAN** LED is on.

4 Press the **WPS** button for more than five seconds and release it. Press the WPS button on another WPS -enabled device within range of the P-870HN-51D. The **WLAN/WPS** LED should flash while the P-870HN-51D sets up a WPS connection with the wireless device.

Note: You must activate WPS in the P-870HN-51D and in another wireless device within two minutes of each other. See Section 7.9.4 on page 121 for more information.

2

Tutorials

2.1 Overview

This chapter describes:

- *How to Set up a Wireless Network on page 27.*
- *Configuring the MAC Address Filter on page 36.*
- *Setting Up NAT Port Forwarding on page 37.*
- *Access the P-870HN-51D Using DDNS on page 38.*
- *Configuring Static Route for Routing to Another Network on page 40.*
- *Configuring QoS Queue and Class Setup on page 43.*

Note: The tutorials featured in this chapter require a basic understanding of connecting to and using the Web Configurator on your P-870HN-51D. For details, see the included Quick Start Guide. For field descriptions of individual screens, see the related technical reference in this User's Guide.

2.2 How to Set up a Wireless Network

This tutorial gives you examples of how to set up an access point and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through an AP wirelessly.

2.2.1 Example Parameters

SSID	SSID_Example3
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
802.11 mode	IEEE 802.11b/g/n Mixed

An access point (AP) or wireless router is referred to as "AP" and a computer with a wireless network card or USB/PCI adapter is referred to as "wireless client" here.

We use the P-870HN-51D web screens and M-302 utility screens as an example. The screens may vary slightly for different models.

2.2.2 Configuring the AP

Follow the steps below to configure the wireless settings on your AP.

1 Open the **Network > Wireless LAN** screen in the AP's web configurator.

Figure 3   AP: Wireless LAN

2 Make sure the **Active Wireless LAN** check box is selected.

3 Enter "SSID_Example3" as the SSID and select **Auto** to have the P-870HN-51D automatically determine a channel which is not used by another AP.

4 Set security mode to **WPA-PSK** and enter "ThisismyWPA-PSKpre-sharedkey" in the **Pre-Shared Key** field. Click **Apply**.

5 Click the **Advanced Setup** tab and select **802.11b/g/n Mixed** in the **802.11 Mode** field. Click **Apply**.

Figure 4 AP: Wireless LAN > Advanced Setup

6 Open the **Status** screen.Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 5 AP: Status

7 Click the **WLAN Station List** hyperlink in the AP's **Status** screen. You can see if any wireless client has connected to the AP.

Figure 6 AP: Status: WLAN Station List

2.2.3 Configuring the Wireless Client

This section describes how to connect the wireless client to a network.

2.2.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.
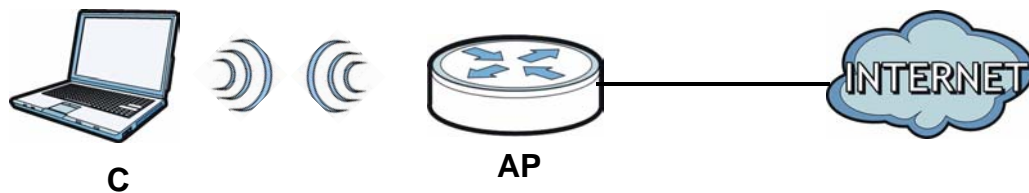
There are three ways to connect the client to an access point.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is "SSID_Example3" and the pre-shared key is "ThisismyWPA-PSKpre-sharedkey".

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

Figure 7 ZyXEL Utility: Site Survey
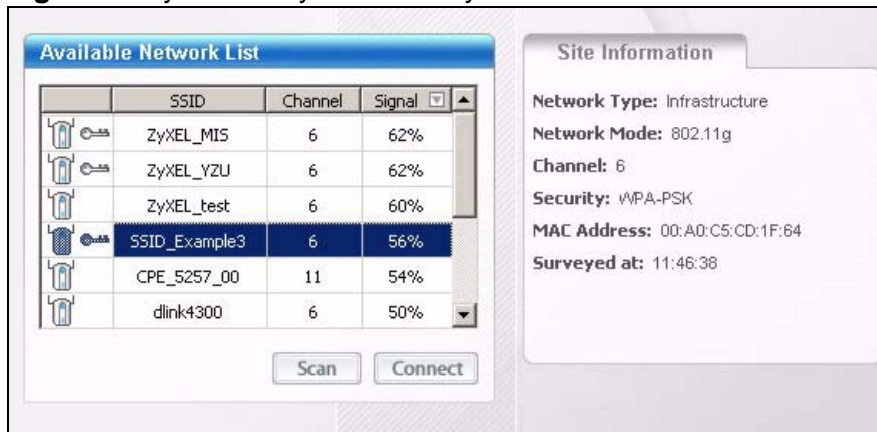
2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.

3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

Figure 8 ZyXEL Utility: Security Settings
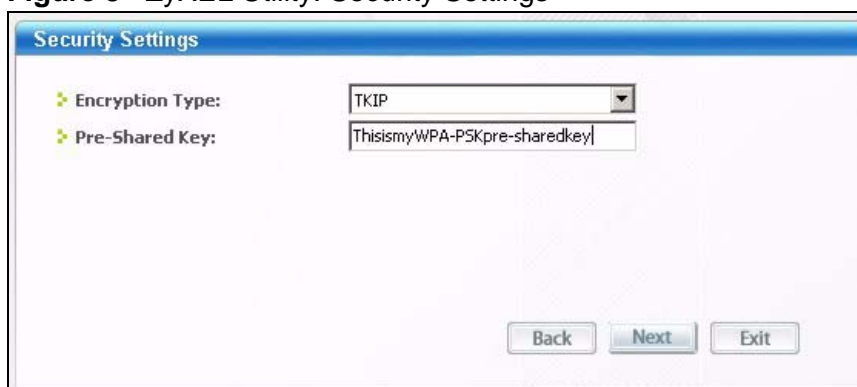
4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 9   ZyXEL Utility: Confirm Save
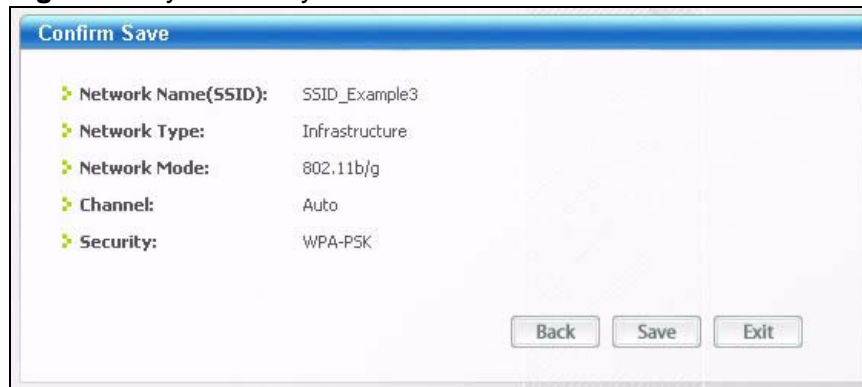
5 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.

Figure 10   ZyXEL Utility: Link Info

6 Open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

2.2.3.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the wireless client. You can also configure different profiles for different

networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the SSID is "SSID_Example3", the profile name is "PN_Example3" and the pre-shared key is "ThisismyWPA-PSKpre-sharedkey". You have chosen the profile name "PN_Example3".

1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.

Figure 11 ZyXEL Utility: Profile
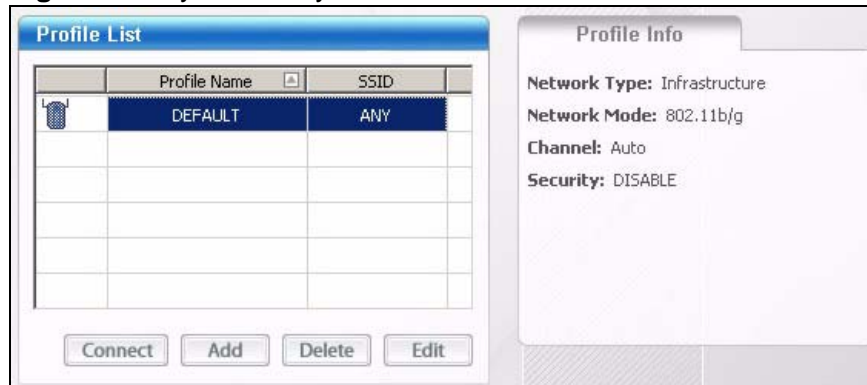
2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. Click on **Scan** if you want to search again. You can also configure your profile for a wireless network that is not in the list.

Figure 12 ZyXEL Utility: Add New Profile
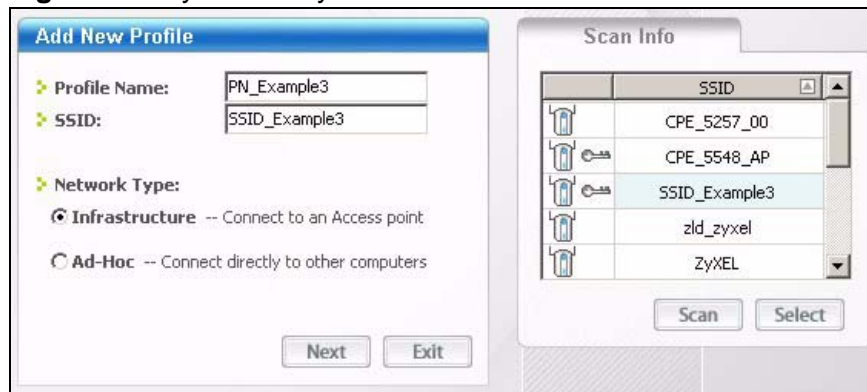
3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

Figure 13   ZyXEL Utility: Profile Security
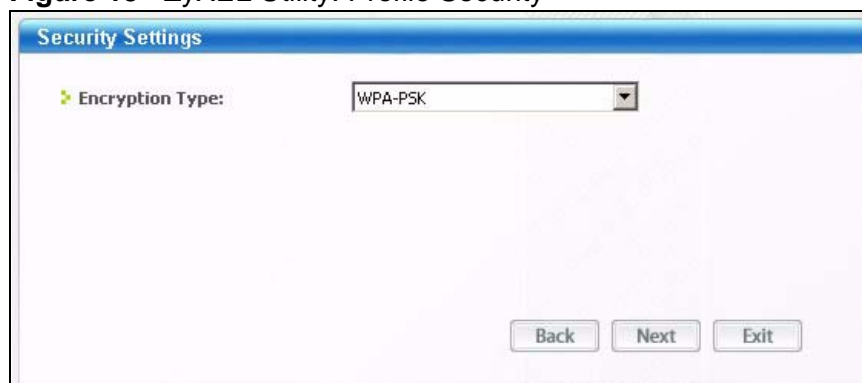
5 This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.

Figure 14   ZyXEL Utility: Profile Encryption
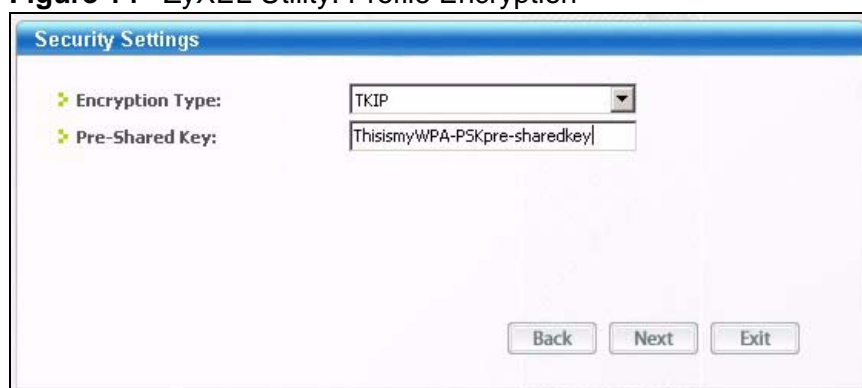
6 In the next screen, leave both boxes checked.

Figure 15   Profile: Wireless Protocol Settings.

7 Verify the profile settings in the read-only screen. Click **Save** to save and go to the next screen.

Figure 16   Profile: Confirm Save
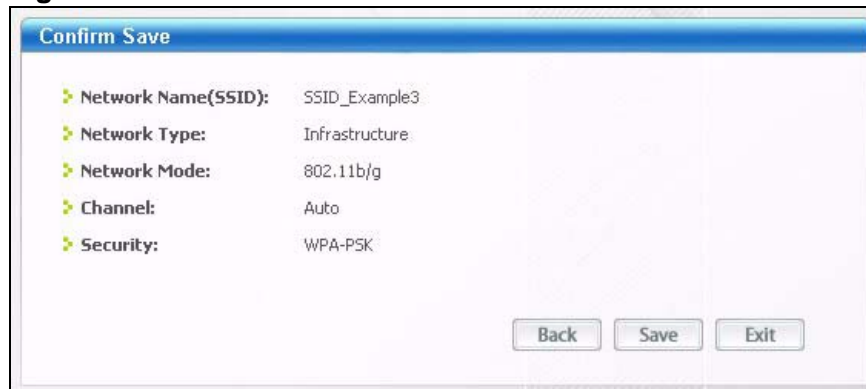
8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

If you clicked **Activate Later**, you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Note: Only one profile can be activated and used at any given time.

Figure 17   Profile: Activate

9 When you activate the new profile, the ZyXEL utility returns to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.

10 Open your Internet browser, enter http://www.zyxel.com or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.

11 If you cannot access the Internet go back to the **Profile** screen, select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

2.3 Configuring the MAC Address Filter

Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the P-870HN-51D. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.
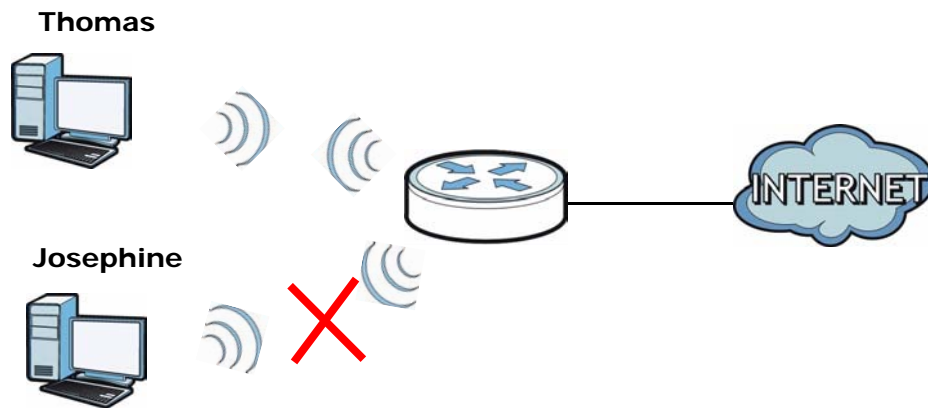
1 Click **Status** > **Client List** to open the following screen. Look for the MAC address of Thomas' computer.

2 Click **Security** > **MAC Filter** to open the **MAC Filter** screen. Select **Active**. Enter the MAC address you found in the **Client List** screen. Click **Apply**.

Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the P-870HN-51D.

2.4 Setting Up NAT Port Forwarding

Thomas recently received an Xbox 360 as his birthday gift. His friends invited him to play online games with them on Xbox LIVE. In order to communicate and play with other gamers on Xbox LIVE, Thomas needs to configure the port settings on his P-870HN-51D.

Xbox 360 requires the following ports to be available in order to operate Xbox LIVE correctly:

  TCP: 53, 80, 3074
  UDP: 53, 88, 3074

Thomas can configure the port settings for Xbox 360.

2.4.1 Port Forwarding

Configure the ports for Xbox 360 by doing the following.

1 Click **Network** > **NAT** > **Port Forwarding** to open the following screen. Select **User define** from the **Service Name** field.

2 Configure the screen as follows to open TCP/UDP port 53 for Xbox 360. Click **Apply**.

3 Repeat steps 2 and 3 to open the rest of the ports for Xbox 360. Use a different service name for each port you want to add The port forwarding settings you configured are listed in the **Port Forwarding** screen.

Thomas can then connect his Xbox 360 to the Internet and play online games with his friends.

2.5 Access the P-870HN-51D Using DDNS

If you connect your P-870HN-51D to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The P-

870HN-51D's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the P-870HN-51D using a domain name.
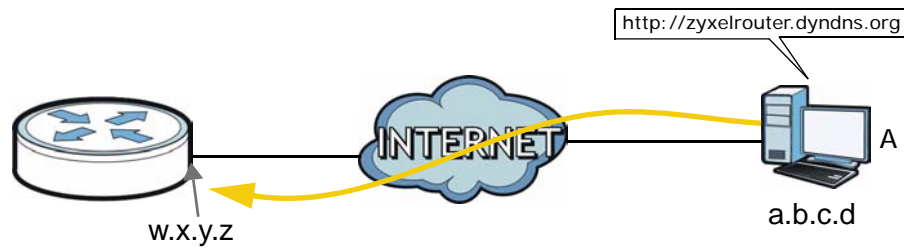
To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial shows you how to:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your P-870HN-51D
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

2.5.1 Registering a DDNS Account on www.dyndns.org

1 Open a browser and type **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

4 Add a new DDNS host name. This tutorial uses the following settings as an example.

- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your P-870HN-51D is currently using. You can find the IP address on the P-870HN-51D's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the P-870HN-51D later.

2.5.2 Configuring DDNS on Your P-870HN-51D

1 Log into the P-870HN-51D's advanced mode.
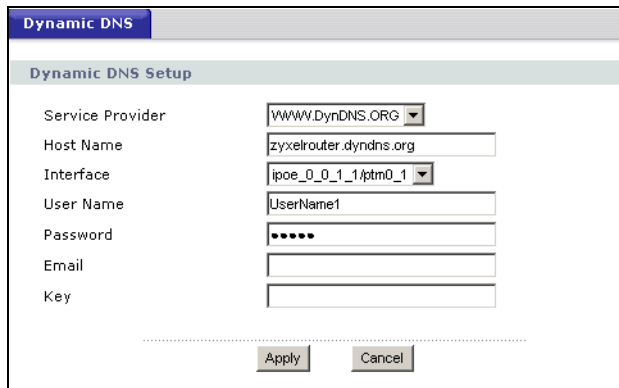
2 Configure the following settings in the **Advanced** > **Dynamic DNS** screen.

2a Select **WWW.DynDNS.ORG** for the **Service Provider**.

2b Type **zyxelrouter.dyndns.org** in the **Host Name** field.

2c Select interface for which the DDNS applies.

2d Enter the user name (**UserName1**) and password (**12345**).

2e Click **Apply**.

2.5.3 Testing the DDNS Setting

Now you should be able to access the P-870HN-51D from the Internet. To test this:

1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

2 Type **http://zyxelrouter.dyndns.org** and press [Enter].

3 The P-870HN-51D's login page should appear. You can then log into the P-870HN-51D and manage it.

2.6 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the P-870HN-51D's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the P-870HN-51D's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the P-870HN-51D's WAN default gateway by default. In this case, **B** will never receive the traffic.
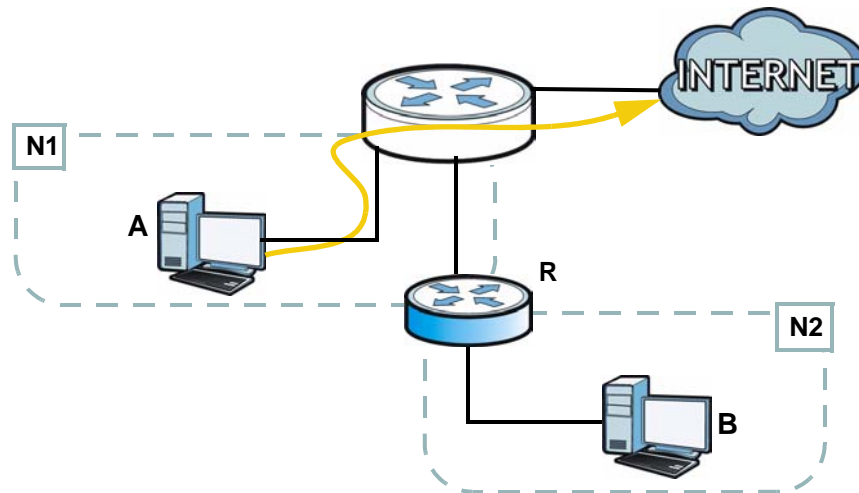
You need to specify a static routing rule on the P-870HN-51D to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the P-870HN-51D routes traffic from **A** to **R** and then **R** routes the traffic to **B**.
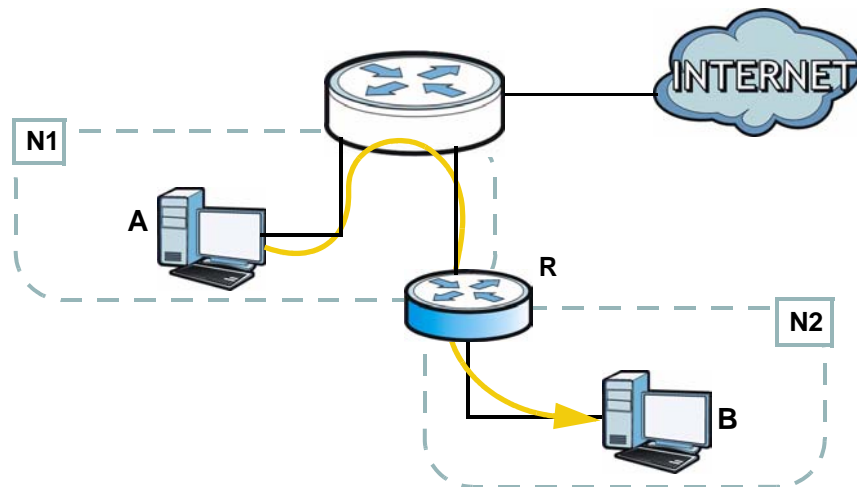
This tutorial uses the following example IP settings:

Table 2 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The P-870HN-51D's WAN	172.16.1.1
The P-870HN-51D's LAN	192.168.1.1
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

1   Log into the P-870HN-51D's Web Configurator in advanced mode.

2   Click **Advanced** > **Static Route**.

3   Click **Add** to add a new rule in the **Static Route** screen.
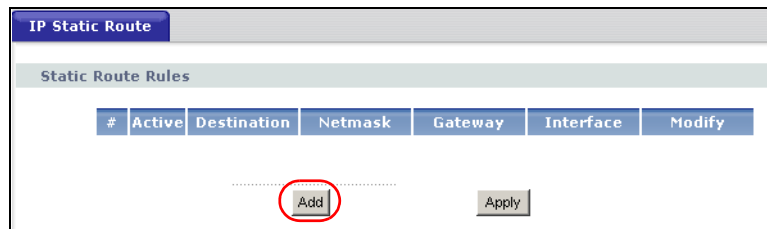
4   Configure the **Static Route Setup** screen using the following settings:

4a   Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination (N2).

4b   Select the WAN interface to which the rule applies. This example uses the default WAN interface.

4c   Select **Gateway Address** and type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.
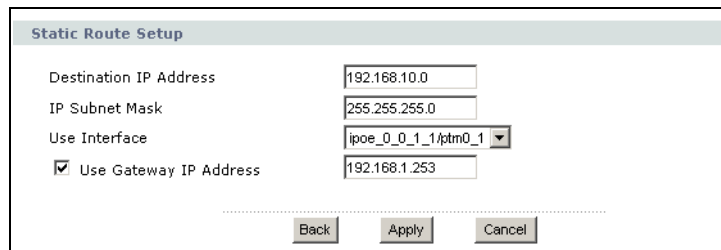
4a   Click **Apply**.

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**′s firewall settings to allow specific traffic to pass through.

2.7 Configuring QoS Queue and Class Setup

This section contains tutorials on how you can configure the QoS screen.

Let′s say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues use the Internet for research, as well as chat applications for communicating with other branch offices.

In the following figure, your Internet connection has an upstream transmission bandwidth of 10,000 kbps. For this example, you want to configure QoS so that e-mail traffic gets the highest priority with at least 5,000 kbps. You can do the following:

• Configure a queue to assign the highest priority queue (7) to e-mail traffic from the LAN interface, so that e-mail traffic would not get delayed when there is network congestion.
• Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to queue 7.

Note: QoS is applied to traffic flowing out of the P-870HN-51D.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the P-870HN-51D.

DSL
10,000 kbps

INTERNET

Your computer
IP=192.168.1.23
and/or
MAC=AA:FF:AA:FF:AA:FF
Email traffic: Highest priority

A colleague's computer
Other traffic: Automatic classifier
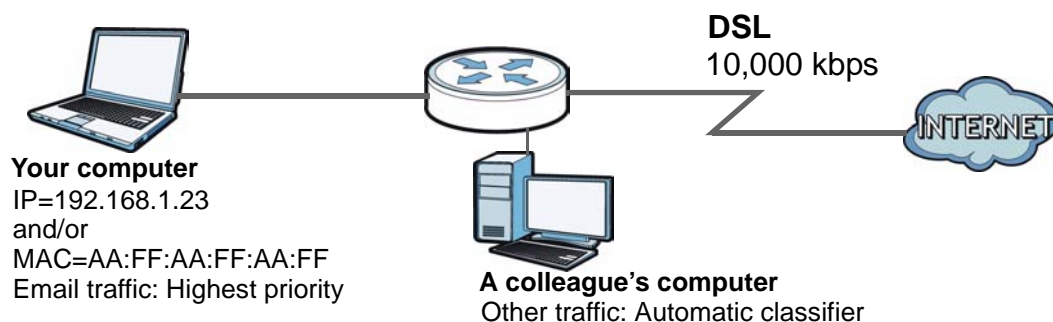
1 Click **Advanced > QoS > General** and check **Active**. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the P-870HN-51D automatically determine this figure).

2 Go to **Advanced > QoS > Queue Setup**. Click **Add** to create a new queue. In the screen that opens, check **Active** and enter or select the following values:

- **Name**: E-mail
- **Interface**: LAN/WLAN
- **Priority**: 4 (High)
- **Weight**: 8
- **Rate Limit**: 5,000 (kbps)

3 Go to **Advanced > QoS > Class Setup**. Click **Add** to create a new class. Check **Active** and follow the settings as shown in the screen below.

Class Name	Give a class name to this traffic, such as **E-mail** in this example.
To Queue	Link this to an item in the **Advanced > QoS > Queue Setup** screen, which is the **E-mail** queue created in this example.
From Interface	This is the interface from which the traffic will be coming from. Select **Local**.
Ether Type	Select **IP** to identify the traffic source by its IP address or MAC address.

MAC Address	Type the MAC address of your computer - **AA:FF:AA:FF:AA:FF**. Type the **MAC Mask** if you know it.
IP Address	Type the IP address of your computer - **192.168.1.23**. Type the **IP Subnet Mask** if you know it.

This maps e-mail traffic coming from port 25 to the highest priority, which you have created in the previous screen (see the **IP Protocol** field). This also maps your computer's IP address and MAC address to the **E-mail** queue (see the **Source** fields).

4 Verify that the queue setup works by checking **Advanced > QoS > Monitor**. This shows the bandwidth alloted to e-mail traffic compared to other network traffic.

Introducing the Web Configurator

3.1 Web Configurator 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 3.6 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

• JavaScripts (enabled by default).

• Java permissions (enabled by default).

See Appendix C on page 299 if you need to make sure these functions are allowed in Internet Explorer.

3.1.1 Accessing the Web Configurator

1   Make sure your P-870HN-51D hardware is properly connected (refer to the Quick Start Guide).

2   Launch your web browser.

3   Type "https://192.168.1.1" as the URL.

4 A password screen displays. Enter the default admin user name **admin** and default admin password **1234**. The password displays in non-readable characters. If you have changed the password, enter your password and click **OK**. Click **Cancel** to revert to the default password in the password field.

Figure 18 Password Screen

3.2 Web Configurator Main Screen

Figure 19 Main Screen
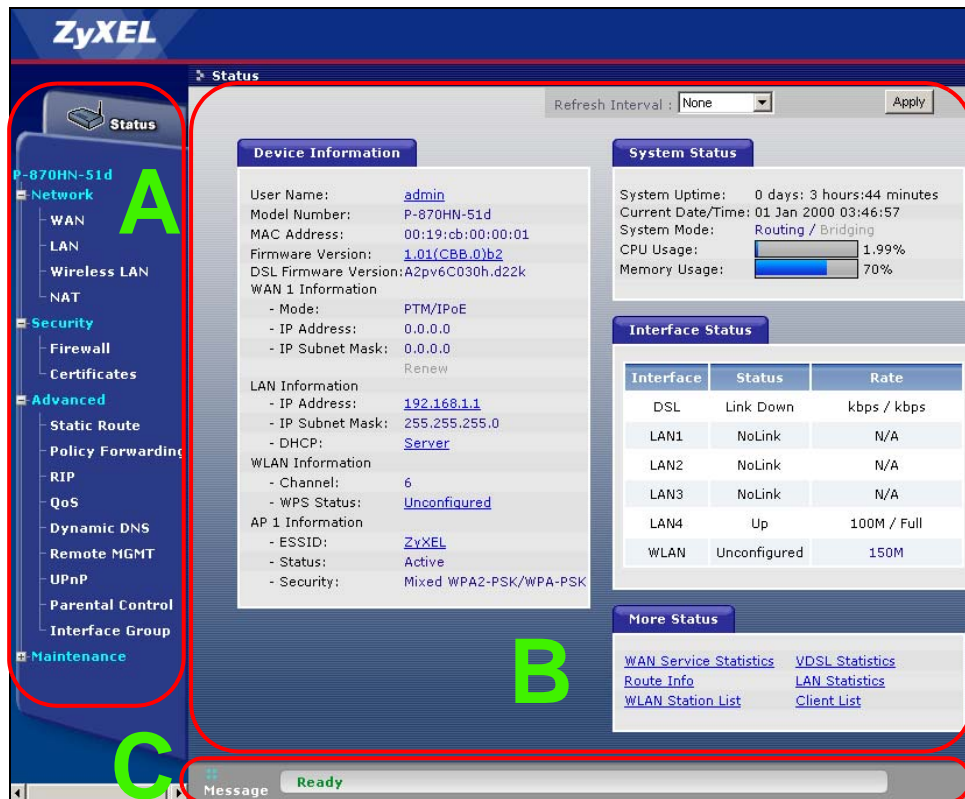
As illustrated above, the main screen is divided into these parts:

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

3.2.1 Navigation Panel

Use the menu items on the navigation panel to open screens to configure P-870HN-51D features. The following tables describe each menu item.

Table 3   Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen shows the P-870HN-51D's general device and network status information. Use this screen to access the statistics and client list.
Network		
WAN	Layer 2 Interface	Use this screen to add or remove a DSL PTM (Packet Transfer Mode) interface.
	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment, and other advanced properties.
LAN	IP	Use this screen to configure LAN TCP/IP, DHCP and IP alias settings.
Wireless LAN	General	Use this screen to configure the wireless LAN settings, WLAN authentication/security settings and MAC filtering rules.
	More AP	Use this screen to configure multiple BSSs on the P-870HN-51D.
	WPS	Use this screen to enable WPS (Wi-Fi Protected Setup) and view the WPS status.
	WPS Station	Use this screen to use WPS to set up your wireless network.
	Advanced Setup	Use this screen to configure the advanced wireless LAN settings.
NAT	Port Forwarding	The **NAT** screens are available only when you enable NAT in a WAN connection. Use this screen to make your local servers visible to the outside world.
	Trigger Port	Use this screen to change your P-870HN-51D's port triggering settings.
	DMZ Host	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 allow SIP sessions to pass through the P-870HN-51D.
Security		
Firewall	Incoming	This screen shows a summary of the IP filtering rules, and allows you to add or remove an incoming IP filtering rule that allows incoming traffic from the WAN.

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Certificate	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.
Advanced		
Static Route	IP Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
Policy Forwarding		Use this screen to configure policy routing on the P-870HN-51D.
RIP		Use this screen to configure RIP (Routing Information Protocol) settings.
QoS	General	Use this screen to enable QoS.
	Queue Setup	Use this screen to configure QoS queues.
	Class Setup	Use this screen to define a classifier.
	Policer Setup	Use this screen to specify the committed rate and committed burst size for incoming packets.
	Monitor	Use this screen to view QoS packets statistics.
Dynamic DNS		This screen allows you to use a static hostname alias for a dynamic IP address.
Remote MGMT	TR069	Use this screen to configure the P-870HN-51D to be managed by an ACS (Auto Configuration Server).
	TR064	Use this screen to enable management via TR-064 on the LAN.
	ServiceControl	Use this screen to configure which services/protocols can access which P-870HN-51D interface.
	IP Address	Use this screen to configure from which IP address(es) users can manage the P-870HN-51D.
UPnP	General	Use this screen to turn UPnP on or off.
Parental Control	Time Restriction	Use this screen to configure the days and times when the restrictions are enforced.
	URL Filter	Use this screen to prevent users of your netowrk from viewing inappropriate web content.
Interface Group		Use this screen to map a port to a PVC or bridge group.
Maintenance		
System	General	Use this screen to configure your device's name, domain name, management inactivity timeout and password.
	Time Setting	Use this screen to change your P-870HN-51D's time and date.
Logs	View Log	Use this screen to view the logs for the level that you selected.
	Log Settings	Use this screen to change your P-870HN-51D's log settings.
Tools	Firmware	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.
	Restart	This screen allows you to reboot the P-870HN-51D without turning the power off.

Table 3   Navigation Panel Summary

LINK	TAB	FUNCTION
Diagnostic	General	Use this screen to test the connections to other devices.
	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.

3.2.2 Main Window

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

Right after you log in, the **Status** screen is displayed. See for more information about the **Status** screen.

3.2.3 Status Bar

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

PART II
Technical Reference

Status Screens

4.1 Overview

Use the **Status** screens to look at the current status of the device, system resources and interfaces (LAN, WAN and WLAN). The **Status** screen also provides detailed information from DHCP and statistics from traffic.

4.2 Status Screen

Click **Status** to open this screen.

Figure 20   Status Screen

Each field is described in the following table.

Table 4 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the P-870HN-51D to update this screen.
Apply	Click this to update this screen immediately.
Device Information	
User Name	This field displays the P-870HN-51D system name. It is used for identification. Click this to go to the screen where you can change it.
Model Number	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your P-870HN-51D.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
DSL Firmware Version	This field displays the current version of the device's DSL modem code.
WAN Information	
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the P-870HN-51D in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
LAN Information	
IP Address	This field displays the current IP address of the P-870HN-51D in the LAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the P-870HN-51D is providing to the LAN. Choices are: **Server** - The P-870HN-51D is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The P-870HN-51D acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The P-870HN-51D is not providing any DHCP services to the LAN. Click this to go to the screen where you can change it.
WLAN Information	
Channel	This is the channel number used by the P-870HN-51D now.

Table 4 Status Screen

LABEL	DESCRIPTION
WPS Status	This field displays the status of WPS (Wi-Fi Protected Setup). Click this to go to the screen where you can change it.
AP Information	
ESSID	This is the descriptive name used to identify the P-870HN-51D in this wireless network. Click this to go to the screen where you can change it.
Status	This shows the current status of the wireless network.
Security	This shows the level of wireless security the P-870HN-51D is using in this wireless network.
System Status	
System Uptime	This field displays how long the P-870HN-51D has been running since it last started up. The P-870HN-51D starts up when you plug it in, when you restart it (**Maintenance > Tools > Restart**), or when you reset it (see Section 1.6 on page 25).
Current Date/Time	This field displays the current date and time in the P-870HN-51D. You can change this in **Maintenance > System > Time Setting**.
System Mode	This displays whether the P-870HN-51D is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the P-870HN-51D's processing ability is currently used. When this percentage is close to 100%, the P-870HN-51D 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 14 on page 169).
Memory Usage	This field displays what percentage of the P-870HN-51D's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the P-870HN-51D is probably becoming unstable, and you should restart the device. See Section 22.4 on page 232, or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the P-870HN-51D has.
Status	This field indicates whether or not the P-870HN-51D is using the interface. For the DSL interface, this field displays **LinkDown** (line is down) or **Up** (line is up or connected). For the LAN or Ethernet WAN interface, this field displays **Up** when the P-870HN-51D is using the interface and **NoLink** when the line is disconnected. For the WLAN interface, it displays **Up** when WLAN is enabled or **Disabled** when WLAN is not active.

Table 4   Status Screen

LABEL	DESCRIPTION
Rate	For the DSL interface, it displays the downstream and upstream transmission rate.
	For the LAN or Ethernet WAN interface, this displays the port speed and duplex setting.
	For the WLAN interface, it displays the maximum transmission rate.
More Status	
WAN Service Statistics	Click this link to view packet specific statistics of the WAN connection(s). See Section 4.2.1 on page 58.
Route Info	Click this link to view the internal routing table on the P-870HN-51D. See Section 4.2.2 on page 60.
WLAN Station List	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the P-870HN-51D. See Section 4.2.3 on page 61.
VDSL Statistics	Click this to check the VDSL status and detailed performance data.
LAN Statistics	Click this link to view packet specific statistics on the LAN and WLAN interfaces. See Section 4.2.5 on page 66.
Client List	Click this link to view current DHCP client information. See Section 4.2.6 on page 66.

4.2.1 WAN Service Statistics

Click **Status > WLAN Service Statistics** to access this screen. Use this screen to view the WAN statistics.

Figure 21   Status > WAN Service Statistics

The following table describes the labels in this screen.

Table 5 Status > WAN Service Statistics

LABEL	DESCRIPTION
Interface	This shows the name of the WAN interface used by this connection. A default name **ipoa0**, **pppoa1, atmx** (where x starts from 0 and is the index number of ATM layer-2 interfaces using different VPI and/or VCI values) or **ptm0** indicates the DSL port. The **pppx** name (where x starts from 0 and is the index number of PPP connection on the P-870HN-51D) indicates a PPP connection via any one of the WAN interface. **eth4** indicates the Ethernet WAN interface (the physical Ethernet WAN port). The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection. The number after the underscore (**_**) represents the index number of connections through the same interface. **(null)** means the entry is not valid.
Description	This shows the descriptive name of this connection. **0** and **35** or **0** and **1** are the default VPI and VCI numbers. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection. **(null)** means the entry is not valid.
Received	
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.
Drops	This indicates the number of outgoing packets dropped on this interface.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.

4.2.2 Route Info

Routing is based on the destination address only and the P-870HN-51D takes the shortest path to forward a packet. Click **Status > Route Info** to access this screen. Use this screen to view the internal routing table on the P-870HN-51D.

Figure 22 Status > Route Info

The following table describes the labels in this screen.

Table 6 Status > Route Info

LABEL	DESCRIPTION
Destination	This indicates the destination IP address of this route.
Gateway	This indicates the IP address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of this route.
Flag	This indicates the route status.
	Up: The route is up.
	!(Reject): The route is blocked and will force a route lookup to fail.
	Gateway: The route uses a gateway to forward traffic.
	Host: The target of the route is a host.
	Reinstate: The route is reinstated for dynamic routing.
	Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect
	Modified (redirect): The route is modified from a routing daemon or rederict.
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".

Table 6 Status > Route Info (continued)

LABEL	DESCRIPTION
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. • **br0** indicates the LAN interface. • **ptm0** indicates the VDSL WAN interface using IPoE or in bridge mode. • **pppoa1** indicates the ADSL WAN interface using PPPoA. • **ipoa0** indicates the ADSL WAN interface using IPoA. • **ppp0** indicates the WAN interface using PPPoE. • **eth4** indicates the Ethernet WAN interface using IPoE.

4.2.3 WLAN Station List

Click **Status > WLAN Station List** to access this screen. Use this screen to view the wireless stations that are currently associated to the P-870HN-51D.

Figure 23 Status > WLAN Station List

The following table describes the labels in this screen.

Table 7 Status > WLAN Station List

LABEL	DESCRIPTION
MAC	This field shows the MAC (Media Access Control) address of an associated wireless station.
SSID	This field shows the SSID to which the wireless station is connected.
Interface	This field shows the wireless interface to which the wireless station is connected.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.

4.2.4 VDSL Statistics

Click **Status > VDSL Statistics** to open the following screen. Use this screen to check VDSL status and detailed performance data.

Figure 24   Status > VDSL Statistics
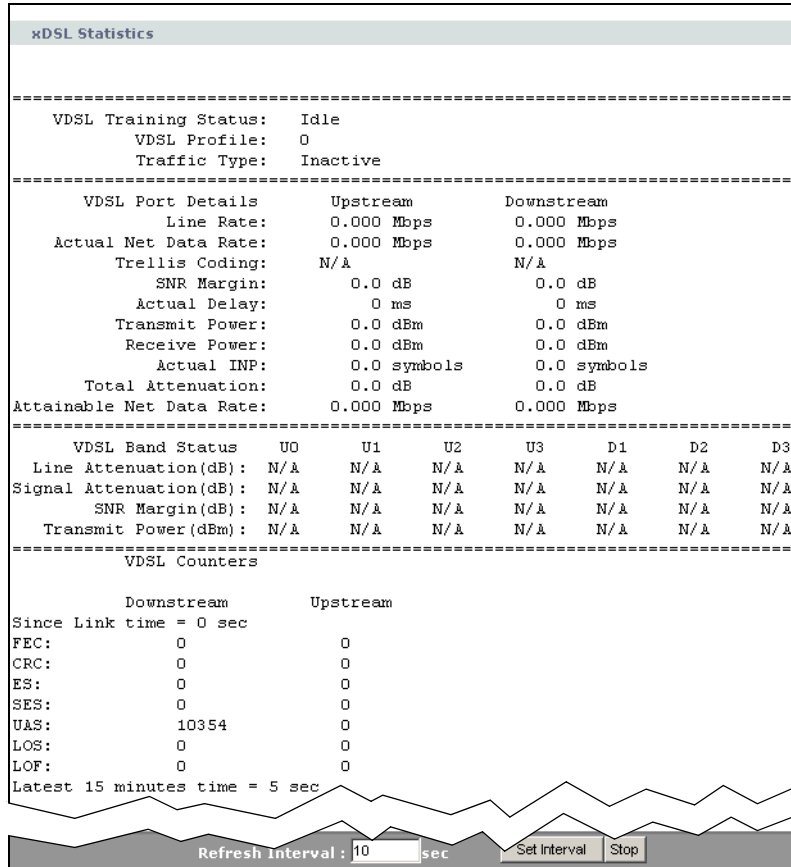
The following table describes the labels in this screen.

Table 8   Status > VDSL Statistics

LABEL	DESCRIPTION
VDSL Training Status	This shows whether the DSL port is connected (**Showtime**); idle (**Idle**); not connected; is negotiating a connection with a COE device (**G.994 Training**); is under loop test (**RUN_LD_INIT**); or under channel analysis(**G.922 Channel Analysis**).
VDSL Profile	This shows the name of the VDSL profile which is applied to the VDSL port to which the P-870HN-51D is connected.
Traffic Type	This indicates whether the PTM interface is active (**PTM Mode**) or inactive (**Inactive**).

Table 8   Status > VDSL Statistics (continued)

LABEL	DESCRIPTION
VDSL Port Details	
These are the maximum **Upstream** and **Downstream** transfer rates for the ports that belong to this profile. Upstream traffic refers to traffic from the P-870HN-51D to the Central Organization Equipment (COE). Downstream traffic refers to traffic from the COE to the P-870HN-51D.	
Line Rate	This indicates the maximum upstream/downstream net data rate currently attainable on this line.
Actual Net Line Rate	This indicates the actual upstream/downstream data transmission rate.
Trellis Coding	Trellis coding is a modulation scheme which allows highly efficient transmission of information over band-limited channels such as telephone lines. **N/A** means Trellis coding is disabled or not used on the P-870HN-51D.
SNR Margin	This indicates the upstream/downstream SNR margin.
Actual Delay	This indicates the actual upstream/downstream transmission delay (in milliseconds).
Transmit Power	This indicates the upstream/downstream transmission power of the line.
Receive Power	This indicates the upstream/downstream receiving power of the line.
Actual INP	This indicates the actual impulse noise protection (INP).
Total Attenuation	This indicates the upstream/downstream attenuation.
Attainable Net Data Rate	This indicates the maximum upstream/downstream net data rate currently attainable on this line.
VDSL Band Status	The fields in this section indicate the status for upstream bands 0, 1, 2, 3 (**U0**, **U1**, **U2**, **U3**) and downstream bands 1, 2, 3 (**D1**, **D2**, **D3**).
Line Attenuation	This indicates the line attenuation status for each upstream and downstream band. **NA** displays when the band is not used.
Signal Attenuation	This indicates the signal attenuation status for each upstream and downstream band. **NA** displays when the band is not used.
SNR Margin	This indicates the signal to noise ratio for each upstream and downstream band. **NA** displays when the band is not used.
Transmit Power	This indicates the line transmission power for each upstream and downstream band. **NA** displays when the band is not used.
Since Link time	This indicates VDSL performance information recorded since the connection is up.
FEC	This indicates the number of Forward Error Correction Seconds (FECs) failures since the last reset.
CRC	This indicates the number of CRC (Cyclic Redundant Check) error(s) since the last reset.
ES	This indicates the number of port endpoint errored seconds (ESs) since the last reset.
SES	This indicates the number of port endpoint severely errored seconds (SESs) since the last reset.

63

Table 8 Status > VDSL Statistics (continued)

LABEL	DESCRIPTION
UAS	This indicates the number of UnAvailable Seconds (UAS) since the last reset.
LOS	This indicates the number of Loss of Signal (LOS) failures since the last reset.
LOF	This indicates the number of Loss of Framing (LOF) failures since the last reset.
Latest 15 minutes time	This indicates VDSL performance information recorded since the last 15 minute time segment.
FEC	This indicates the number of Forward Error Correction Seconds (FECs) failures since the last 15 minute time segment.
CRC	This indicates the number of CRC (Cyclic Redundant Check) error(s) since the last 15 minute time segment.
ES	This indicates the number of port endpoint errored seconds (ESs) since the last 15 minute time segment.
SES	This indicates the number of port endpoint severely errored seconds (SESs) since the last 15 minute time segment.
UAS	This indicates the number of UnAvailable Seconds (UAS) since the last 15 minute time segment.
LOS	This indicates the number of Loss of Signal (LOS) failures since the last 15 minute time segment.
LOF	This indicates the number of Loss of Framing (LOF) failures since the last 15 minute time segment.
Previous 15 minutes time	This indicates VDSL performance information recorded within the last 15 minute time segment.
FEC	This indicates the number of Forward Error Correction Seconds (FECs) failures within the last 15 minute time segment.
CRC	This indicates the number of CRC (Cyclic Redundant Check) error(s) within the last 15 minute time segment.
ES	This indicates the number of port endpoint errored seconds (ESs) within the last 15 minute time segment.
SES	This indicates the number of port endpoint severely errored seconds (SESs) within the last 15 minute time segment.
UAS	This indicates the number of UnAvailable Seconds (UAS) within the last 15 minute time segment.
LOS	This indicates the number of Loss of Signal (LOS) failures within the last 15 minute time segment.
LOF	This indicates the number of Loss of Framing (LOF) failures within the last 15 minute time segment.
Latest 1 day time	This indicates VDSL performance information recorded since the last 1-day period.
FEC	This indicates the number of Forward Error Correction Seconds (FECs) failures since the last 1-day period.
CRC	This indicates the number of CRC (Cyclic Redundant Check) error(s) since the last 1-day period.

Table 8 Status > VDSL Statistics (continued)

LABEL	DESCRIPTION
ES	This indicates the number of port endpoint errored seconds (ESs) since the last 1-day period.
SES	This indicates the number of port endpoint severely errored seconds (SESs) since the last 1-day period.
UAS	This indicates the number of UnAvailable Seconds (UAS) since the last 1-day period.
LOS	This indicates the number of Loss of Signal (LOS) failures since the last 1-day period.
LOF	This indicates the number of Loss of Framing (LOF) failures since the last 1-day period.
Previous1 day time	This indicates VDSL performance information recorded in the past one day.
FEC	This indicates the number of Forward Error Correction Seconds (FECs) failures in the past one day.
CRC	This indicates the number of CRC (Cyclic Redundant Check) error(s) in the past one day.
ES	This indicates the number of port endpoint errored seconds (ESs) in the past one day.
SES	This indicates the number of port endpoint severely errored seconds (SESs) in the past one day.
UAS	This indicates the number of UnAvailable Seconds (UAS) in the past one day.
LOS	This indicates the number of Loss of Signal (LOS) failures in the past one day.
LOF	This indicates the number of Loss of Framing (LOF) failures in the past one day.
Total time	This indicates the number of packets transmitted/received through the VDSL connection since the last reset.
FEC	This indicates the number of Forward Error Correction Seconds (FECs) failures since the connection is up.
CRC	This indicates the number of CRC (Cyclic Redundant Check) error(s) since the connection is up.
ES	This indicates the number of port endpoint errored seconds (ESs) since the connection is up.
SES	This indicates the number of port endpoint severely errored seconds (SESs) since the connection is up.
UAS	This indicates the number of UnAvailable Seconds (UAS) since the connection is up.
LOS	This indicates the number of Loss of Signal (LOS) failures since the connection is up.
LOF	This indicates the number of Loss of Framing (LOF) failures since the connection is up.

4.2.5 LAN Statistics

Click **Status > LAN Statistics** to access this screen. Use this screen to view the LAN statistics.

Figure 25   Status > LAN Statistics

The following table describes the labels in this screen.

Table 9   Status > LAN Statistics

LABEL	DESCRIPTION
Interface	This shows the LAN or WLAN interface.
Received	
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.
Drops	This indicates the number of outgoing packets dropped on this interface.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Refresh Interval** field.
Stop	Click **Stop** to stop refreshing statistics.

4.2.6 Client List

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the P-870HN-51D as a DHCP server or disable it. When configured as a server, the P-870HN-51D provides the TCP/IP configuration for the clients. If

DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Status > Client List** to open the following screen. The read-only DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the P-870HN-51D's DHCP server.

Figure 26   Status > Client List

The following table describes the labels in this screen.

Table 10   Status > Client List

LABEL	DESCRIPTION
Host Name	This indicates the computer host name.
MAC Address	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. This indicates the MAC address of the client computer.
IP Address	This indicates the IP address assigned to this client computer.

5

WAN Setup

5.1 Overview

This chapter discusses the P-870HN-51D's **WAN** screens. Use these screens to configure your P-870HN-51D for Internet access.

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

Figure 27   LAN and WAN
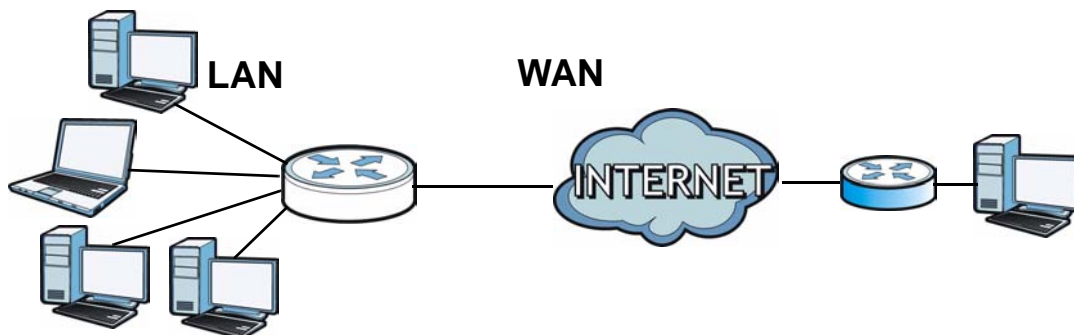
See Section 5.6 on page 84 for advanced technical information on WAN.

5.1.1 What You Can Do in this Chapter

• The **Layer 2 Interface** screen lets you view, remove or add a layer-2 WAN interface (Section 5.4 on page 71).

• The **Internet Connection** screen lets you view and configure the WAN settings on the P-870HN-51D for Internet access (Section 5.5 on page 73).

Table 11 WAN Setup Overview

LAYER-2 INTERFACE		INTERNET CONNECTION	
INTERFACE	CONNECTION MODE	WAN SERVICE TYPE	CONNECTION SETTINGS
PTM	Default Mode VLAN MUX Mode MSC Mode	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
		IPoE	WAN IP address, NAT, DNS server and default gateway
		Bridging	N/A

5.2 What You Need to Know

Encapsulation Method

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

WAN IP Address

The WAN IP address is an IP address for the P-870HN-51D, which makes it accessible from an outside network. It is used by the P-870HN-51D to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the P-870HN-51D tries to access the Internet.

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

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.

5.3 Before You Begin

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

5.4 The Layer 2 Interface Screen

The P-870HN-51D must have a layer-2 interface to allow users to use the DSL port to access the Internet.

Figure 28   Layer 2 Interface

The following table describes the fields in this screen.

Table 12   Layer 2 Interface

LABEL	DESCRIPTION
Interface	This is the name of the interface.
Connection Mode	This displays the connection mode of the layer-2 interface.
QoS	This displays whether QoS (Quality of Service) is enabled on the P-870HN-51D.
Remove	Click the **Remove** button to delete this interface from the P-870HN-51D. A window displays asking you to confirm that you want to delete the interface. Note: You cannot remove the layer-2 interface when a WAN service is associated with it.
Add	Click this button to create a new layer-2 interface.

5.4.1 Layer 2 Interface Configuration

Click the **Add** button in the **Layer 2 Interface** screen to open the following screen. Use this screen to create a new layer-2 interface. At the time of writing, you can configure only one PTM layer-2 interface on the P-870HN-51D.

Figure 29   Layer 2 Interface Configuration: DSL PTM WAN

The following table describes the fields in this screen.

Table 13   Layer 2 Interface Configuration

LABEL	DESCRIPTION
Select Connection Mode	Select **Default Mode** to allow only one WAN service over a single virtual circuit. Select **MSC Mode** to allow multiple WAN services over a single virtual circuit. Each WAN connection has its own MAC address. Select **VLAN MUX Mode** to allow multiplexing of multiple protocols over a single virtual circuit. You need to assign a VLAN ID and priority level to traffic through each WAN connection. All WAN connections share one MAC address.
Enable Quality Of Service	Select this option to activate QoS (Quality of Service) on this interface to group and prioritize traffic. Traffic is grouped according to the VLAN group. The QoS setting applies to all WAN connections over the same PVC.
Back	Click this button to return to the previous screen without saving any changes.
Apply/Save	Click this button to save your changes and go back to the previous screen.

5.5 The Internet Connection Screen

Use this screen to change your P-870HN-51D's WAN settings. Click **Network > WAN > Internet Connection**. The summary table shows you the configured WAN services (connections) on the P-870HN-51D.

To use NAT, firewall or IGMP proxy in the P-870HN-51D, you need to configure a WAN connection with PPPoE or IPoE.

Note: When a layer-2 interface is in **VLAN MUX Mode** or **MSC Mode**, you can configure up to eight WAN services for each interface.

Figure 30   Internet Connection

The following table describes the labels in this screen.

Table 14   Internet Connection

LABEL	DESCRIPTION
Interface	This shows the name of the interface used by this connection.
	A default name **ipoa0**, **pppoa1** or **ptm0** indicates the DSL port. The **pppx** name (where x starts from 0 and is the index number of PPP connection on the P-870HN-51D) indicates a PPP connection.
	The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection. The number after the underscore (**_**) represents the index number of connections through the same interface.
	(null) means the entry is not valid.
Description	This is the service name of this connection.
	0 and **35** or **0** and **1** are the default VPI and VCI numbers. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection.
	(null) means the entry is not valid.
Type	This shows the layer-2 interface type and method of encapsulation used by this connection.
Rate	This shows the maximum data rate (in Kbps) allowed for traffic sent through this connection. This displays **N/A** when there is no limit on transmission rate.

Table 14 Internet Connection

LABEL	DESCRIPTION
Vlan8021p	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.
VlanMuxId	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.
ConnId	This shows the index number of each connection. This displays **N/A** when the interface used by the connection is in **Default Mode**.
IGMP	This shows whether IGMP (Internet Group Multicast Protocol) is activated or not for this connection. IGMP is not available when the connection uses the bridging service.
NAT	This shows whether NAT is activated or not for this interface. NAT is not available when the connection uses the bridging service.
Firewall	This shows whether the firewall is activated or not for this connection. The firewall is not available when the connection uses the bridging service.
Modify	Click the **Edit** icon to configure the WAN connection. Click the **Remove** icon to delete the WAN connection.
Add	Click **Add** to create a new connection.

5.5.1 WAN Connection Configuration

Click the **Edit** or **Add** button in the **WAN Service** screen to configure a WAN connection.

5.5.1.1 WAN Interface

This screen displays when you add a new WAN connection.

Figure 31   WAN Configuration: WAN Interface

The following table describes the labels in this screen.

Table 15   WAN Configuration: WAN Interface

LABEL	DESCRIPTION
Select a layer 2 interface for this service	Select a PTM interface to use the DSL port as the WAN port and use the VDSL technology for data transmission.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.2 Service Type

Use this screen to configure how you want the P-870HN-51D to connect to the Internet.

Figure 32   WAN Configuration: Service Type

The following table describes the labels in this screen.

Table 16   WAN Configuration: Service Type

LABEL	DESCRIPTION
Select WAN service type	Select the method of encapsulation used by your ISP. Choices are **PPP over Ethernet (PPPoE)**, **IP over Ethernet** and **Bridging**.
Enter Service Description	Specify a name for this connection or use the automatically generated one.

Table 16 WAN Configuration: Service Type

LABEL	DESCRIPTION
Rate Limit	Enter the maximum transmission rate in Kbps for traffic sent through the WAN connection. Otherwise, leave this field blank to disable the rate limit. This field is not available for an ATM connection.
MTU [1-1500]	Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the P-870HN-51D divides it into smaller fragments. Allowed values are 1 - 1500. Usually, this value is 1500.
Tag VLAN ID for egress packets	Select this option to add the VLAN tag (specified below) to the outgoing traffic through this connection. This field is available when the Connect interface is in **VLAN MUX** mode.
Enter 802.1P Priority	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. This field is available when the Connect interface is in **VLAN MUX** mode.
Enter 802.1Q VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection. This field is available when the PTM interface is in **VLAN MUX** mode.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.3 WAN IP Address and DNS Server

The screen differs by the encapsulation you selected in the previous screen. See for more information.

PPPoE

This screen displays when you select **PPP over Ethernet (PPPoE)** in the **WAN Service Configuration** screen.

Figure 33   WAN Configuration: PPPoE

The following table describes the labels in this screen.

Table 17   WAN Configuration: PPPoE

LABEL	DESCRIPTION
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.
PPPoE Service Name	Type the name of your PPPoE service here.

Table 17 WAN Configuration: PPPoE

LABEL	DESCRIPTION
Authentication Method	The P-870HN-51D supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO** - Your P-870HN-51D accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your P-870HN-51D accepts CHAP only. **PAP** - Your P-870HN-51D accepts PAP only. **MSCHAP** - Your P-870HN-51D accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.
Enable NAT	Select this option to enable NAT on the P-870HN-51D. You can also select the **NAT Type** you want the P-870HN-51D to implement. The choices are as follows: • **Symmetric NAT (default)** - Symmetric NAT maps requests from the same private IP address and port to a different public source IP address and/or port depending on the packet's destination IP address. • **Port Restricted Cone NAT** - Restricted cone NAT maps all requests from the same private IP address and port to the same public source IP address and port. • **Restricted Cone NAT** - Restricted cone NAT maps all requests from the same private IP address to the same public source IP address. • **Full Cone NAT** - In full cone NAT, all requests from the same private IP address and port are mapped to the same public source IP address and port. Someone on the Internet only needs to know the mapping scheme in order to send packets to a device behind the NAT router.
Dial on Demand	Select this check box when you do not want the connection up all the time and specify an idle time-out in the **Inactivity Timeout** field.
Inactivity Timeout	Specify an idle time-out when you select **Dial on Demand**. The default setting is 0, which means the Internet session will not timeout.
Use Static IPv4 Address	A static IPv4 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 want to use a static IP address instead of a dynamic IP address.
IPv4 Address	Enter the static IP address provided by your ISP.
Enable PPP Debug Mode	Select this option to display PPP debugging messages on the console.

Table 17 WAN Configuration: PPPoE

LABEL	DESCRIPTION
Bridge PPPoE Frames Between WAN and Local Ports	Select this option to forward PPPoE packets from the WAN port to the LAN ports and from the LAN ports to the WAN port.
	In addition to the P-870HN-51D's built-in PPPoE client, you can select this to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the P-870HN-51D. Each host can have a separate account and a public WAN IP address.
	This is an alternative to NAT for application where NAT is not appropriate.
	Clear this if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Enable IGMP Multicast Proxy	Select this check box to have the P-870HN-51D act as an IGMP proxy on this connection. This allows the P-870HN-51D to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoE

This screen displays when you select **IP over Ethernet** in the **WAN Service Configuration** screen.

Figure 34 WAN Configuration: IPoE

The following table describes the labels in this screen.

Table 18 WAN Configuration: IPoE

LABEL	DESCRIPTION
Obtain an IP address automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you want to get a dynamic IP address from the ISP.
Enable DHCP Option 60	Select this to identify the vendor and functionality of the P-870HN-51D in DHCP requests that the P-870HN-51D sends to a DHCP server when getting a WAN IP address.
Vendor Class Identifier	Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.
Enable DHCP Option 61	Select this to identify the P-870HN-51D in DHCP requests that the P-870HN-51D sends to a DHCP server when getting a WAN IP address.
IAID	Enter the Identity Association Identifier (IAID) of the P-870HN-51D. For example, the WAN connection index number.
DUID Type	Select **Other** to enter any string that identifies the P-870HN-51D in the **DUID** field. Select **DUID-LL** (DUID Based on Link-layer Address) to enter the P-870HN-51D's hardware address, that is the MAC address in the **DUID** field. Select **DUID-EN** (DUID Assigned by Vendor Based on Enterprise Number) to enter the vendor's registered private enterprise number.
DUID	Enter the DHCP Unique Identifier (DUID) of the P-870HN-51D.
Identifier	Enter a unique identifier assigned by the vendor. This field is available when you select **DUID-EN** in the **DUID Type** field.
Enable DHCP Option 125	Select this to add vendor specific information to DHCP requests that the P-870HN-51D sends to a DHCP server when getting a WAN IP address.
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 P-870HN-51D.
Model Name	Enter the model name of the P-870HN-51D.
Serial Number	Enter the serial number of the P-870HN-51D.
Use the following Static IP address	Select this if you have a static IP address.
WAN IP Address	Enter the static IP address provided by your ISP.
WAN Subnet Mask	Enter the subnet mask provided by your ISP.
WAN gateway IP Address	Enter the gateway IP address provided by your ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

...

5.5.1.4 NAT, IGMP Multicast and Firewall Activation

The screen is available only when you select **IP over Ethernet** in the **WAN Service Configuration** screen.

Figure 35   WAN Configuration: NAT, IGMP Multicast and Firewall Activation

The following table describes the labels in this screen.

Table 19   WAN Configuration: NAT, IGMP Multicast and Firewall Activation

LABEL	DESCRIPTION
Enable NAT	Select this option to enable NAT on the P-870HN-51D. You can also select the **NAT Type** you want the P-870HN-51D to implement. The choices are as follows: • **Symmetric NAT (default)** - Symmetric NAT maps requests from the same private IP address and port to a different public source IP address and/or port depending on the packet's destination IP address. • **Port Restricted Cone NAT** - Restricted cone NAT maps all requests from the same private IP address and port to the same public source IP address and port. • **Restricted Cone NAT** - Restricted cone NAT maps all requests from the same private IP address to the same public source IP address. • **Full Cone NAT** - In full cone NAT, all requests from the same private IP address and port are mapped to the same public source IP address and port. Someone on the Internet only needs to know the mapping scheme in order to send packets to a device behind the NAT router.
Enable Firewall	Select this check box to activate Firewall on this connection.
Enable IGMP Multicast Proxy	Select this check box to have the P-870HN-51D act as an IGMP proxy on this connection. This allows the P-870HN-51D to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.5 Default Gateway

The screen is not available when you select **Bridging** in the **WAN Service Configuration** screen.

Figure 36 WAN Configuration: Default Gateway

The following table describes the labels in this screen.

Table 20 WAN Configuration: Default Gateway: PPPoE, PPPoA, IPoE or IPoA

LABEL	DESCRIPTION
Selected Default Gateway Interfaces	Select a WAN interface through which you want to forward the traffic.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.6 DNS Server

The screen is not available when you select **Bridging** in the **WAN Service Configuration** screen.

Figure 37 WAN Configuration: DNS Server

The following table describes the labels in this screen.

Table 21 WAN Configuration: DNS Server

LABEL	DESCRIPTION
Obtain DNS info from a WAN interface	Select this to have the P-870HN-51D get the DNS server addresses from the ISP automatically.
WAN Interface selected	Select a WAN interface through which you want to obtain the DNS related information.
Use the following Static DNS IP address	Select this to have the P-870HN-51D use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.5.1.7 Configuration Summary

This read-only screen shows the current WAN connection settings.

Figure 38 WAN Configuration: Configuration Summary

83

The following table describes the labels in this screen.

Table 22   WAN Configuration: Configuration Summary

LABEL	DESCRIPTION
Connection Type	This is the encapsulation method used by this connection.
Service Name	This is the name of the service.
Service Category	This is the ATM traffic class.
	This field is blank for a PTM or Ethernet WAN conenction.
IP Address	This shows whether the WAN IP address is assigned by the ISP, manually configured or not configurable.
Service State	This shows whether this service is active or not.
NAT	This shows whether NAT is active or not for this connection.
NAT Type	This shows the type of NAT implemented for this connection.
Firewall	This shows whether Firewall is active or not for this connection.
Quality Of Service	This shows whether QoS is active or not for this connection.
IGMP Multicast	This shows whether IGMP multicasting is active or not for this connection.
Back	Click this button to return to the previous screen.
Apply/Save	Click this button to save your changes.

5.6 Technical Reference

The following section contains additional technical information about the P-870HN-51D features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The P-870HN-51D can work in bridge mode or routing mode. When the P-870HN-51D is in routing mode, it supports the following methods.

IP over Ethernet

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

PPP over Ethernet

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

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

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

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

By implementing PPPoE directly on the P-870HN-51D (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the P-870HN-51D does that part of the task. Furthermore, with NAT, all of the LAN's computers will have access.

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.

Full Cone NAT

In full cone NAT, the NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The NAT router also maps packets coming to that external IP address and port to the internal IP address and port.

In the following example, the P-870HN-51D maps the source address of all packets sent from the internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. The P-870HN-51D also performs NAT on all incoming

packets sent to IP address **2** and port **B** and forwards them to IP address **1**, port **A**.

Figure 39 Full Cone NAT Example
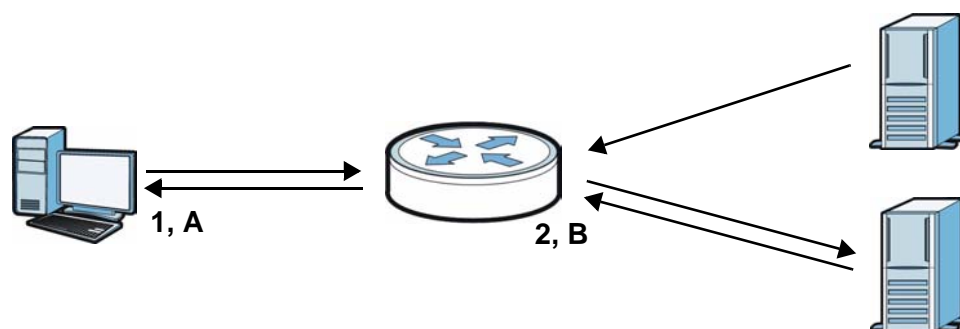
Symmetric NAT

The full, restricted and port restricted cone NAT types use the same mapping for an outgoing packet's source address regardless of the destination IP address and port. In symmetric NAT, the mapping of an outgoing packet's source address to a source address in another network is different for each different destination IP address and port.

In the following example, the P-870HN-51D maps the source address IP address **1** and port **A** to IP address **2** and port **B** on the external network for packets sent to IP address **3** and port **C**. The P-870HN-51D uses a different mapping (IP address **2** and port **M**) for packets sent to IP address **4** and port **D**.

A host on the external network (IP address **3** and port **C** for example) can only send packets to the internal host via the external IP address and port that the NAT router used in sending a packet to the external host's IP address and port. So in

the example, only **3, C** is allowed to send packets to **2, B** and only **4, D** is allowed to send packets to **2, M**.

Figure 40 Symmetric NAT
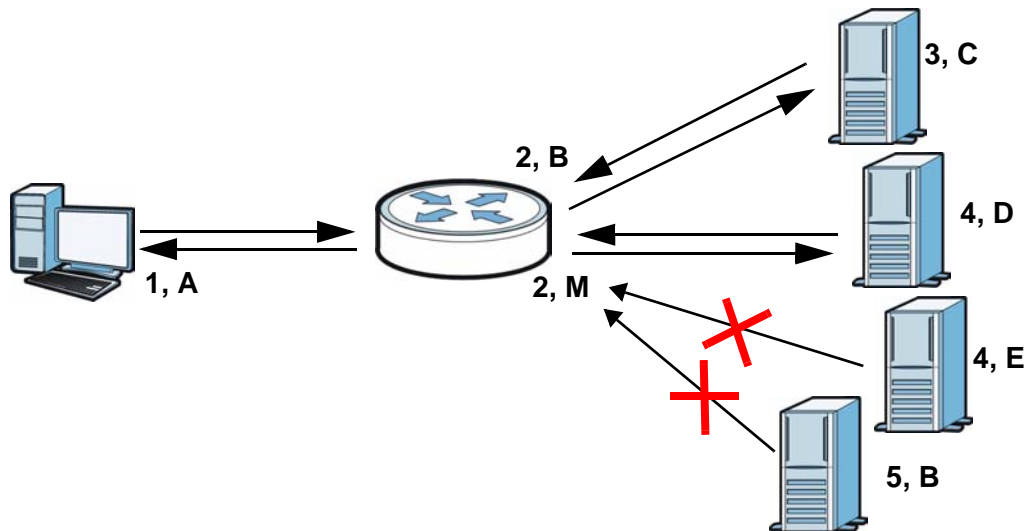
Introduction to VLANs

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

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

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

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and

contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

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

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

Multicast

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

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

At start up, the P-870HN-51D queries all directly connected networks to gather group membership. After that, the P-870HN-51D periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is

204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The P-870HN-51D can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2 If your ISP dynamically assigns the DNS server IP addresses (along with the P-870HN-51D's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

LAN Setup

6.1 Overview

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

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

LAN
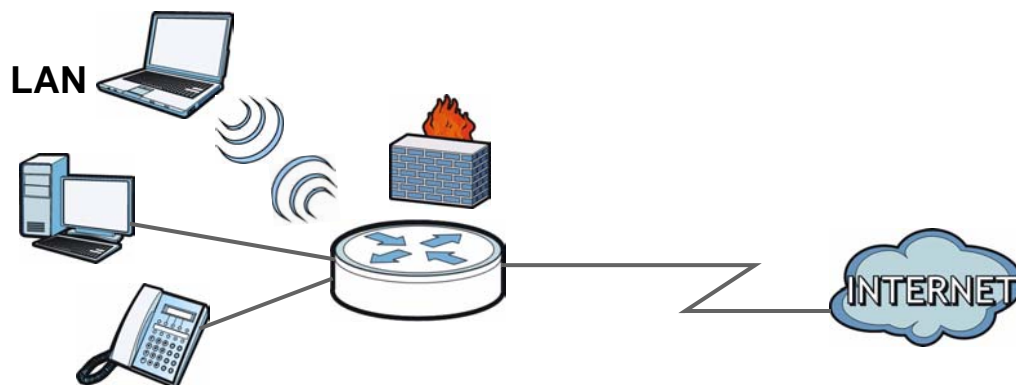
* See Section 6.4 on page 95 for more information on LANs.
* See Appendix E on page 321 for more information on IP addresses and subnetting.

6.1.1 What You Can Do in this Chapter

The **LAN IP** screen lets you set the LAN IP address and subnet mask of your ZyXEL device and configure other LAN TCP/IP settings (Section 6.3 on page 93).

6.2 What You Need To Know

IP Address

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. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your P-870HN-51D will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the P-870HN-51D unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This P-870HN-51D has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DHCP Relay

You can also configure the P-870HN-51D to relay client DHCP requests to a DHCP server and the server's responses back to the clients.

RIP

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

Multicast and IGMP

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

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

DNS

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.

6.3 The LAN IP Screen

Click **Network > LAN** to open the **IP** screen. See Section 6.4 on page 95 for background information. Use this screen to set the Local Area Network IP address and subnet mask of your P-870HN-51D.

Figure 41 LAN > IP

The following table describes the fields in this screen.

Table 23   LAN > IP

LABEL	DESCRIPTION
LAN TCP/IP	
Group Name	Select the interface group for which you want to configure the LAN TCP/IP settings. See Chapter 19 on page 213 for how to create a new interface group.
IP Address	Enter the LAN IP address you want to assign to your P-870HN-51D in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
DHCP Setup	
Enable DHCP	Select this to have the P-870HN-51D act as a DHCP server or DHCP relay agent. Otherwise, deselect this to not have the P-870HN-51D provide any DHCP services. The DHCP server will be disabled.
DHCP Server	Select this option to have the P-870HN-51D assign IP addresses and provide subnet mask, gateway, and DNS server information to the network. The P-870HN-51D is the DHCP server for the network. When the P-870HN-51D acts as a DHCP server, the following items need to be set:
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DHCP Relay	Select this option to have the P-870HN-51D forward DHCP request to the DHCP server.
Relay Server	If you select **DHCP Relay**, enter the IP address of the DHCP server.
DNS Servers Assigned by DHCP Server	
Obtain DNS info from a WAN interface	When a LAN client sends a DNS query to the P-870HN-51D, the P-870HN-51D forwards the query to the system DNS server configured in the WAN interface you select. If you do not configure DNS servers on the selected WAN inteface, the P-870HN-51D uses the LAN IP address and tells the DHCP clients on the LAN that itself is the DNS server.
Use the following Static DNS IP address	
First DNS Server	Enter the first DNS (Domain Name System) server IP address the P-870HN-51D passes to the DHCP clients.
Second DNS Server	Enter the second DNS (Domain Name System) server IP address the P-870HN-51D passes to the DHCP clients.
IGMP Snooping	
Enable IGMP Snooping	Select this option to enable IGMP snooping. This allows the P-870HN-51D to passively learn multicast group.
Standard Mode	Select this to have the P-870HN-51D forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports.

Table 23 LAN > IP

LABEL	DESCRIPTION
Blocking Mode	Select this to have the P-870HN-51D block all unknown multicast packets from the WAN.
Enable IP Alias	Select the check box to configure another LAN network for the P-870HN-51D.
IP Address	Enter the IP address of your P-870HN-51D in dotted decimal notation.
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
Apply	Click **Apply** to save your changes back to the P-870HN-51D.

6.4 Technical Reference

The following section contains additional technical information about the P-870HN-51D features described in this chapter.

LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the P-870HN-51D 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 42 LAN and WAN IP Addresses
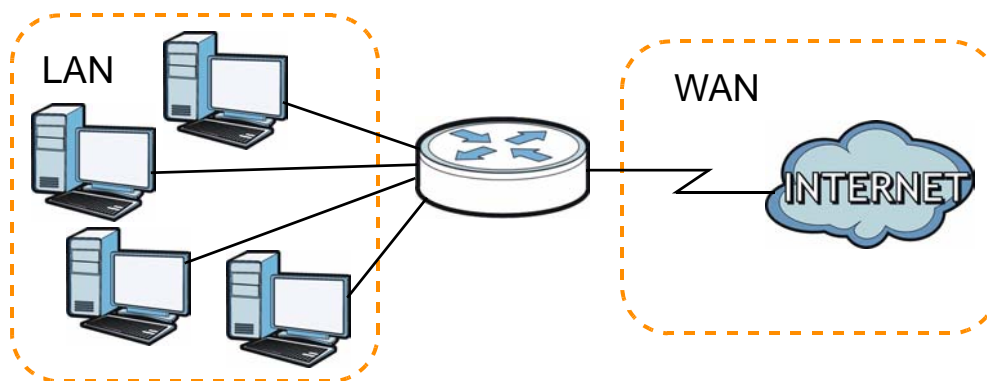
DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the P-870HN-51D as a DHCP server or disable it. When configured as a server, the P-870HN-51D provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The P-870HN-51D 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.

LAN TCP/IP

The P-870HN-51D has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the P-870HN-51D. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your P-870HN-51D, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your P-870HN-51D will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the P-870HN-51D 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".

Multicast

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

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

The P-870HN-51D supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the P-870HN-51D queries all directly connected networks to gather group membership. After that, the P-870HN-51D periodically updates this information. IP multicasting can be enabled/disabled on the P-870HN-51D LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The P-870HN-51D supports three logical LAN interfaces via its single physical Ethernet interface with the P-870HN-51D itself as the gateway for each LAN network.

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

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

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

Figure 43 Physical Network & Partitioned Logical Networks
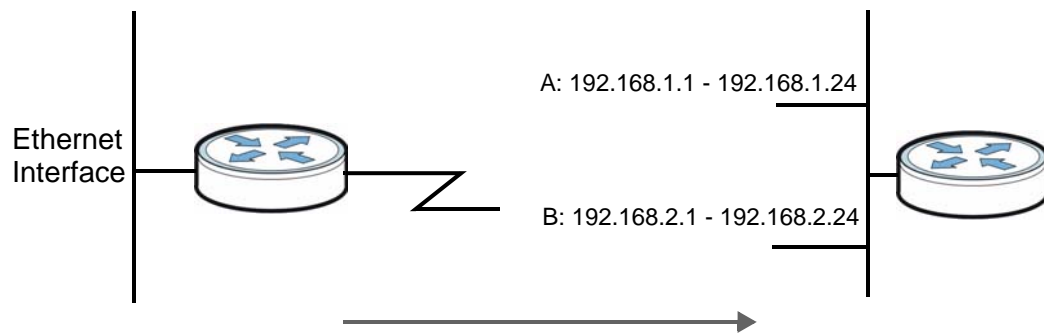
Wireless LAN

7.1 Overview

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

• Turning the wireless connection on or off.

• Configuring a name, wireless channel and security for the network.

• Using WiFi Protected Setup (WPS) to configure your wireless network.

• Using a MAC (Media Access Control) address filter to restrict access to the wireless network.

See Chapter 2 on page 27 for a tutorial showing how to set up your wireless connection in an example scenario.

See Section 7.9 on page 117 for advanced technical information on wireless networks.

7.1.1 What You Can Do in this Chapter

This chapter describes the P-870HN-51D's **Network > Wireless LAN** screens. Use these screens to set up your P-870HN-51D's wireless connection.

• The **General** screen lets you turn the wireless connection on or off, set up wireless security and make other basic configuration changes (Section 7.4 on page 102). You can also configure the MAC filter to allow or block access to the P-870HN-51D based on the MAC addresses of the wireless stations.

• The **More AP** screen lets you set up multiple wireless networks on your P-870HN-51D (Section 7.5 on page 112).

• Use the **WPS** screen and the **WPS Station** screen to use WiFi Protected Setup (WPS). WPS lets you set up a secure network quickly, when connecting to other WPS-enabled devices.

Use the **WPS** screen (see Section 7.6 on page 113) to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the P-870HN-51D's WPS status.

Use the **WPS Station** (see Section 7.7 on page 115) screen to set up WPS by pressing a button or using a PIN.

- The **Advanced Setup** screen lets you change the wireless mode, and make other advanced wireless configuration changes (Section 7.8 on page 116).

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

7.2 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.

Wireless Network Construction

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.

Network Names

Each network must have a name, referred to as the SSID - "Service Set IDentifier". The "service set" is the network, so the "service set identifier" is the network's name. This helps you identify your wireless network when wireless networks' coverage areas overlap and you have a variety of networks to choose from.

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.

Wireless Security

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 she/he can either 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 perfectly 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.

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.

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.

7.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See Section 7.2 on page 100 if some of the terms used here do not make sense to you.

* What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?

* What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?

* Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

  Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.

* What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

7.4 The General Screen

Note: If you are configuring the P-870HN-51D from a computer connected to the wireless LAN and you change the P-870HN-51D's SSID 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 P-870HN-51D's new settings.

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

Figure 44 Network > Wireless LAN > General

The following table describes the labels in this screen.

Table 24 Network > Wireless LAN > General

LABEL	DESCRIPTION
Active Wireless LAN	Click the check box to activate wireless LAN.
Channel Selection	Set the operating frequency/channel depending on your particular region.
	Select a channel or use **Auto** to have the P-870HN-51D 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 P-870HN-51D is currently using then displays next to this field.

Table 24 Network > Wireless LAN > General

LABEL	DESCRIPTION
Bandwidth	Select whether the P-870HN-51D uses a wireless channel width of **20MHz** or **40MHz**. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. This field is available only when you set the **802.11 Mode** to **802.11n Only** or **802.11b/g/n Mixed** in the **Advanced Setup** screen.
Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the P-870HN-51D from a computer connected to the wireless LAN and you change the P-870HN-51D's SSID or wireless 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 P-870HN-51D's new settings.
Hide Network Name (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.
BSSID	This shows the MAC address of the wireless interface on the P-870HN-51D when wireless LAN is enabled.
Security Mode	See the following sections for more details about this field.
MAC Filter	Click this button to go to the **MAC Filter** screen to configure whether the wireless devices with the MAC addresses listed are allowed or denied to access the P-870HN-51D using this SSID.
Apply	Click this to save your changes back to the P-870HN-51D.
Reset	Click this to reload the previous configuration for this screen.

7.4.1 No Security

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

Note: If you do not enable any wireless security on your P-870HN-51D, your network is accessible to any wireless networking device that is within range.

Figure 45   Wireless LAN > General: No Security

The following table describes the labels in this screen.

Table 25   Wireless LAN > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.

7.4.2 WEP Encryption

In order to configure and enable WEP encryption; click **Network > Wireless LAN** to display the **General** screen. Select **WEP** from the **Security Mode** list.

Figure 46   Wireless LAN > General: Static WEP Encryption

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

Table 26   Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
Security Mode	Choose **WEP** from the drop-down list box.

Table 26   Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **64-bit** or **128-bit** to enable data encryption.
Key 1 to Key 4	The WEP key is used to secure your data from eavesdropping by unauthorized wireless users. Both the P-870HN-51D and the wireless stations must use the same WEP key for data transmission. Only one key can be activated at any one time. Select a default key to use for data encryption. If you chose **64-bit** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.

7.4.3 WPA(2)-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 47   Wireless LAN > General: WPA(2)-PSK

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

Table 27 Wireless LAN > General: WPA(2)-PSK

LABEL	DESCRIPTION
Auto Generate Key	This field is only available for WPA-PSK and WPA2-PSK.
	Select this option to have the P-870HN-51D automatically generate an SSID and pre-shared key. The **SSID** and **Pre-Shared Key** fields will not be configurable when you select this option.
Security Mode	Choose **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
Active Compatible	This field is only available for WPA2-PSK. Select this if you want the P-870HN-51D to support WPA-PSK and WPA2-PSK simultaneously.
Encryption	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption.
	Select **TKIP** if your wireless clients can all use TKIP.
	Select **AES** if your wireless clients can all use AES.
	Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.
Pre-Shared Key	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials.
	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients.
ReKey Method	Select **Time** to change encryption keys automatically using the time interval specified in the **Group Key Update Timer** field. If no value is entered in the said field, this feature is disabled.
	Select **None** if you do not want to use this feature.

7.4.4 WPA(2) Authentication

Use this screen to configure and enable WPA or WPA2 authentication; click the **Wireless LAN** link under **Network** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Note: WPA or WPA2 is not available if you enable WPS before you configure WPA or WPA2 in the **Wireless LAN** > **General** screen.

Note: If you select **WPA** or **WPA2** in the **Wireless LAN > General** screen, the WDS and WPS features are not available on the P-870HN-51D.

Figure 48 Wireless LAN > General: WPA(2)

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

Table 28 Wireless LAN > General: WPA(2)

LABEL	DESCRIPTION
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.
Active Compatible	This field is only available for WPA2. Select this if you want the P-870HN-51D to support WPA and WPA2 simultaneously.
Encryption	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption. Select **TKIP** if your wireless clients can all use TKIP. Select **AES** if your wireless clients can all use AES. 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.

Table 28   Wireless LAN > General: WPA(2)

LABEL	DESCRIPTION
ReKey Method	Select **Time** to change encryption keys automatically using the time interval specified in the **Group Key Update Timer** field. If no value is entered in the said field, this feature is disabled. Select **None** if you do not want to use this feature.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. 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 P-870HN-51D. The key must be the same on the external authentication server and your P-870HN-51D. The key is not sent over the network.

7.4.5 MAC Filter

This screen allows you to configure the P-870HN-51D to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the P-870HN-51D (**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 change your P-870HN-51D's MAC filter settings. Click the **Edit** button in the **Wireless LAN > General** screen. The following screen displays.

Figure 49   Wireless LAN > MAC Filter

The following table describes the labels in this screen.

Table 29 Wireless LAN > MAC Filter

LABEL	DESCRIPTION
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the table below.
	Select **Disabled** to turn off MAC address filtering.
	Select **Allow** to permit access to the P-870HN-51D, MAC addresses not listed will be denied access to the P-870HN-51D.
	Select **Deny** to block access to the P-870HN-51D, MAC addresses not listed will be allowed to access the P-870HN-51D
#	This is the index number of the MAC address.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the P-870HN-51D.
Modify	Click the **Remove** icon to delete the entry.
Back	Click this to return to the previous screen without saving changes.
Add	Click this to create a new MAC filtering rule.

7.4.6 Adding a New MAC Filtering Rule

Click the **Add** button in the **MAC Filter** screen. The following screen displays.

Figure 50 Wireless LAN > MAC Filter > Add

The following table describes the labels in this screen.

Table 30 Wireless LAN > MAC Filter > Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC addresses of the wireless devices that are allowed or denied access to the P-870HN-51D 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.
Back	Click this to return to the previous screen without saving changes.
Apply	Click this to save your changes and go back to the previous screen.

7.5 The More AP Screen

This screen allows you to enable and configure multiple wireless networks on the P-870HN-51D.

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

Figure 51   Network > Wireless LAN > More AP

The following table describes the labels in this screen.
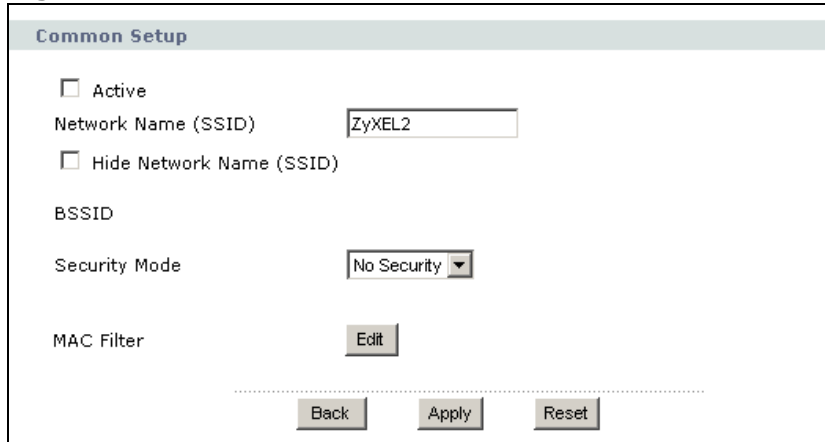
Table 31   Network > Wireless LAN > More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Active	Select the check box to activate an SSID profile.
SSID	An SSID profile is the set of parameters relating to one of the P-870HN-51D's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the **Edit** icon to configure the SSID profile.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.1 More AP Edit

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

Figure 52   Network > Wireless LAN > More AP: Edit

See Section 7.4 on page 102 for more details about the fields in this screen.

7.6 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your P-870HN-51D.

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.

Click **Network > Wireless LAN >WPS**. The following screen displays.

Figure 53 Network > Wireless LAN > WPS

The following table describes the labels in this screen.

Table 32 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select the check box to activate WPS on the P-870HN-51D.
PIN Number	This shows the PIN (Personal Identification Number) of the P-870HN-51D. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method.
Generate	Click this button to have the P-870HN-51D create a new PIN.
WPS Status	This displays **Configured** when the P-870HN-51D has connected to a wireless network using WPS or **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there is no wireless or wireless security changes on the P-870HN-51D or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release_Co nfiguration	This button is available when the WPS status is **Configured** but not configurable if you disable WPS. Click this button to remove all configured wireless and wireless security settings for WPS connections on the P-870HN-51D.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.

7.7 The WPS Station Screen

Use this screen to set up a WPS wireless network using either Push Button Configuration (PBC) or PIN Configuration.

Note: If you select **No Security** in the **Wireless LAN > General** screen and click **Push Button** in the **WPS Station** screen, the P-870HN-51D automatically changes to use WPA-PSK/WPA2-PSK mixed mode and generates a pre-shared key.

Click **Network > Wireless LAN > WPS Station**. The following screen displays.

Figure 54   Network > Wireless LAN > WPS Station

The following table describes the labels in this screen.

Table 33   Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Click this button to add another WPS-enabled wireless device (within wireless range of the P-870HN-51D) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **Push Button** on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Or input station's PIN number	Enter the PIN of the device that you are setting up a WPS connection with and click **Start** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the P-870HN-51D.

7.8 The Advanced Setup Screen

To configure advanced wireless settings, click **Network > Wireless LAN > Advanced Setup**. The screen appears as shown.

Figure 55   Wireless LAN > Advanced Setup

The following table describes the labels in this screen.

Table 34   Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
802.11 Mode	Select **802.11b Only** to only allow IEEE 802.11b compliant WLAN devices to associate with the P-870HN-51D.
	Select **802.11g Only** to allow IEEE 802.11g compliant WLAN devices to associate with the P-870HN-51D. IEEE 802.11b compliant WLAN devices can associate with the P-870HN-51D only when they use the short premble type.
	Select **802.11n Only** to only allow IEEE 802.11n compliant WLAN devices to associate with the P-870HN-51D. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the P-870HN-51D.
	Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the P-870HN-51D. The P-870HN-51D adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices.
	Select **802.11 b/g/n mixed mode** to allow both IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the P-870HN-51D. The transmission rate of your P-870HN-51D might be reduced.
RTS/CTS Threshold	Enter a value between 0 and 2432.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.

Table 34 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
Number of Wireless Stations Allowed	Specify the maximum number (from 1 to 64) of the wireless stations that may connect to the P-870HN-51D.
Output Power	Set the output power of the P-870HN-51D. 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%**.
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). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select **Off** to disable 802.11 protection. The transmission rate of your P-870HN-51D might be reduced in a mixed-mode network. 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 menu. Choices are **Long** or **Short**. The default setting is **Long**. See the appendix for more information. This field is not configurable and the P-870HN-51D uses **Short** when you set **802.11 Mode** to **802.11g Only** or **802.11n Only**.
Apply	Click this to save your changes back to the P-870HN-51D.
Reset	Click this to reload the previous configuration for this screen.

7.9 Technical Reference

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

7.9.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 56   Example of a Wireless Network
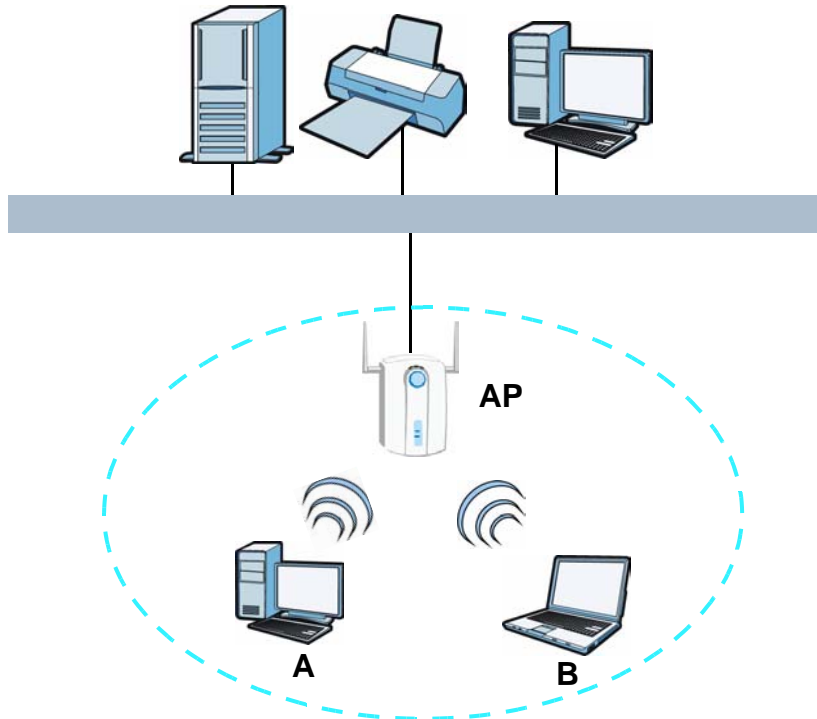
The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your P-870HN-51D is the AP.

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 IDentity.

• 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.

7.9.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the P-870HN-51D's Web Configurator.

Table 35   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. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the P-870HN-51D. The lower the value, the more often the devices must get permission. 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 P-870HN-51D.
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 P-870HN-51D does, it cannot communicate with the P-870HN-51D.
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.

7.9.3 Wireless Security Overview

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

7.9.3.1 SSID

Normally, the P-870HN-51D acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the P-870HN-51D 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.

7.9.3.2 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 P-870HN-51D 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.

7.9.3.3 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 they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

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

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

7.9.3.4 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.

---

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.

The types of encryption you can choose depend on the type of authentication. (See Section 7.9.3.3 on page 120 for information about this.)

Table 36 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	
↕	Static WEP	
	WPA-PSK	
		WPA
Stronges t	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 P-870HN-51D 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 P-870HN-51D, 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 P-870HN-51D.

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.

7.9.4 WiFi Protected Setup

Your P-870HN-51D 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.

7.9.4.1 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 P-870HN-51D, see Section 7.7 on page 115).

3 Press the button on one of the devices (it doesn't matter which). For the P-870HN-51D 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.

7.9.4.2 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 P-870HN-51D, see).

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

Note: 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.

5 Start WPS on both devices within two minutes.

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

6 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 57   Example WPS Process: PIN Method
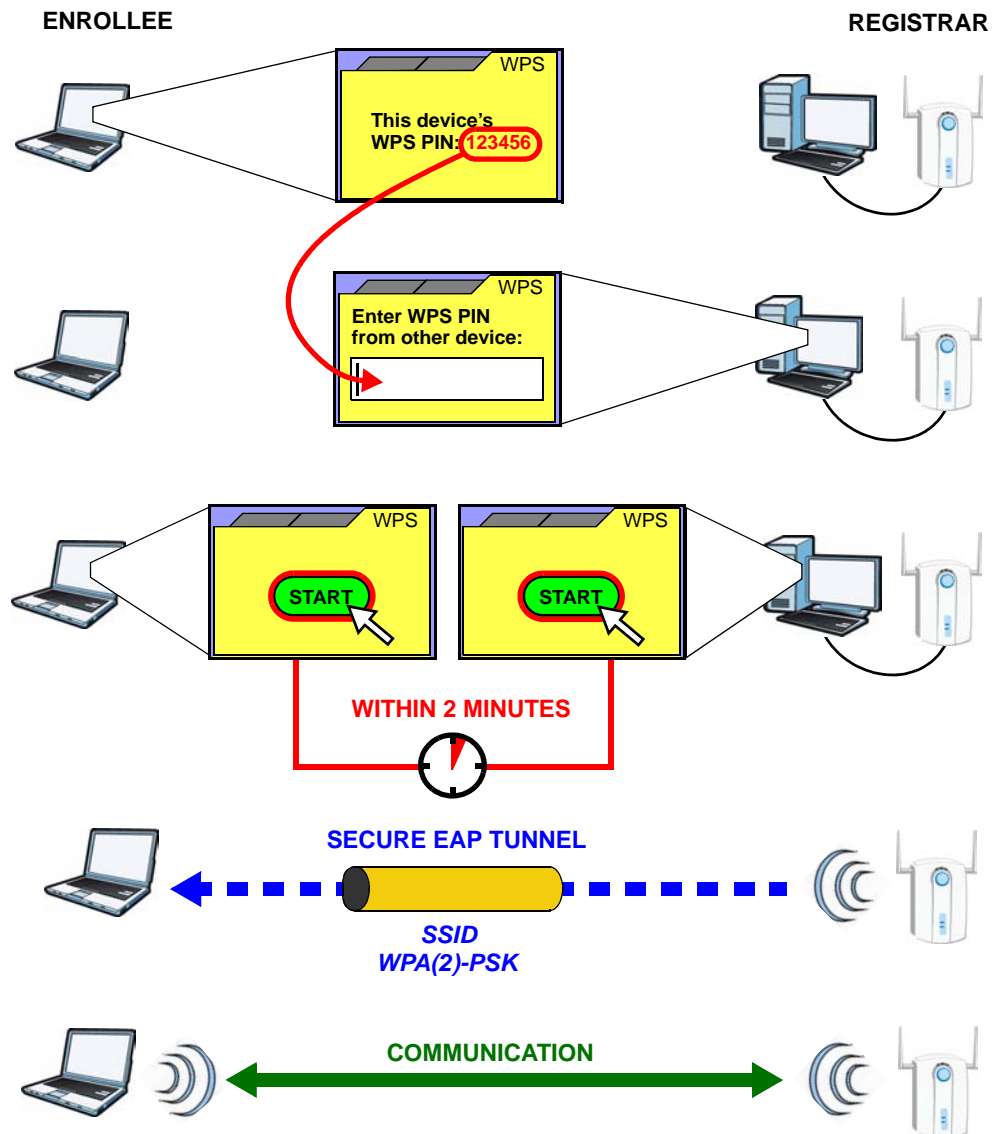
7.9.4.3 How WPS Works

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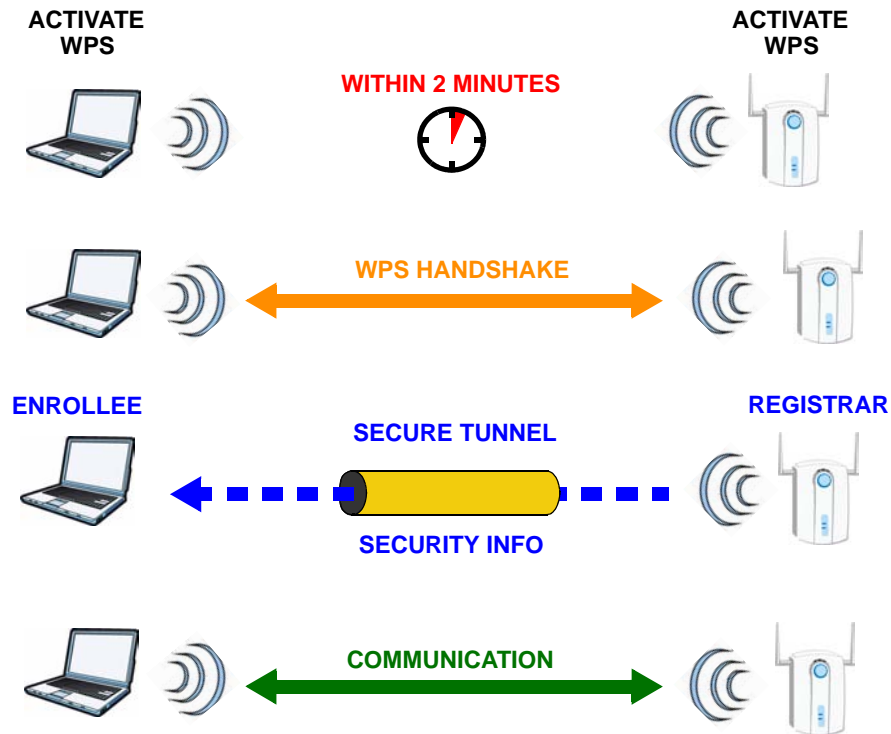
The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

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.

7.9.4.4 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 59   WPS: Example Network Step 1
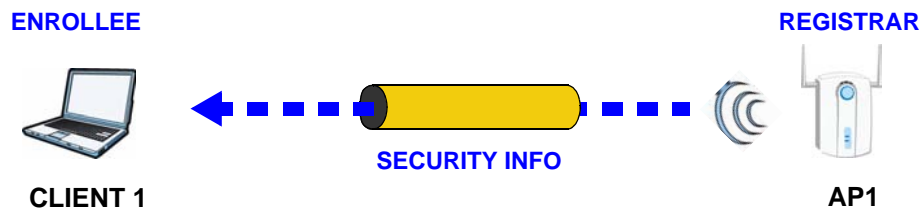
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 60   WPS: Example Network Step 2
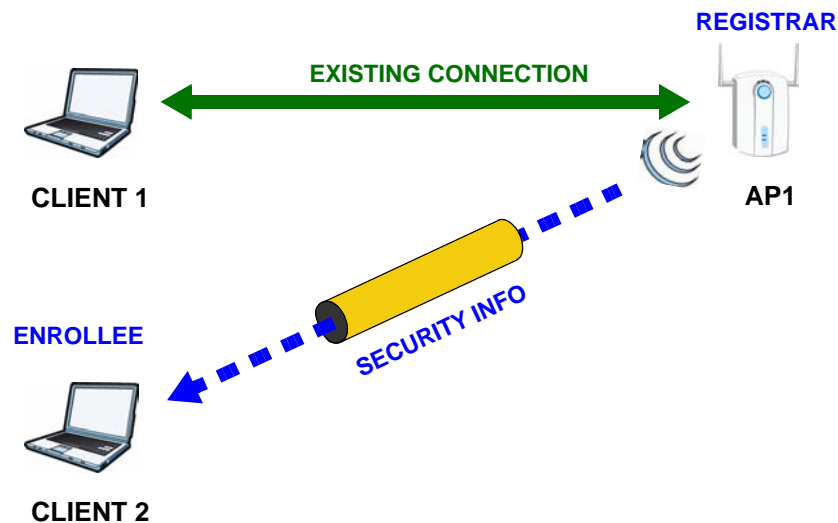
In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access

point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 61   WPS: Example Network Step 3
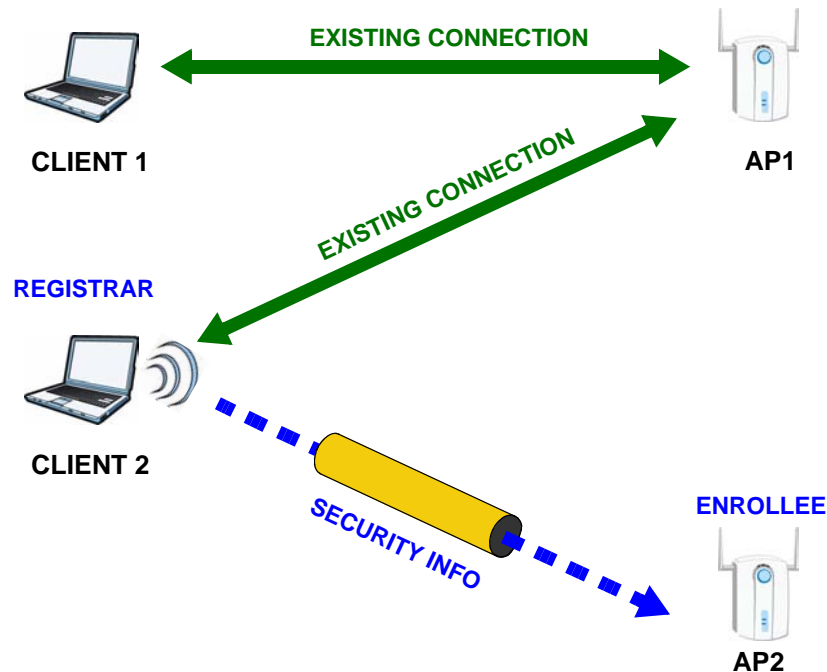
7.9.4.5 Limitations of WPS

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.

Network Address Translation (NAT)

8.1 Overview

This chapter discusses how to configure NAT on the P-870HN-51D.

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.

8.1.1 What You Can Do in this Chapter

- The **Port Forwarding** screen lets you configure forward incoming service requests to the server(s) on your local network (Section 8.3 on page 130).
- The **Trigger Port** screen lets you change the P-870HN-51D's trigger port settings (Section 8.4 on page 133).
- The **DMZ Host** screen lets you configure a default server (Section 8.5 on page 137).
- The **ALG** screen lets you enable SIP ALG on the P-870HN-51D (Section 8.6 on page 138).

8.2 What You Need to Know

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

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.

8.3 The Port Forwarding Screen

This summary screen provides a summary of all port forwarding rules and their configuration. In addition, this screen allows you to create new port forwarding rules and delete existing rules.

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.

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.

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

Figure 62   NAT Port Forwarding

The following table describes the labels in this screen.

Table 37 NAT Port Forwarding

LABEL	DESCRIPTION
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will display in the **External port**, **Internal port** and **Protocol** fields.
	Otherwise, select **User Define** to open the **Rule Setup** screen where you can manually enter the port number(s) and select the IP protocol.
WAN Interface	Select the WAN interface through which the service is forwarded.
	You must have already configured a WAN connection with NAT enabled.
Server IP Address	Enter the IP address of the server for the specified service.
External Port Start	Enter the original destination port for the packets.
	To forward only one port, enter the port number again in the **External Port End** field.
	To forward a series of ports, enter the start port number here and the end port number in the **External Port End** field.
External Port End	Enter the last port of the original destination port range.
	To forward only one port, enter the port number in the **External Port Start** field above and then enter it again in this field.
	To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Port Start** field above.
Internal Port Start	Enter the port number to which you want the P-870HN-51D to translate the incoming port.
	To forward only one port, enter the port number again in the **Internal Port End** field.
	For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Internal Port End	Enter the last port of the translated port range.
Protocol	This is the transport layer protocol used for the service.
Add	Click this button to add a rule to the table below.
No.	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not.
	Clear the check box to disable the rule. Select the check box to enable it.
Server Name	This field displays the name of the service used by the packets for this virtual server.
WAN Interface	This field displays the WAN interface through which the service is forwarded.
External Start Port	This is the first external port number that identifies a service.
External End Port	This is the last external port number that identifies a service.

Table 37 NAT Port Forwarding (continued)

LABEL	DESCRIPTION
Internal Start Port	This is the first internal port number that identifies a service.
Internal End Port	This is the last internal port number that identifies a service.
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the **Edit** icon to go to the screen where you can edit the port forwarding rule. Click the **Remove** icon to delete an existing port forwarding rule. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to return to the previous configuration.

8.3.1 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Select **User Define** in the **Service Name** field or click the rule's **Edit** icon in the **Port Forwarding** screen to open the following screen.

Figure 63 Port Forwarding Edit

The following table describes the labels in this screen.

Table 38 Port Forwarding Edit

LABEL	DESCRIPTION
Active	Clear the check box to disable the rule. Select the check box to enable it. This field is not editable if you are configuring a **User Define** rule.
Service Name	Enter a name to identify this rule. This field is read-only if you click the **Edit** icon in the **Port Forwarding** screen.
WAN Interface	Select a WAN interface for which you want to configure port forwarding rules.

Table 38 Port Forwarding Edit (continued)

LABEL	DESCRIPTION
External Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field.
External End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Start Port** field above.
Internal Start Port	Enter the port number here to which you want the P-870HN-51D 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.
Internal End Port	Enter the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the transport layer protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.4 The Trigger Port 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 P-870HN-51D 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 P-870HN-51D's WAN port receives a response with a specific port number and protocol ("open" port), the P-870HN-51D 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 64 Trigger Port Forwarding Process: Example
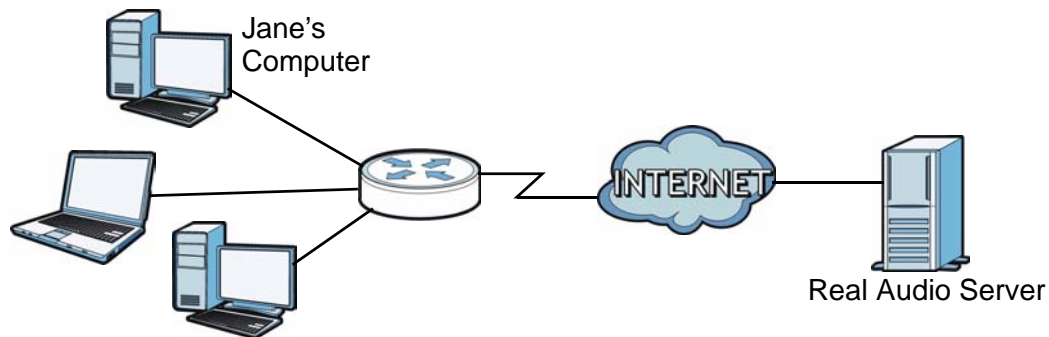
1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a "trigger" port and causes the P-870HN-51D to record Jane's computer IP address. The P-870HN-51D 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 P-870HN-51D 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 P-870HN-51D times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **NAT** > **Trigger Port** to open the following screen. Use this screen to view and configure your P-870HN-51D's trigger port settings.

Figure 65 Trigger Port

The following table describes the labels in this screen.

Table 39 NAT Trigger Port

LABEL	DESCRIPTION
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will display in the **Trigger port**, **Open port** and **Protocol** fields. Otherwise, select **User Define** to open the **Rule Setup** screen where you can manually enter the port number(s) and select the transport layer protocol.
WAN Interface	Select the WAN interface through which the service is forwarded.
Trigger Port	The trigger port is a port (or a range of ports) that causes (or triggers) the P-870HN-51D to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start	This is the first port number that identifies a service.
End	This is the last port number that identifies a service.
Protocol	This is the transport layer protocol used for the service.
Open 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 P-870HN-51D forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start	This is the first port number that identifies a service.
End	This is the last port number that identifies a service.
Protocol	This is the transport layer protocol used for the service.
Add	Click this button to add a rule to the table below.
No.	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Server Name	This field displays the name of the service used by the packets for this virtual server.
WAN Interface	This field displays the WAN interface through which the service is forwarded.
Trigger Start Port	This is the first trigger port number that identifies a service.
Trigger End Port	This is the last trigger port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol. **1** means TCP, **2** means UDP and **3** means TCP/UDP.
Open Start Port	This is the first open port number that identifies a service.
Open End Port	This is the last open port number that identifies a service.
Open Proto.	This is the open transport layer protocol. **1** means TCP, **2** means UDP and **3** means TCP/UDP.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Remove** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.

Table 39 NAT Trigger Port (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to return to the previous configuration.

8.4.1 Trigger Port Configuration

This screen lets you create new port triggering rules. Click the **Add** icon in the **NAT - Trigger Port** screen to open the following screen.

Figure 66   NAT > Trigger Port > Add

The following table describes the labels in this screen.

Table 40   NAT > Port Triggering > Add

LABEL	DESCRIPTION
Active	Clear the check box to disable the rule. Select the check box to enable it. This field is not editable if you are configuring a **User Define** rule.
Service Name	Enter a name to identify this rule. This field is read-only if you click the **Edit** icon in the **Trigger Port** screen.
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 P-870HN-51D to record the IP address of the LAN computer that sent the traffic to a server on the WAN. 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**.

Table 40   NAT > Port Triggering > Add

LABEL	DESCRIPTION
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 P-870HN-51D forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. 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**.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.5 The DMZ Host 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 67   NAT > DMZ Host

The following table describes the fields in this screen.

Table 41   NAT > DMZ Host
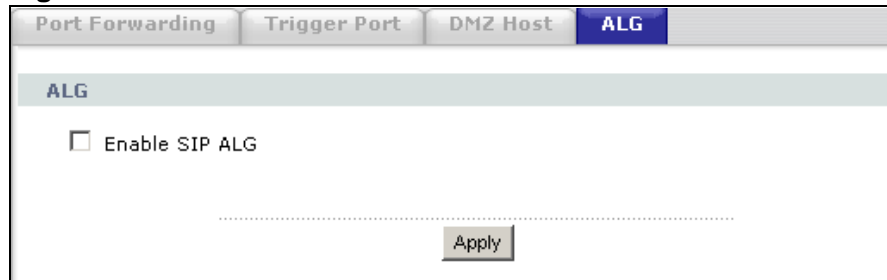
LABEL	DESCRIPTION
Default Server	Enter the IP address of the default server which receives packets from ports that are not specified in the **NAT Port Forwarding** screen. Note: If you do not assign a **Default Server**, the P-870HN-51D discards all packets received for ports that are not specified in the **NAT Port Forwarding** screen.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.

8.6 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. The SIP ALG translates the P-870HN-51D's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if you enable the SIP ALG.

Use this screen to enable or disable the SIP (VoIP) ALG in the P-870HN-51D. To access this screen, click **NAT > ALG**.

Figure 68   NAT > ALG

Each field is described in the following table.

Table 42   NAT > ALG

LABEL	DESCRIPTION
Active SIP ALG	Select this check box to allow SIP sessions to pass through the P-870HN-51D. SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol.
Apply	Click **Apply** to save your customized settings.

8.7 Technical Reference

The following section contains additional technical information about the P-870HN-51D features described in this chapter.

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 43 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 69 Multiple Servers Behind NAT Example

9
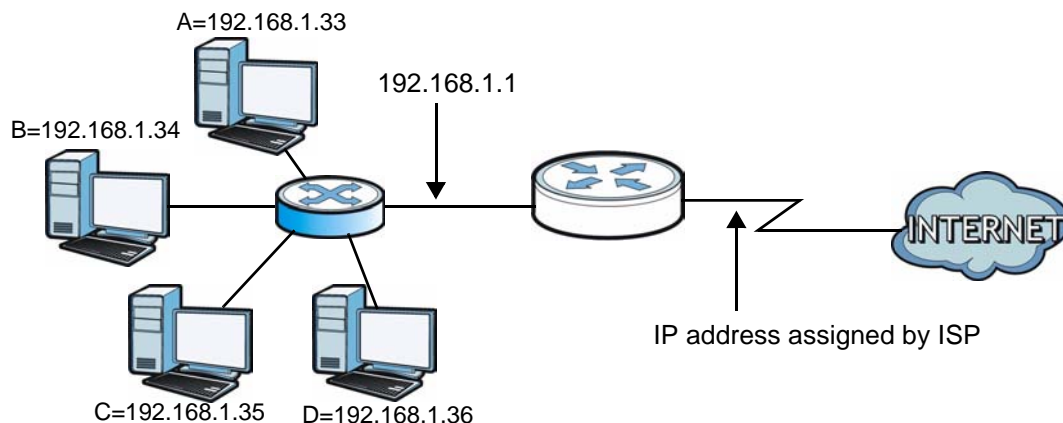
Firewall

9.1 Overview

This chapter shows you how to enable and configure the P-870HN-51D firewall settings.

The P-870HN-51D firewall is a packet filtering firewall and restricts access based on the source/destination computer network address of a packet and the type of application.

9.1.1 What You Can Do in this Chapter

The **Incoming** screen lets you view and configure incoming IP filtering rules (Section 9.3 on page 142).

9.2 What You Need to Know

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

Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An "extension number", called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 44   Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

Default Filtering Policies

Filtering rules are grouped based on the direction of travel of packets to which they apply.

The default rule for incoming traffic blocks all incoming connections from the WAN to the LAN. If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

Note: If you configure filtering rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the P-870HN-51D's default rules.

9.3 The Firewall Screen

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

Figure 70   Firewall > Incoming

The following table describes the labels in this screen.

Table 45 Firewall > Incoming

LABEL	DESCRIPTION
Active Firewall	Select this check box to enable the firewall on the P-870HN-51D. When the firewall is enabled, the P-870HN-51D blocks all incoming traffic from the WAN to the LAN. Create custome rules below to allow certain WAN users to access your LAN or to allow traffic from the WAN to a certain computer on the LAN.
Active	Select this check box to enable the rule.
Filter Name	This displays the name of the rule.
Interfaces	This displays the WAN interface(s) to which this rule is applied.
Protocol	This displays the transport layer protocol that defines the service to which this rule applies.
Source Address / Mask	This displays the source IP addresses and subnet mask to which this rule applies. Please note that a blank source address is equivalent to **Any**.
Source Port	This is the source port number.
Dest. Address / Mask	This displays the destination IP addresses and subnet mask to which this rule applies. Please note that a blank destination address is equivalent to **Any**.
Dest. Port	This is the destination port number.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Remove** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.
Add	Click **Add** to create a new rule.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.

9.3.1 Creating Incoming Firewall Rules

In the **Incoming** screen, click **Add** to display this screen and refer to the following table for information on the labels.

Figure 71   Firewall > Incoming: Add

The following table describes the labels in this screen.

Table 46   Firewall > Incoming: Add

LABEL	DESCRIPTION
Active	Select this check box to enable the rule.
Filter Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces.
	To add a firewall rule, you need to configure at least one of the following fields (except the **Interface** field).
Protocol	Select the transport layer protocol (**TCP/UDP**, **TCP**, **UDP** or **ICMP**) and enter the protocol (service type) number in the port field. Select **NONE** to apply the rule to any protocol.
Source IP Address	Enter the source IP address in dotted decimal notation.
Source Subnet Mask	Enter the source subnet mask.
Source Port	Enter a single port number or the range of port numbers of the source.
Destination IP Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Mask	Enter the destination subnet mask.
Destination Port	Enter the port number of the destination.

Table 46 Firewall > Incoming: Add (continued)

LABEL	DESCRIPTION
Interface	Select **Select All** to apply the rule to all interfaces on the P-870HN-51D or select the specific WAN interface(s) to which this rule applies.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.

10

Certificate

10.1 Overview

The P-870HN-51D 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.

10.1.1 What You Can Do in this Chapter

• The **Local Certificates** screen lets you generate certification requests and import the P-870HN-51D's CA-signed certificates (Section 10.4 on page 154).

• The **Trusted CA** screen lets you save the certificates of trusted CAs to the P-870HN-51D (Section 10.4 on page 154).

10.2 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 P-870HN-51D to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

10.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. This is the P-870HN-51D's summary list of certificates and certification requests.

Figure 72 Local Certificates
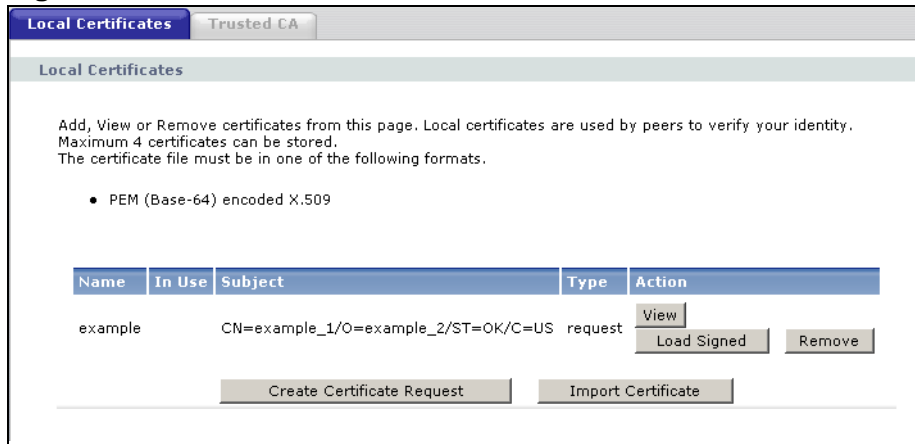
The following table describes the labels in this screen.

Table 47 Local Certificates

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
In Use	This field displays how many applications use the certificate.
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.
Type	This field displays what kind of certificate this is. **request** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **Load Certificate** screen to import the certificate and replace the request. **signed** represents a certificate issued by a certification authority.
Action	Click the **View** button to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Load Signed** button to import a valid certification to replace the request. Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

Table 47 Local Certificates (continued)

LABEL	DESCRIPTION
Create Certificate Request	Click this button to go to the screen where you can have the P-870HN-51D generate a certification request.
Import Certificate	Click this button to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the P-870HN-51D.

10.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the **My Certificate Create** screen. Use this screen to have the P-870HN-51D generate a certification request.

Figure 73 Create Certificate Request

The following table describes the labels in this screen.

Table 48 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. 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 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the P-870HN-51D drops trailing spaces.
State/Province Name	Type up to 127 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the P-870HN-51D drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.

Table 48 Create Certificate Request (continued)

LABEL	DESCRIPTION
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to begin certificate or certification request generation.

After you click **Apply**, the **Certificate Request Details** screen displays. Click **Load Signed Certificate** to import a certificate signed by the CA to replace the request (see). Otherwise, click **Back** to return to the **Local Certificates** screen. See for field information.

Figure 74 Certificate Request Details

10.3.2 Import Certificate

Click **Security > Certificates > Local Certificates** and then **Import Certificate** to open the **Import Local Certificate** screen. Follow the instructions in this screen to save an existing certificate to the P-870HN-51D.

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

Figure 75 Import Local Certificate

The following table describes the labels in this screen.

Table 49 Import Local Certificate

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the P-870HN-51D.
Private Key	Copy and paste the private key into the text box to store it on the P-870HN-51D.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the certificate on the P-870HN-51D.

10.3.3 Certificate Details

Click **Security** > **Certificates** > **Local Certificates** to open the **My Certificates** screen (see Figure 72 on page 148). Click the **View** icon to open the **Certificate Details** screen. Use this screen to view in-depth certificate information and change the certificate's name.

Figure 76 Certificate Details

The following table describes the labels in this screen.

Table 50 Certificate Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Type	This field displays general information about the certificate. **signed** means that a Certification Authority signed the certificate. **request** means this is a certification request.

Table 50 Certificate Details (continued)

LABEL	DESCRIPTION
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organization (O), State (ST) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. This displays **null** in a certification request. 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).
Private Key	This read-only text box displays the private key in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the private key 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).
Signing Request	This read-only text box displays the request information in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. This displays **null** in a signed certificate.
Back	Click **Back** to return to the previous screen.
Load Signed Certificate	This button is available only in a certification request details screen Click this to import a certificate signed by the CA to replace the request.

10.3.4 Load Signed Certificate

Click **Security > Certificates > Local Certificates** and then **Load Signed** or the **Load Signed Certificate** button in the **Certificate Details** screen of a certification request to open the **Load Certificate** screen. Follow the instructions in this screen to save a valid certificate to repalce the request.

Figure 77   Load Certificate

The following table describes the labels in this screen.

Table 51   Load Certificate

LABEL	DESCRIPTION
Certificate Name	This field is read-only and displays the identifying name of this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the P-870HN-51D.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the certificate on the P-870HN-51D.

10.4 The Trusted CA Screen

Click **Advanced Setup > 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 P-870HN-51D to accept as trusted. The P-870HN-51D 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 78   Trusted CA
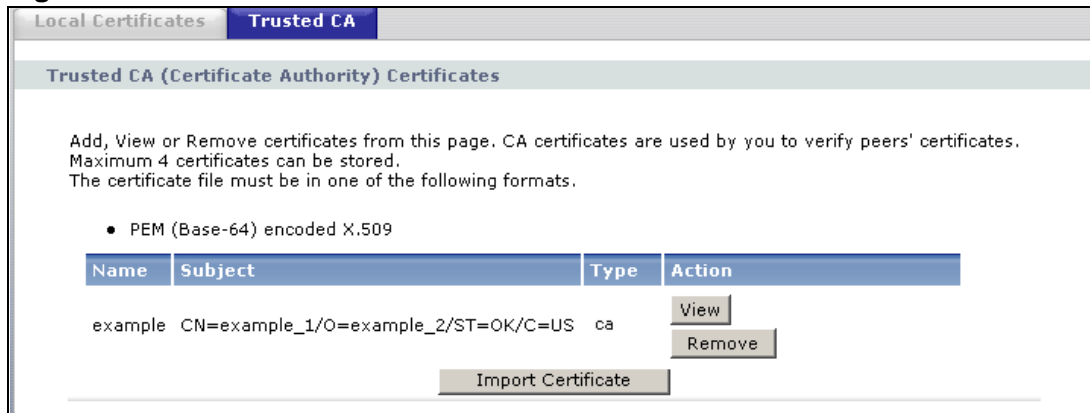
The following table describes the fields in this screen.

Table 52   Trusted CA

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

Click **Remove** to delete the certificate. |
| Import Certificate | Click this button to open a screen where you can save the certificate of a certification authority that you trust to the P-870HN-51D. |

10.4.1 View Trusted CA Certificate

Click the **View** button 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 79   Trusted CA: View

The following table describes the fields in this screen.

Table 53   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 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this button to return to the previous screen.

10.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The P-870HN-51D trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 80   Trusted CA: Import Certificate

The following table describes the fields in this screen.

Table 54   Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate Name	Enter the name that identifies this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the P-870HN-51D.
Back	Click this button to return to the previous screen.
Apply	Click this button to save your changes back to the P-870HN-51D.

Static Route

11.1 Overview

The P-870HN-51D usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the P-870HN-51D send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the P-870HN-51D's LAN interface. The P-870HN-51D routes most traffic from **A** to the Internet through the P-870HN-51D'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 81   Example of Static Routing Topology
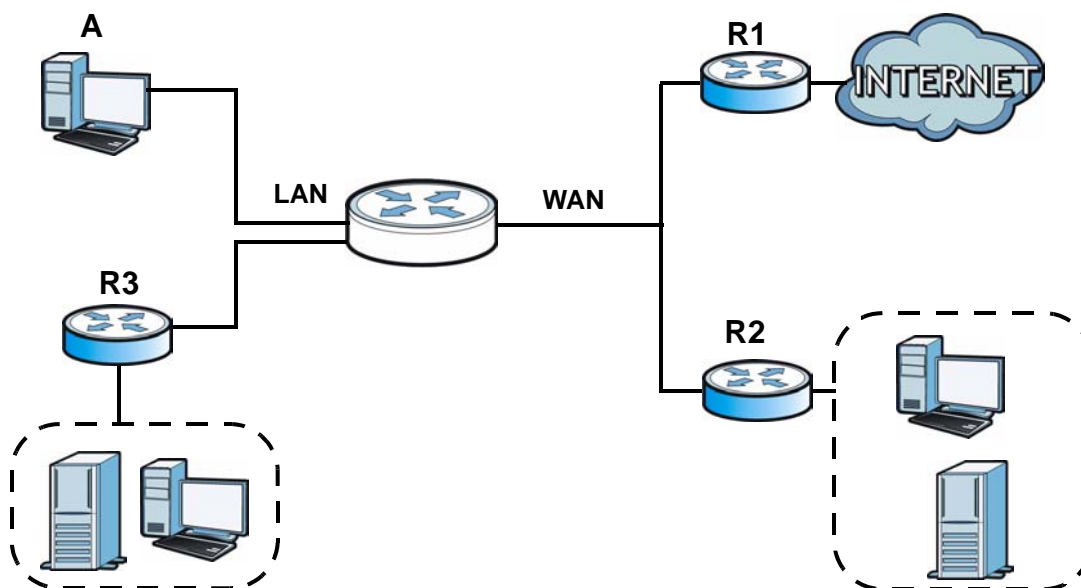
11.1.1 What You Can Do in this Chapter

The **Static Route** screens let you view and configure IP static routes on the P-870HN-51D (Section 11.2 on page 160).

11.2 The Static Route Screen

Click **Advanced > Static Route** to open the **Static Route** screen.

Figure 82   Advanced > Static Route

The following table describes the labels in this screen.

Table 55   Advanced > Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Netmask	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 through which the traffic is routed.
Remove	Click the icon to remove a static route from the P-870HN-51D. A window displays asking you to confirm that you want to delete the route.
Add	Click this to create a new rule.
Apply	Click this to apply your changes to the P-870HN-51D.

11.2.1 Static Route Edit

Click the **Add** button in the **Static Route** screen. Use this screen to configure the required information for a static route.

Figure 83   Static Route: Add

The following table describes the labels in this screen.

Table 56   Static Route: Add

LABEL	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **WAN** screens.
Use Gateway IP Address	Select this option and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your P-870HN-51D's interface(s). The gateway helps forward packets to their destinations.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Policy Forwarding

12.1 Overview

Traditionally, routing is based on the destination address only and the P-870HN-51D takes the shortest path to forward a packet. Policy forwarding allows the P-870HN-51D 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.

12.1.1 What You Can Do in this Chapter

The **Policy Forwarding** screens let you view and configure routing policies on the P-870HN-51D (Section 12.2 on page 163).

12.2 The Static Route Screen

Click **Advanced > Policy Forwarding** to open the **Policy Forwarding** screen.

Figure 84   Advanced > Policy Forwarding

Policy Name	SourceIP	Protocol	SourcePort	SourceMac	WAN	Remove
test	192.168.1.99	TCP	23		ptm0_1	🗑

A maximum 8 entries can be configured.
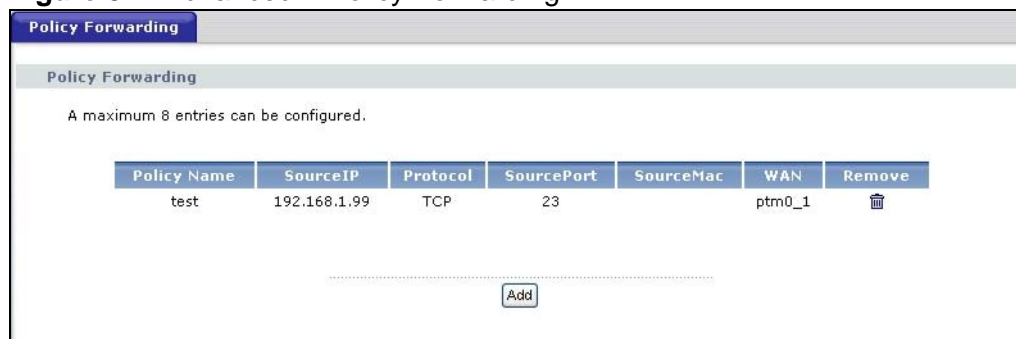
The following table describes the labels in this screen.

Table 57 Advanced > Policy Forwarding

LABEL	DESCRIPTION
Policy Name	This is the name of the rule.
SourceIP	This is the source IP address.
Protocol	This is the transport layer protocol.
SourcePort	This is the source port number.
SourceMAC	This is the source MAC address.
Interface	This is the WAN interface through which the traffic is routed.
Remove	Click the icon to remove a rule from the P-870HN-51D. A window displays asking you to confirm that you want to delete the rule.
Add	Click this to create a new rule.

12.2.1 Policy Forwarding Setup

Click the **Add** button in the **Policy Forwarding** screen. Use this screen to configure the required information for a policy route.

Figure 85   Policy Forwarding: Add

The following table describes the labels in this screen.

Table 58   Policy Forwarding: Add

LABEL	DESCRIPTION
Policy Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces.
Source IP Address	Enter the source IP address.
Protocol	Select the transport layer protocol (**TCP** or **UDP**).
Source Port	Enter the source port number.
Source Mac Address	Enter the source MAC address.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **WAN** screens.

Table 58 Policy Forwarding: Add

LABEL	DESCRIPTION
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

RIP

13.1 Overview

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

13.1.1 What You Can Do in this Chapter

The **RIP** screen lets you set up RIP settings on the P-870HN-51D (Section 13.2 on page 167).

13.2 The RIP Screen

Click **Advanced > RIP** to open the **RIP** screen.

Figure 86   Advanced > RIP

The following table describes the labels in this screen.

Table 59 Advanced > RIP

LABEL	DESCRIPTION
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 P-870HN-51D 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 P-870HN-51D update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface.
	Select **Active** to have the P-870HN-51D advertise its route information and also listen for routing updates from neighboring routers.
Enabled	Select the check box to activate the settings.
Apply/Save	Click **Apply/Save** to save your changes back to the P-870HN-51D.

Quality of Service (QoS)

14.1 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 P-870HN-51D 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 P-870HN-51D 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.

14.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth (Section 14.3 on page 170).
- The **Queue Setup** screen lets you lets you configure QoS queue assignment (Section 14.4 on page 172).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers (Section 14.5 on page 174).
- The **Policer Setup** screen lets you control ingress (or incoming) traffic (Section 14.6 on page 180).

• The **Monitor** screen lets you view the P-870HN-51D's QoS-related packet statistics (Section 14.7 on page 183).

14.2 What You Need to Know

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.

14.3 The Quality of Service General Screen

Use this screen to enable or disable QoS, set the upstream bandwidth for WAN and downsteam bandwidth for LAN/WLAN.

Upstream bandwdith refers to resources alloted to traffic, which goes from the LAN device to the WAN device. On the other hand, downstream bandwidth refers to resources alloted to traffic that comes back from the WAN device to the LAN device

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

Figure 87 QoS General

The following table describes the labels in this screen.

Table 60 QoS General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interface that you want to allocate using QoS.
	The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps.
	You can set this number higher than the interface's actual transmission speed. The P-870HN-51D 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.
	You can also set this number lower than the interface's actual transmission speed. This will cause the P-870HN-51D to not use some of the interface's available bandwidth.
	If you leave this field blank, the P-870HN-51D automatically sets this number to be 95% of the DSL port's actual upstream transmission speed.
LAN/WLAN Managed Downstream Bandwidth	Enter the amount of downstream bandwidth for the LAN and WLAN interfaces that you want to allocate using QoS.
	This value depends on what the network adapter supports. If the network adapter supports at least 100 Mbps, the effective value for the field is any value between 1 Kbps to 100 Mbps. The default value is 100 Mbps.

Table 60 QoS General

LABEL	DESCRIPTION
Upstream traffic priority will be automatically assigned by	This field is ignored if traffic matches a class you previously configured in the **Advanced > QoS > Class Setup screen.** If traffic does not match a class configured in the **Class Setup** screen, the P-870HN-51D assigns priority to unmatched traffic based on what you select in this field: **Ethernet Priority**, **IP Precedence** and/or **Packet Length**. See Section 14.8.1 on page 185 for more information on these traffic priority schemes. If you do not configure this field, traffic which does not match a class is mapped to queue two.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.4 The Queue Setup Screen

Click **QoS > Queue Setup** to open the screen as shown next. Use this screen to configure QoS queue assignment.

Figure 88 QoS Queue Setup

The following table describes the labels in this screen.

Table 61 QoS Queue Setup

LABEL	DESCRIPTION
Add	Click this button to create a new entry.
No.	This is the index number of this entry.
Active	Select the check box to enable the queue.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the P-870HN-51D's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.

Table 61   QoS Queue Setup

LABEL	DESCRIPTION
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the P-870HN-51D 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 go to the screen where you can edit the queue. Click the **Remove** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.

14.4.1 Adding a QoS Queue

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

Figure 89   QoS Queue Setup: Add

The following table describes the labels in this screen.

Table 62   QoS Queue Setup: Add

LABEL	DESCRIPTION
Enable	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.
Priority	Select the priority level (from 1 to 3) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.

Table 62   QoS Queue Setup: Add

LABEL	DESCRIPTION
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the P-870HN-51D 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 P-870HN-51D 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.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.5 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 P-870HN-51D 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 **QoS > Class Setup** to open the following screen.

Figure 90   QoS Class Setup

The following table describes the labels in this screen.

Table 63 QoS Class Setup

LABEL	DESCRIPTION
Add	Click this button to create a new classifier.
Order	This field displays the index number of the classifier.
Active	Select the check box to enable 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 and the source MAC address of traffic that matches this classifier.
Forward To	This is the interface through which traffic that matches this classifier is forwarded out.
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 go to the screen where you can edit the classifier. Click the **Remove** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.

14.5.1 QoS Class Edit

Click the **Add** button or the **Edit** icon in the **Class Setup** screen to configure a classifier.

Figure 91   QoS Class Setup: Add

The following table describes the labels in this screen.

Table 64 QoS Class Configuration

LABEL	DESCRIPTION
Class Configuration	
Enable	Select to enable or disable this classifier.
Class Name	Enter a descriptive name of up to 20 printable English keyboard characters, 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**. Select **Last** to put this rule in the back of the classifier list.
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the P-870HN-51D forward traffic of this class according to the default routing table.
DSCP Mark	This field is available only when you select the **Ether Type** check box. If you select **Mark**, enter a DSCP value with which the P-870HN-51D replaces the DSCP field in the packets. If you select **Auto Mapping** and there is a VLAN tag carried in the matched packets, the P-870HN-51D will replace the IP ToS field with the 802.1p priority field. If you select **Unchange**, the P-870HN-51D keep the DSCP field in the packets.
802.1p Mark	Select a priority level with which the P-870HN-51D replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the P-870HN-51D keep the 802.1p priority field in the packets.
VLAN ID Tag	If you select **Remark**, enter a VLAN ID number (between 1 and 4095) with which the P-870HN-51D replaces the VLAN ID of the frames. If you select **Remove**, the P-870HN-51D deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the P-870HN-51D treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the P-870HN-51D keep the VLAN ID in the packets.
To Queue	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Criteria Configuration	
Use the following fields to configure the criteria for traffic classification.	
Basic	
From Interface	Select from which Ethernet port or wireless interface traffic of this class should come.

Table 64 QoS Class Configuration (continued)

LABEL	DESCRIPTION
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select **8021Q**, you can configure an 802.1p priority level and VLAN ID in the **Others** section.
Source	
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP 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.
IP Subnet Mask	Enter the source subnet mask.
TCP/UDP 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.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
MAC Address	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified 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.
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.
TCP/UDP 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.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	

Table 64 QoS Class Configuration (continued)

LABEL	DESCRIPTION
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and select a priority level (between 0 and 7) from the drop down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and specify a VLAN ID number between 1 and 4095.
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. 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.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 28 to 1500) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
DHCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select a DHCP option. 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. 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.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.6 The Policer Setup Screen

A policer is a QoS policy.

Click **QoS > Policer Setup** to open the following screen. The P-870HN-51D can control ingress (or incoming) traffic by dropping packets that exceed the committed rate and/or committed burst size specified in this screen.

Figure 92   QoS > Policer

The following table describes the labels in this screen.

Table 65   QoS > Policer Setup

LABEL	DESCRIPTION
Add	Click this button to create a new policy.
No	This field displays the index number of the policy.
Active	Select the check box to enable the policy.
Name	This is the name of the policy.
Regulated Classes	This shows to which classes the policy applies.
Meter Type	This shows the method that the P-870HN-51D uses for determining which packets to pass, drop or mark (DSCP), whether it's **Simple Token Bucket**, **Single Rate Three Color Meter** or **Two Rate Three Color Meter**. Refer to Section 14.8.2 on page 186 for information on these meter types.
Parameter	**Committed Rate** - This shows the maximum committed rate for the specified class/es. **Committed Burst Size** - This shows the maximum committed burst size for the specified class/es.

Table 65   QoS > Policer Setup (continued)

LABEL	DESCRIPTION
Action	**Conforming Action -** This shows the action that the P-870HN-51D applies to packets that conform to the meter type selected, and can be **Pass**, **Drop** or **DSCP mark**. **Non Conforming Action -** This shows the action that the P-870HN-51D applies to packets that do not conform to the meter type selected, and can be **Pass**, **Drop** or **DSCP mark**. • **Pass** - the packet is allowed to flow to its destination. • **Drop** - the packet is discarded. • **DSCP mark** - the packet is given a DSCP mark and processed accordingly. See Section 14.8.1 on page 185 for information on DSCP mark.
Modify	Click the **Edit** icon to go to the screen where you can edit the classifier. Click the **Remove** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.

14.6.1 Policer Setup Add/Edit

Figure 93   QoS > Policer: Edit

The following table describes the labels in this screen.

Table 66 QoS > Policer Setup: Edit

LABEL	DESCRIPTION
Enable	Select this to have the P-870HN-51D pass, drop or mark packets that exceed the committed rate and/or committed burst size specified in this screen.
Meter Type	Select the method that the P-870HN-51D uses for determining which packets to pass, drop or mark (DSCP). Choices are: **Simple Token Bucket**, **Single Rate Three Color Meter** and **Two Rate Three Color Meter**. Refer to Section 14.8.2 on page 186 for information on these meter types.
Committed Rate	Enter the maximum committed rate for the specified class/es.
Committed Burst Size	Enter the maximum committed burst size for the specified class/es.
Conforming Action	Select the action that the P-870HN-51D applies to packets that conform to the meter type selected. Choices are **Pass**, **Drop** and **DSCP mark**. • **Pass** - the packet is allowed to flow to its destination. • **Drop** - the packet is discarded. • **DSCP mark** - the packet is given a DSCP mark and processed accordingly. See Section 14.8.1 on page 185 for information on DSCP mark.
Non-comforming Action	Select the action that the P-870HN-51D applies to packets that do not conform to the meter type selected. Choices are **Pass**, **Drop** and **DSCP mark**. • **Pass** - the packet is allowed to flow to its destination. • **Drop** - the packet is discarded. • **DSCP mark** - the packet is given a DSCP mark and processed accordingly. See Section 14.8.1 on page 185 for information on DSCP mark.
Regularted Classes Member Setting	Use the **Add** and **Remove** buttons to select or deselect classes to which the policy applies.
Available Class	This shows the available classes.
Selected Class	This shows classes to which the policy applies.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.7 The QoS Monitor Screen

To view the P-870HN-51D's QoS packet statistics, click **Advanced > QoS > Monitor**. The screen appears as shown.

Figure 94   QoS > Monitor

The following table describes the labels in this screen.

Table 67   QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the P-870HN-51D to update this screen. Select **No Refresh** to stop refreshing statistics.
Interface Monitor	
No.	This is the index number of the entry.
Name	This shows the name of the WAN interface on the P-870HN-51D.
Pass	This shows how many packets forwarded to this interface are transmitted successfully.
Drop	This shows how many packets forwarded to this interface are dropped.
Queue Monitor	
No.	This is the index number of the entry.
Name	This shows the name of the queue.
Pass	This shows how many packets assigned to this queue are transmitted successfully.
Drop	This shows how many packets assigned to this queue are dropped.

183

14.8 Technical Reference

The following section contains additional technical information about the P-870HN-51D 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 68   IEEE 802.1p Priority Level and Traffic Type

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

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.

DSCP (6 bits)	Unused (2 bits)

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

14.8.1 Automatic Priority Queue Assignment

If you enable QoS on the P-870HN-51D, the P-870HN-51D can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the P-870HN-51D. On the P-870HN-51D, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 69   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

Table 69 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)
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

14.8.2 Traffic Policing Meter Types

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.

Simple Token Bucket is similar to tokens in a bucket to control when traffic can be transmitted. The bucket is a buffer that temporarily stores outgoing packets and transmits them at an average rate.

Single Rate Three Color Marker (SRTCM) and **Two Rate Three Color Marker** (TRTCM) evaluate incoming packets and mark them with one of three colors which

refer to packet loss priority (PLP) levels. High PLP level is referred to as red, medium is referred to as yellow and low is referred to as green. The difference between the two meters is the types of parameters used to evaluate packets. SRTCM uses committed information rate (CIR), the committed burst size and the excess burst size. TRTCM uses peak information rate (PIR), CIR, peak burst size and a committed burst size. After SRTCM and TRTCM are configured and DiffServ is enabled the following actions are performed on the colored packets:

• Red (high loss priority level) packets are dropped.

• Yellow (medium loss priority level) packets are dropped if there is congestion on the network.

• Green (low loss priority level) packets are forwarded.

15

Dynamic DNS Setup

15.1 Overview

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

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

15.1.1 What You Can Do in this Chapter

Use the **Dynamic DNS** screen (Section 15.3 on page 190) to enable DDNS and configure the DDNS settings on the P-870HN-51D.

15.2 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.

15.3 The Dynamic DNS Screen

To change your P-870HN-51D's DDNS, click **Advanced > Dynamic DNS**. The screen appears as shown.

Figure 95   Advanced > Dynamic DNS

The following table describes the fields in this screen.

Table 70   Advanced > Dynamic DNS

LABEL	DESCRIPTION
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your P-870HN-51D by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Interface	Select the WAN interface to use for updating the IP address of the domain name.
User Name	Type your user name.
Password	Type the password assigned to you.
Email	Enter the user name you used to register for this service.
Key	Enter the password you used to register for this service.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Remote Management

16.1 Overview

This chapter explains how to configure the remote management and access control settings on the P-870HN-51D.

16.1.1 What You Can Do in this Chapter

• The **TR-069** screen lets you configure the P-870HN-51D's TR-069 auto-configuration settings (Section 16.3 on page 193).

• The **TR-064** screen lets you enable management via TR-064 on the P-870HN-51D (Section 16.3 on page 193).

• The **Service Control** screens let you configure through which interface(s) users can use which service(s) to manage the P-870HN-51D (Section 16.4 on page 194).

• The **IP Address** screens let you configure from which IP address(es) users can use a service to manage the P-870HN-51D (Section 16.5 on page 195).

16.2 The TR-069 Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your P-870HN-51D, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the P-870HN-51D, modify settings, perform firmware upgrades as well as monitor and diagnose the P-870HN-51D. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Advanced > Remote MGMT** to open the following screen. Use this screen to configure your P-870HN-51D to be managed by an ACS.

Figure 96 TR-069

The following table describes the fields in this screen.

Table 71 TR-069

LABEL	DESCRIPTION
Inform	Select **Enable** to activate remote management via TR-069 on the WAN. Otherwise, select **Disable**.
Inform Interval	Enter the time interval (in seconds) at which the P-870HN-51D sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes. If you select **Multi_WAN**, you should also select the pre-configured WAN connection(s).
Display SOAP messages on serial console	Select **Enable** to show the SOAP messages on the console.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the P-870HN-51D, this user name is used to authenticate the ACS.

Table 71 TR-069 (continued)

LABEL	DESCRIPTION
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the P-870HN-51D, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the P-870HN-51D.
Apply/Save	Click this button to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.3 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 **Advanced > Remote MGMT** > **TR064** to open the following screen.

Figure 97 TR-064

The following table describes the fields in this screen.

Table 72 TR-064

LABEL	DESCRIPTION
Enable TR064	Select the check box to activate management via TR-064 on the LAN.
Enable Authenticator	Some TR-064 commands require authentication before it can be executed. Select this to have the P-870HN-51D authenticate the user before running the command. Deselect this to disable authentication and have the P-870HN-51D run all commands.
Apply	Click this button to save your changes back to the P-870HN-51D.

16.4 The Service Control Screen

Click **Advanced > Remote MGMT > Service Control** to open the following screen. Use this screen to decide what services you may use to access which P-870HN-51D interface.

Figure 98 Service Control

The following table describes the fields in this screen.

Table 73 Access Control: Services

LABEL	DESCRIPTION
Service Control	Select **Enable** to turn on service control. Otherwise, select **Disable**.
#	This is the index number of the entry.
Services	This is the service you may use to access the P-870HN-51D.
LAN	Select the **Enable** check box for the corresponding services that you want to allow access to the P-870HN-51D from the LAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the P-870HN-51D from the WAN.
Apply	Click this button to save your changes back to the P-870HN-51D.

16.5 The IP Address Screen

Click **Advanced > Remote MGMT > IP Address** to open the following screen. Use this screen to specify the "trusted" computers from which an administrator may use a service to manage the P-870HN-51D.

Figure 99   IP Address

The following table describes the fields in this screen.
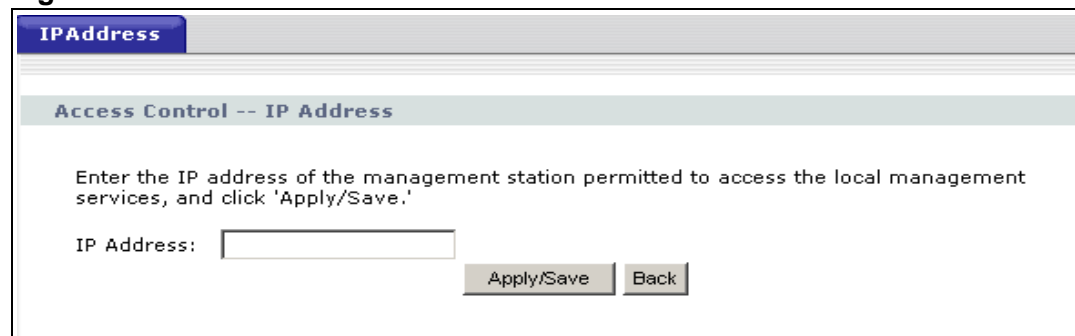
Table 74   IP Address

LABEL	DESCRIPTION
Access Control Mode	Select **Enable** to activate the secured client list. Select **Disable** to disable the list without deleting it.
IP Address	This is the IP address of the trusted computer from which you can manage the P-870HN-51D.
Remove	Select this check box and click the **Remove** button to delete this entry from the P-870HN-51D.
Add	Click this button to create a new entry.
Remove	Click this button to delete the selected entry.

16.5.1 Adding an IP Address

Click the **Add** button in the **IP Address** screen to open the following screen.

Figure 100   IP Address: Add

The following table describes the fields in this screen.

Table 75   IP Address: Add

LABEL	DESCRIPTION
IP Address	Enter the IP address of the trusted computer from which you can manage the P-870HN-51D.
Apply/Save	Click this button to save your changes back to the P-870HN-51D.
Back	Click this button to return to the previous screen without saving.

Universal Plug-and-Play (UPnP)

17.1 Overview

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

17.1.1 What You Can Do in this Chapter

The **UPnP** screen lets you enable UPnP on the P-870HN-51D ().

17.2 What You Need to Know

How do I know if I'm using UPnP?

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

NAT Traversal

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

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

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

See the NAT chapter for more information on NAT.

Cautions with UPnP

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

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the P-870HN-51D allows multicast messages on the LAN only.

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

UPnP and ZyXEL

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

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

17.3 The UPnP Screen

Click **Advanced > UPnP** to display the screen shown next.

See for more information.

Figure 101   Advanced > UPnP
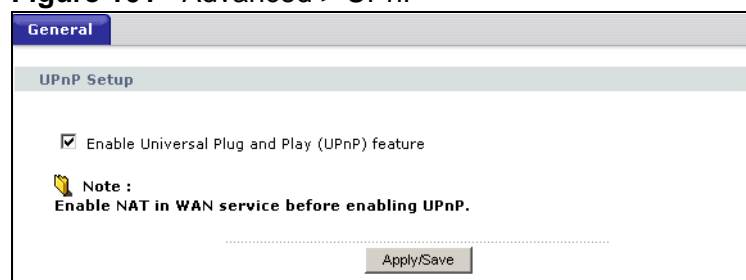
The following table describes the fields in this screen.

Table 76 Advanced > UPnP

LABEL	DESCRIPTION
Enable Universal Plug and Play (UPnP) Feature	Select this check box to enable UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the P-870HN-51D's IP address (although you must still enter the password to access the web configurator).
Apply/Save	Click this to save the setting to the P-870HN-51D.

17.4 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**.

Figure 102   Add/Remove Programs: Windows Setup: Communication
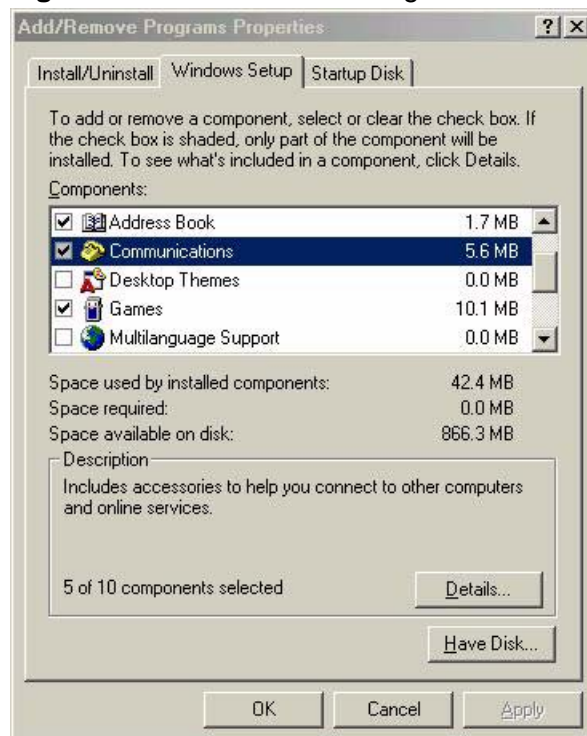
3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 103 Add/Remove Programs: Windows Setup: Communication: Components
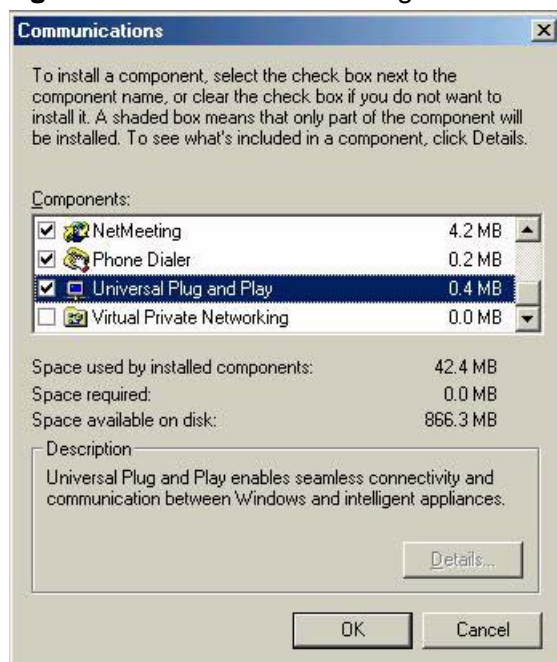
4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

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** ….

Figure 104   Network Connections

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

Figure 105   Windows Optional Networking Components Wizard
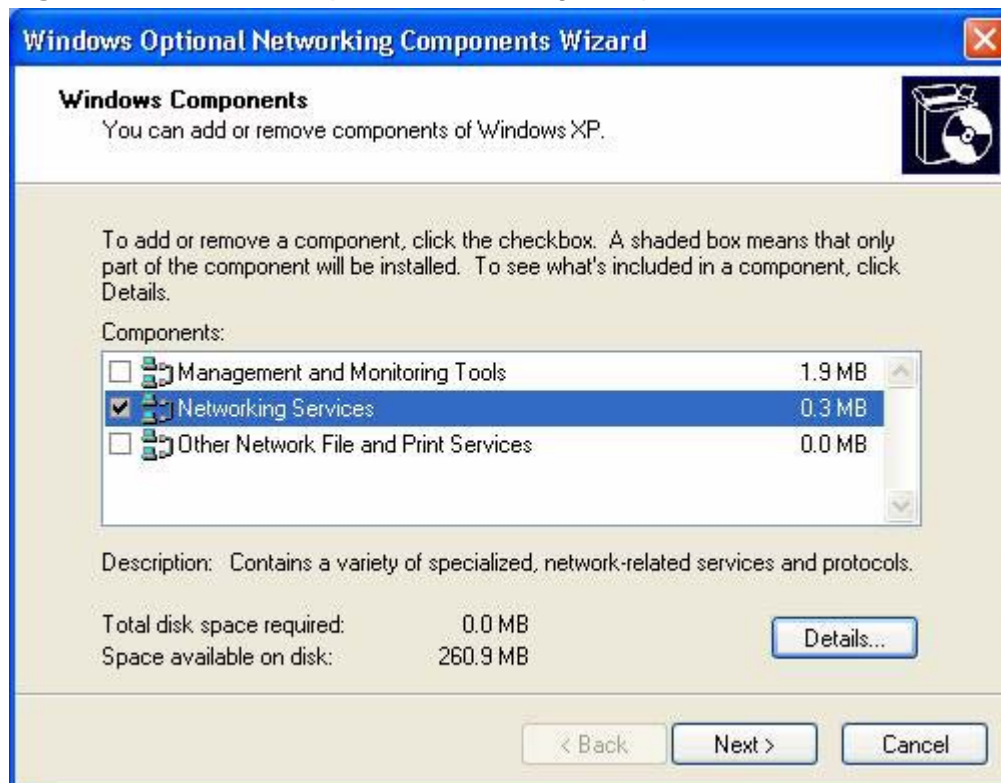
5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 106 Networking Services
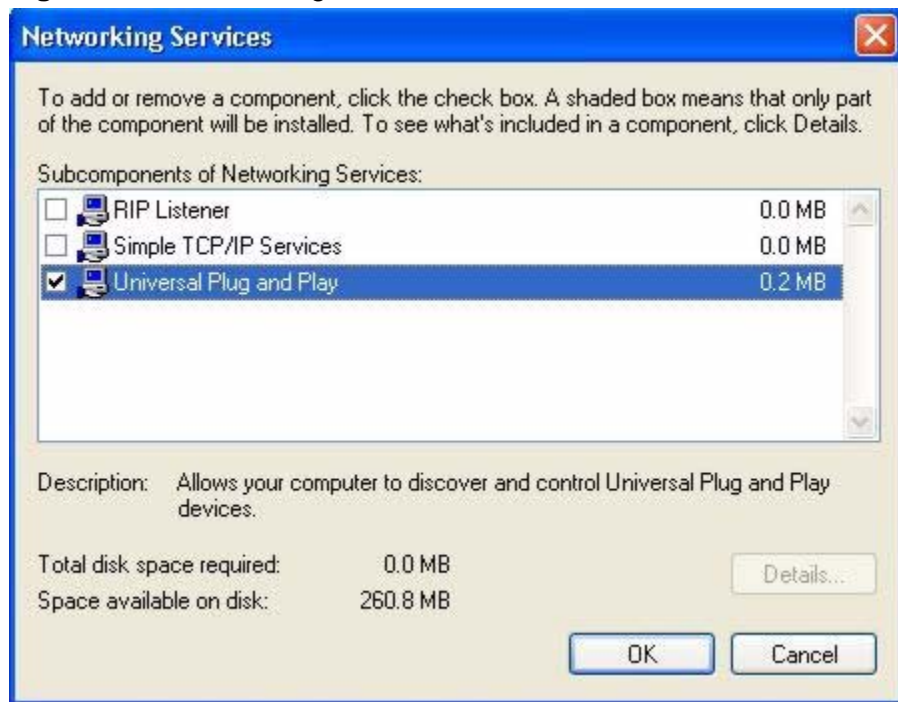
6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

17.5 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the P-870HN-51D.

Make sure the computer is connected to a LAN port of the P-870HN-51D. Turn on your computer and the P-870HN-51D.

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**.

Figure 107 Network Connections

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

Figure 108 Internet Connection Properties

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

Figure 109 Internet Connection Properties: Advanced Settings
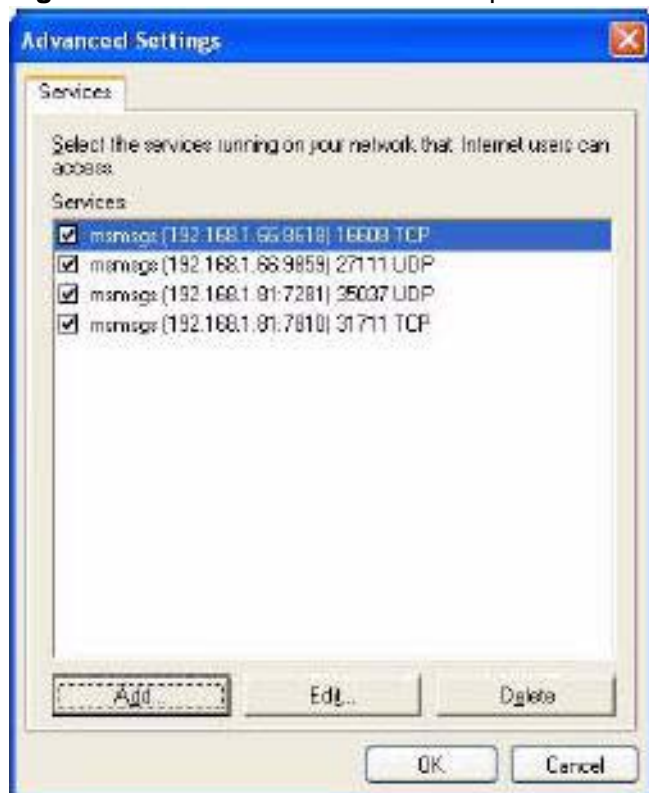
Figure 110 Internet Connection Properties: Advanced Settings: Add
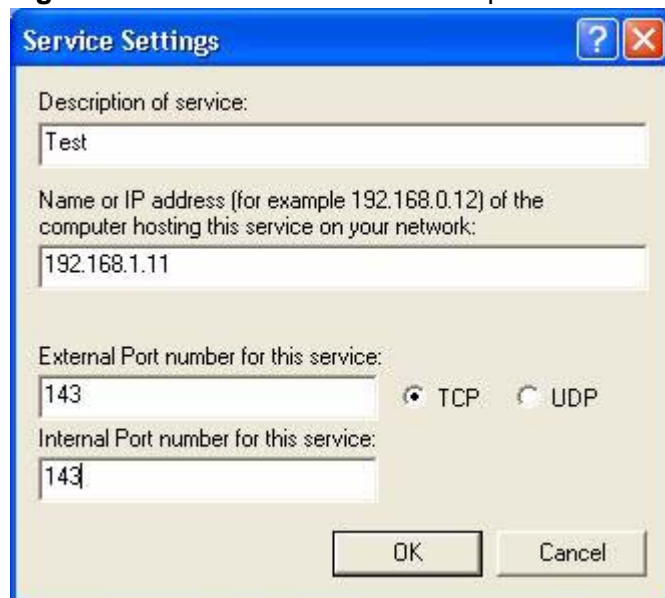
5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

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

Figure 111 System Tray Icon

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

Figure 112 Internet Connection Status

Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the P-870HN-51D without finding out the IP address of the P-870HN-51D first. This comes helpful if you do not know the IP address of the P-870HN-51D.

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**.

Figure 113 Network Connections
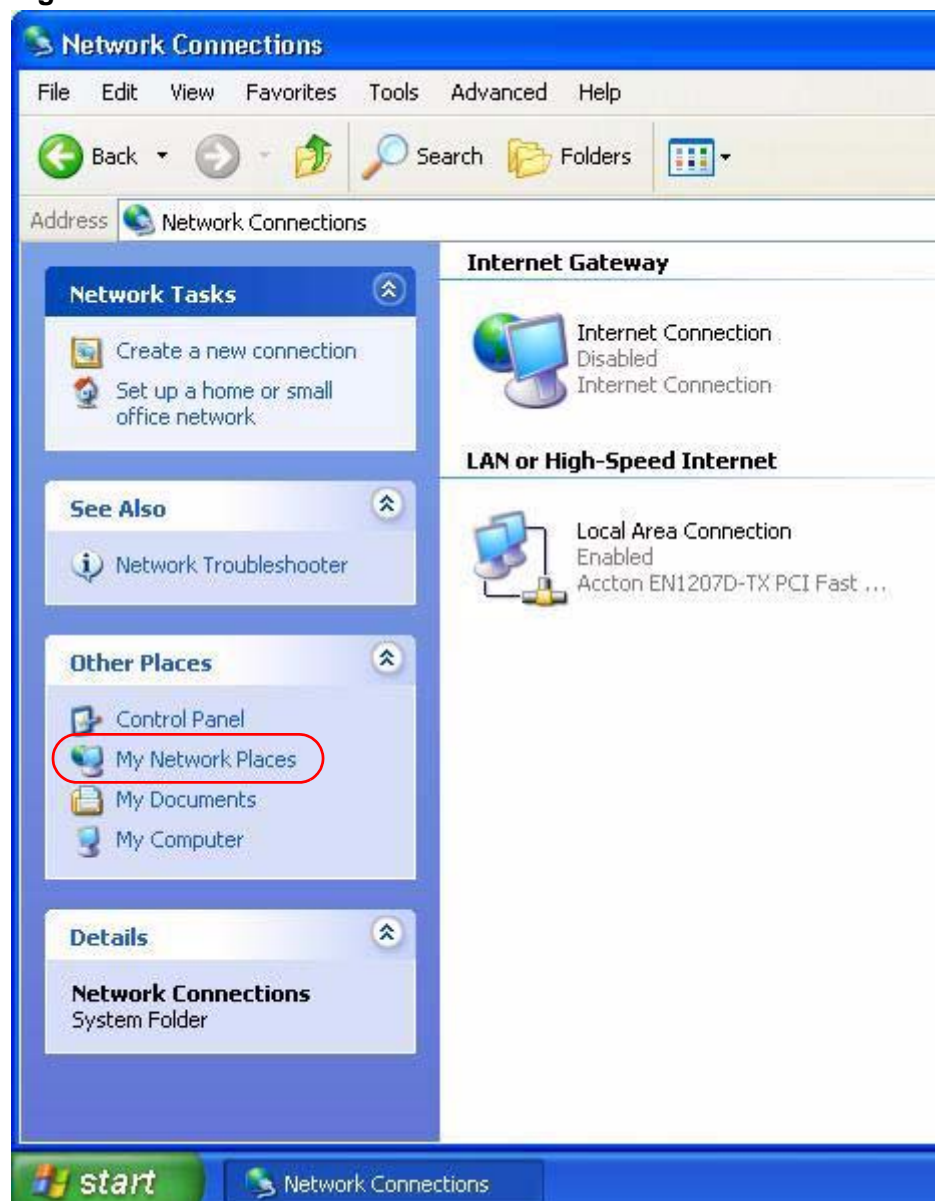
4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your P-870HN-51D and select **Invoke**. The web configurator login screen displays.

Figure 114 Network Connections: My Network Places

6 Right-click on the icon for your P-870HN-51D and select **Properties**. A properties window displays with basic information about the P-870HN-51D.

Figure 115 Network Connections: My Network Places: Properties: Example
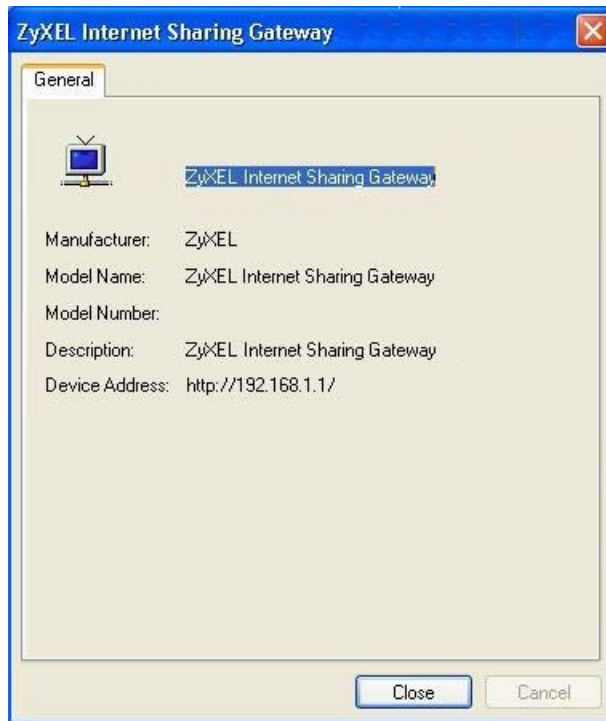
Parental Control

18.1 Overview

Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the P-870HN-51D performs parental control on a specific user.

18.1.1 What You Can Do in this Chapter

• The **Time Restriction** screen lets you give different time restrictions to each user of your network (Section 18.2 on page 209).

• The **URL Filter** screen lets you restrict home network users from viewing inappropriate websites (Section 18.3 on page 211).

18.2 The Time Restriction Screen

Use this screen to view the schedules and enable parental control on a specific user during certain periods.

Click **Advanced Setup > Parental Control** to open the following screen.

Figure 116   Parental Control > Time restriction

The following table describes the fields in this screen.

Table 77 Parental Control > Time Restriction

LABEL	DESCRIPTION
#	This shows the index number of the schedule.
Active	Select the check box to enable the schedule.
username	This shows the name of the user.
MAC	This shows the MAC address of the LAN user's computer to which this schedule applies.
Mon ~ Sun	**x** indicates the day(s) on which parental control is enabled.
Start	This shows the time when the schedule starts.
Stop	This shows the time when the schedule ends.
Modify	Click the **Edit** icon to go to the screen where you can edit the schedule. Click the **Remove** icon to delete an existing schedule.
Add	Click **Add** to create a new schedule.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.

18.2.1 Adding a Schedule

Click the **Add** button in the **Time Restriction** screen to open the following screen. Use this screen to configure a restricted access schedule for a specific user on your network.

Figure 117   Time Restriction Configuration

The following table describes the fields in this screen.

Table 78 Time Restriction Configuration

LABEL	DESCRIPTION
User Name	Enter the name of the user.
MAC Address	Enter the MAC address of the LAN user's computer to which this schedule applies.
Days of the week	Select check boxes for the days that you want the P-870HN-51D to perform parental control.
Start Blocking Time End Blocking Time	Enter the time period of each day, in 24-hour format, during which parental control will be enforced.
Back	Click this button to return to the previous screen without saving any changes.
Save/Apply	Click this button to save your settings back to the P-870HN-51D.

18.3 The URL Filter Screen

Use this screen to configure URL filtering settings to allow or block the users on your network from accessing certian web sites.

Click **Advanced Setup > Parental Control > URL Filter** to open the following screen.

Figure 118   Parental Control > URL Filter

The following table describes the fields in this screen.

Table 79   Parental Control > URL Filter

LABEL	DESCRIPTION
Enable URL Filter	Select the check box to enable URL filtering on the P-870HN-51D.
#	This is the index number of the rule.

Table 79 Parental Control > URL Filter (continued)

LABEL	DESCRIPTION
Active	Select the check box to enable the filtering rule.
Address	This is the URL of the web site in this rule.
Port	This is the port number the web server uses to forward HTTP traffic.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Remove** icon to delete an existing rule.
Add	Click **Add** to create a new rule.
Apply	Click this button to save your settings back to the P-870HN-51D.

18.3.1 Adding URL Filter

Click the **Add** button in the **URL Filter** screen to open the following screen.

Figure 119   URL Filter Configuration

The following table describes the fields in this screen.

Table 80   URL Filter Configuration

LABEL	DESCRIPTION
URL Address	Enter the URL of web site to which the P-870HN-51D blocks or allows access.
Port Number	Specify the port number the web server uses to forward HTTP traffic.
Back	Click this button to return to the previous screen without saving any changes.
Save/Apply	Click this button to save your settings back to the P-870HN-51D.

19

Interface Group

19.1 Overview

By default, all LAN and WAN interfaces on the P-870HN-51D are in the same group and can communicate with each other. You can create multiple groups to have the P-870HN-51D assign the IP addresses in different domains to different groups. Each group acts as an independent network on the P-870HN-51D.

19.1.1 What You Can Do in this Chapter

The **Interface Group** screen lets you create multiple networks on the P-870HN-51D (Section 19.2 on page 213).

19.2 The Interface Group Screen

You can manually add a LAN interface to a new group. Alternatively, you can have the P-870HN-51D automatically add the incoming traffic and the LAN interface on which traffic is received to the new group when its source MAC address or DHCP option information matches the predefined filtering criteria.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the P-870HN-51D assigns to the clients in the default and/or user-defined groups. If you set the P-870HN-51D to assign IP addresses based on the client's source MAC address or DHCP 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 91 for more information.

In the following example, the client that sends packets with the source MAC address 00:19:cb:01:23:45 is assigned the IP address 192.168.2.2 and uses the WAN interface ptm0_2.

Figure 120 Interface Grouping Application
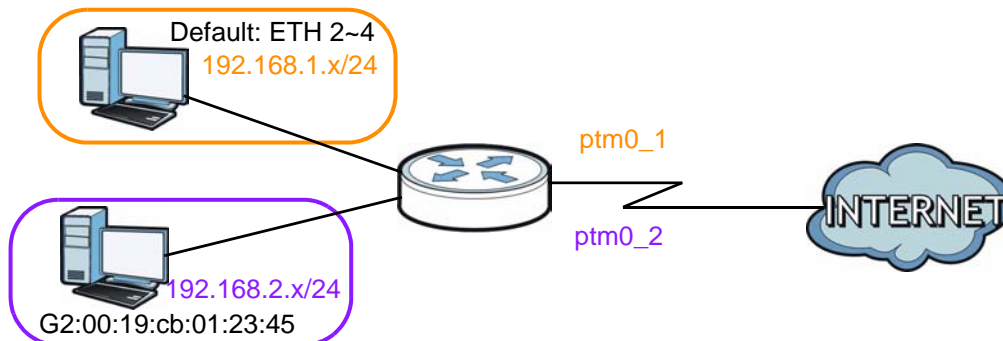
Click **Advanced Setup > Interface Group** to open the following screen.

Figure 121 Interface Group

The following table describes the fields in this screen.

Table 81 Interface Grouping

LABEL	DESCRIPTION
#	This shows the index number of the entry.
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 goup.
Remove	Click the **Remove** icon to delete the group.
Add	Click this button to create a new group.

19.2.1 Interface Group Configuration

Click the **Add** 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 a group only.

Figure 122   Interface Group Configuration

The following table describes the fields in this screen.

Table 82   Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group.
WAN Interfaces used in the grouping	Select a WAN interface to be used in this group. Select **None** to not add a WAN interface to this group.
Grouped LAN Interfaces Available LAN Interfaces	Select a LAN or wireless LAN interface in the **Available LAN Interfaces** and use the left-facing arrow to move it to the **Grouped LAN Interfaces** to add the interface to this group. To remove a LAN or wireless LAN interface from the **Grouped LAN Interfaces**, use the righ-facing arrow.
#	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.

Table 82   Interface Group Configuration (continued)

LABEL	DESCRIPTION
Remove	Click the **Remove** icon to delete this rule from the P-870HN-51D.
Add	Click this button to create a new rule.
Back	Click this button to return to the previous screen without saving any changes.
Apply	Click this button to save your settings back to the P-870HN-51D.

19.2.2 Interface Grouping Criteria

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

Figure 123   Interface Grouping Criteria

The following table describes the fields in this screen.

Table 83   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.
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 83 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. Select **DUID-EN** (DUID Assigned by Vendor Based upon Enterprise Number) to enter the vendor's registered enterprise number. 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. Select **Other** to enter any string that identifies the device in the **DUID** field.
Hardware type	Enter the 16-bit hardware type of the device from which the traffic comes. For example, Ethernet is 1 and Experimental Ethernet is 2.
Time	Enter the time (in seconds since midnight (UTC), January 1, 2000) the DUID is generated.
Link-layer address	Enter the MAC address of the device.
Enterprise number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Identifier	Enter a unique identifier assigned by the vendor.
DUID	Enter the DHCP Unique Identifier (DUID) of the device.
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.
Back	Click this button to return to the previous screen without saving any changes.
Apply	Click this button to save your settings back to the P-870HN-51D.

System Settings

20.1 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.

20.1.1 What You Can Do in this Chapter

• The **General** screen lets you configure system settings (Section 20.2 on page 219).

• The **Time Setting** screen lets you set the system time (Section 20.3 on page 220).

20.2 The General Screen

Use the **General** screen to configure system settings such as the system password.

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

Figure 124   Maintenance > System > General

The following table describes the labels in this screen.

Table 84 Maintenance > System > Genera

LABEL	DESCRIPTION
UserName	Type the user name you use to access 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 (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the P-870HN-51D.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

20.3 The Time Setting Screen

To change your P-870HN-51D's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the P-870HN-51D's time based on your local time zone.

Figure 125 Maintenance > System > Time Setting

The following table describes the fields in this screen.

Table 85 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time	
Current Time	This field displays the time of your P-870HN-51D. Each time you reload this page, the P-870HN-51D synchronizes the time with the time server.
Current Date	This field displays the date of your P-870HN-51D. Each time you reload this page, the P-870HN-51D synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this option to enter the time and date manually.
Get from Time Server	Select this option to have the P-870HN-51D get the time and date from the time server you specified below.
First NTP time server Second NTP time server Third NTP time server Fourth NTP time server Fifth NTP time server	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Select **None** if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
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).
Apply	Click **Apply** to save your changes back to the P-870HN-51D.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Logs

21.1 Overview

This chapter contains information about configuring general log settings and viewing the P-870HN-51D′s logs.

The web configurator allows you to choose which categories of events and/or alerts to have the P-870HN-51D log and then display the logs or have the P-870HN-51D send them to a syslog server.

21.1.1 What You Can Do in this Chapter

• The **View Log** screen lets you see the logs for the categories that you selected in the **Log Settings** screen (Section 21.2 on page 223).

• The **Log Settings** screen lets you configure to where the P-870HN-51D is to send logs and which logs and/or immediate alerts the P-870HN-51D is to record (Section 21.3 on page 224).

21.2 The View Log Screen

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 21.3 on page 224).

The log wraps around and deletes the old entries after it fills.

Figure 126 Maintenance > Logs > View Log

The following table describes the fields in this screen.

Table 86 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	Select a severity level of logs to view. The P-870HN-51D displays the logs with the severity level equal to or higher than what you selected.
#	This field is a sequential value and is not associated with a specific entry.
Date/Time	This field displays the time the log was recorded.
Severity	This field displays the severity level of the log.
System	This field displays the system module from which the logs come.
Message	This field states the reason for the log.

21.3 The Log Settings Screen

Use the **Log Settings** screen to configure to where the P-870HN-51D is to send logs and which logs and/or immediate alerts the P-870HN-51D is to record and display.

To change your P-870HN-51D's log settings, click **Maintenance > Logs** > **Log Settings**. The screen appears as shown.

Figure 127 Maintenance > Logs > Log Settings

The following table describes the fields in this screen.

Table 87 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Active	Select to enable or disable system logging.
Log Level	Select the severity level of the logs that you want the P-870HN-51D to display, record and send to the log server. The P-870HN-51D displays and records the logs with the severity level equal to or higher than what you selected.
Mode	Select **Local** to record the logs and store them in the local memory of the P-870HN-51D only. Select **Remote** to send logs to the specified log server. Select **Both** to record the logs and store them in the local memory and also send logs to the log server.
Syslog Server IP Address	Enter the server name or the IP address of the log server.
Syslog Server UDP Port	Enter the UDP port of the log server.
Apply	Click **Apply** to save your customized settings.

22

Tools

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your P-870HN-51D.

22.1 Overview

This chapter explains how to upload new firmware, manage configuration files and restart your P-870HN-51D.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your P-870HN-51D.

22.1.1 What You Can Do in this Chapter

- The **Firmware** screen lets you upload firmware to your device (Section 22.2 on page 228).

- The **Configuration** screen lets you backup and restore device configurations (Section 22.3 on page 230). You can also reset your device settings back to the factory default.

- The **Restart** screen lets you restart your P-870HN-51D (Section 22.4 on page 232).

22.2 The Firmware Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your P-870HN-51D. 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 P-870HN-51D while firmware upload is in progress!

Figure 128   Maintenance > Tools > Firmware

The following table describes the labels in this screen.

Table 88   Maintenance > Tools > Firmware

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the P-870HN-51D again.

Figure 129 Firmware Upload In Progress

DSL Router Update
Please Wait ...

Uploading is in progress. The DSL Router will reboot upon completion. This process will take about 2 minutes.

The P-870HN-51D automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 130 Network Temporarily Disconnected

ⓘ **Local Area Connection**
Network cable unplugged

⬇ᵪ 10:44

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 **Tools** to go back to the **Firmware** screen.

Figure 131 Error Message

DSL Router Update
Please Wait ...

Image uploading failed. The selected file contains an illegal image.

229

22.3 The Configuration Screen

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

Figure 132   Maintenance > Tools > Configuration

Backup Configuration

Backup Configuration allows you to back up (save) the P-870HN-51D's current configuration to a file on your computer. Once your P-870HN-51D is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the P-870HN-51D's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your P-870HN-51D.

Table 89   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.

Table 89 Restore Configuration

LABEL	DESCRIPTION
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Do not turn off the P-870HN-51D while configuration file upload is in progress.

After you see a "restore configuration successful" screen, you must then wait one minute before logging into the P-870HN-51D again.

Figure 133 Configuration Upload Successful

The P-870HN-51D automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 134 Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Tools > Configuration** to go back to the **Configuration** screen.

Figure 135   Configuration Upload Error

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the P-870HN-51D to its factory defaults. The following warning screen appears.

Figure 136   Reset Warning Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your P-870HN-51D. Refer to Section 1.6 on page 25 for more information on the **RESET** button.

22.4 The Restart Screen

System restart allows you to reboot the P-870HN-51D without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the P-870HN-51D reboot. This does not affect the P-870HN-51D's configuration.

Figure 137 Maintenance > Tools >Restart

23
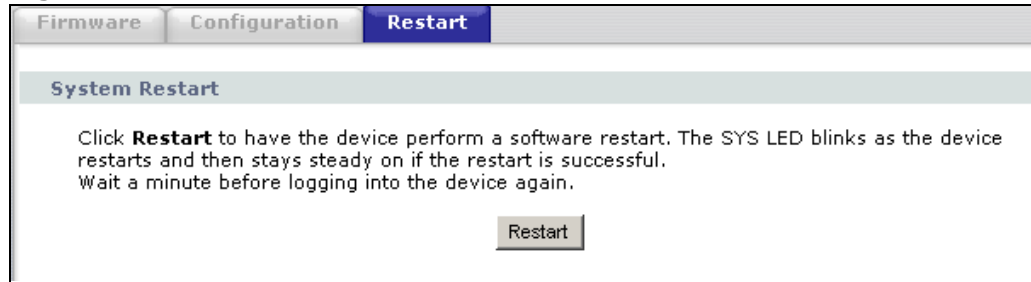
Diagnostic

23.1 Overview

The **Diagnostic** screens display information to help you identify problems with the P-870HN-51D.

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.

23.1.1 What You Can Do in this Chapter

• The **General** screen lets you ping an IP address or trace the route packets take to a host (Section 23.3 on page 236).

• The **802.1ag** screen lets you perform CFM actions (Section 23.4 on page 237).

23.2 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.

23.3 The General Diagnostic Screen

Click **Maintenance > Diagnostic** to open the screen shown next. Ping and traceroute help check availability of remote hosts and also help troubleshoot network or Internet connections.

Figure 138   Maintenance > Diagnostic > General

The following table describes the fields in this screen.

Table 90   Maintenance > Diagnostic > General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection or trace the route packets take to.
Ping	Click this button to ping the IP address that you entered.
Traceoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified host.

23.4 The 802.1ag Screen

Click **Diagnostic** to open the following screen. Use this screen to perform CFM actions.

Figure 139   802.1ag

The following table describes the fields in this screen.

Table 91   Maintenance > Diagnostic > 802.1ag

LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
Maintenance Domain (MD) Name	Type a name of up to 39 printable English keyboard characters for this MD. The combined length of the MD Name and MA name must be less or equal to 44bytes.
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.
Maintenance Association (MA) Name	Type a name of up to 39 printable English keyboard characters for this MA. The combined length of the MD Name and MA name must be less or equal to 44bytes.

Table 91 Maintenance > Diagnostic > 802.1ag (continued)

LABEL	DESCRIPTION
Maintenance Association (MA) Format	Select the format which the P-870HN-51D uses to send this MA information in the domain (MD). Options are **VID**, **String** and **Integer**. If you select **VID** or **Integer**, the P-870HN-51D adds the VLAN ID you specified for an MA in the CCM. If you select **String**, the P-870HN-51D adds the MA name you specified above in the CCM. Note: The MEPs in the same MA shoule use the same MA format.
Destination MAC Address	Enter the target device's MAC address to which the P-870HN-51D performs a CFM loopback test.
Count	Set how many times the P-870HN-51D send loopback messages (LBMs).
802.1Q VLAN ID	Type a VLAN ID (0-4095) for this MA.
Maintenance End Point ID	Enter an ID number (1-8191) for this MEP port. Each MEP port needs a unique ID number within an MD. The MEP ID is to identify an MEP port used when you perform a CFM action
Status	
Continuity Check Message (CCM)	This shows how many Connectivity Check Messages (CCMs) are sent and if there is any invalid CCM or cross-connect CCM.
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).
Save	Click this to save your changes back to the P-870HN-51D.
Enable CCM	Click this button to have the selected MEP send Connectivity Check Messages (CCMs) to other MEPs.
Disable CCM	Click this button to disallow the selected MEP to send Connectivity Check Messages (CCMs) to other MEPs.
Update CC status	Click this button to reload the test result.
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.

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- *Power, Hardware Connections, and LEDs*
- *P-870HN-51D Access and Login*
- *Internet Access*
- *Wireless LAN Troubleshooting*

24.1 Power, Hardware Connections, and LEDs

The P-870HN-51D does not turn on. None of the LEDs turn on.

1 Make sure the P-870HN-51D is turned on.

2 Make sure you are using the power adaptor or cord included with the P-870HN-51D.

3 Make sure the power adaptor or cord is connected to the P-870HN-51D and plugged in to an appropriate power source. Make sure the power source is turned on.

4 Turn the P-870HN-51D 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 23.

2 Check the hardware connections. See the Quick Start Guide.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the P-870HN-51D off and on.

5 If the problem continues, contact the vendor.

24.2 P-870HN-51D Access and Login

I forgot the IP address for the P-870HN-51D.

1 The default IP address is **https://192.168.1.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the P-870HN-51D by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the P-870HN-51D (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 25.

I forgot the password.

1 The default admin password is **1234** and the default user password is **user**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 25.

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 **https://192.168.1.1**.

- If you changed the IP address (Section on page 96), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the P-870HN-51D.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix C on page 299.

4 Reset the device to its factory defaults, and try to access the P-870HN-51D with the default IP address. See Section 1.6 on page 25.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- If your computer is connected to the WAN port or is connected wirelessly, use a computer that is connected to an **ETHERNET** port.
- Try to access the P-870HN-51D using another service, such as Telnet. If you can access the P-870HN-51D, check the remote management settings and firewall rules to find out why the P-870HN-51D does not respond to HTTPS.

I can see the **Login** screen, but I cannot log in to the P-870HN-51D.

1 Make sure you have entered the user name and password correctly. The default admin user name is **admin** and default admin password is **1234**. The default user name is **user** and the default user password is **user**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 Turn the P-870HN-51D off and on.

3 If this does not work, you have to reset the device to its factory defaults. See Section 24.1 on page 239.

I cannot Telnet to the P-870HN-51D.

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.

I cannot access the P-870HN-51D again after configuring a new interface group.

Make sure your computer is connected to a LAN port in the default group. Otherwise, you need to use the P-870HN-51D's LAN IP address for the new group to access the P-870HN-51D again.

24.3 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 23.

2 Make sure you entered your ISP account information correctly in the WAN screens. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

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

5 If the problem continues, contact your ISP.

I cannot access the Internet through a DSL connection.

1 Check if you set the **DSL/WAN** switch (on the back of the P-2812HNU-51c) to the **DSL** side to have the P-870HN-51D use the DSL port for Internet access.

2 Make sure you configured a proper ATM or PTM layer-2 interface and WAN services with the Internet account information provided by your ISP.

3 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 access the Internet through an Ethernet WAN connection.

1 Check if you set the **DSL/WAN** switch (on the back of the P-2812HNU-51c) to the **WAN** side to have the P-870HN-51D use the Ethernet WAN port for Internet access.

2 Make sure you connect the Ethernet WAN port to a DSL modem or router in your netwrok.

3 Make sure you configured a proper Ethernet layer-2 interface and WAN services with the Internet account information provided by your ISP.

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 create multiple connections of the same type.

Your layer-2 interface must be in VLAN MUX Mode or MSC mode to create multiple WAN serivces for each connection.

I cannot access the Internet anymore. I had access to the Internet (with the P-870HN-51D), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 23.

2 Turn the P-870HN-51D off and on.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 23. If the P-870HN-51D is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Check the signal strength. If the signal strength is low, try moving your computer closer to the P-870HN-51D if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 Turn the P-870HN-51D off and on.

4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

• Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

24.4 Wireless LAN Troubleshooting

I cannot access the P-870HN-51D or ping any computer from the WLAN (wireless AP or router).

1 Make sure the wireless LAN is enabled on the P-870HN-51D.

2 Make sure the wireless adapter on the wireless station is working properly.

3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the P-870HN-51D.

4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the P-870HN-51D.

5 Check that both the P-870HN-51D and your wireless station are using the same wireless and wireless security settings.

6 Check if MAC Filter is configured to deny wireless access to certain MAC addresses to the P-870HN-51D. See Chapter 7 Wireless LAN in the User's Guide for more information.

Product Specifications

The following tables summarize the P-870HN-51D's hardware and firmware features.

25.1 Hardware Specifications

Table 92   Hardware Specifications

Dimensions	21.5 cm (L) x 12.3 cm (W) x 3.6 cm (D)
Weight	417 g
Power Specification	12 V DC 1.5A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100/1000 Mbps RJ-45 Ethernet ports
RESET Button	10 seconds: Restores factory defaults
Antennas	One attached external dipole antenna, 2dBi One internal antenna , 2dBi
WPS Button	1 second: turn on or off WLAN 5 seconds: enable WPS (Wi-Fi Protected Setup)
Operation Temperature	0° C ~ 40° C
Storage Temperature	-30° ~ 60° C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH

25.2 Firmware Specifications

Table 93   Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)

Table 93 Firmware Specifications (continued)

Default User Name	admin
Default Password	1234
DHCP Server IP Pool	192.168.1.33 to 192.168.1.65
Static Routes	16
Device Management	Use the web configurator to easily configure the rich range of features on the P-870HN-51D.
Wireless Functionality (wireless devices only)	Allow the IEEE 802.11b, IEEE 802.11g and/or IEEE 802.11n wireless clients to connect to the P-870HN-51D wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator to put it on the P-870HN-51D. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the P-870HN-51D's configuration. You can put it back on the P-870HN-51D later if you decide to revert back to an earlier configuration.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the P-870HN-51D assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The P-870HN-51D supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
NAT	NAT (includes multi-to-multi NAT)/SUA NAT Server (port forwarding) VPN (IPSec, PPTP, and L2TP) Pass Through NAT friendly applications: NetMeeting Microsoft PPTP client MSN Messenger X-Box Live TFTP, FTP, H.323, RTSP, SIP ALG
Time and Date	Get the current time and date from an external server when you turn on your P-870HN-51D. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the P-870HN-51D to an external syslog server.

Table 93 Firmware Specifications (continued)

Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
QoS (Quality of Service)	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTPS or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the P-870HN-51D.
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Other PPPoE Features	PPPoE idle time out PPPoE dial on demand
Packet Filters	Your device's packet filtering function allows added network security and management.
VDSL Standards	Maximum data rate (downstream/upstream): 100 Mbps/100 Mbps VDSL line coding: ITU-T G.993.2 DMT modulation Tranceivers: ITU-T G.993.1 DSL handshake procedure protocol: ITU-T G.994.1 DSL physical layer management protocol: ITU-T G.997.1 VDSL band plan: 997 and 998 Support U0 band VDSL profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a and 30a VDSL speed: up to 100/100 Mbps@ 700 feet Support Annex A, Annex B Rate adaptation OLR: Bit Swapping/ SRA (Seamless Rate Adaption) Upstream power back-off (UPBO) VDSL OAM communication channels: Indicator bits (IB) channel, VDSL embedded operations channel (EOC) and VDSL overhead control channel (VOC) Erasure and Broadcom PhyR PHY Level Retransmission Technology PTM mode Trellis coding INP capability: At least two symbols protection (INP_MIN = 2), up to 16 symbols (INP_MIN = 16)

249

Table 93 Firmware Specifications (continued)

Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol
	Transparent bridging for unsupported network layer protocols
	RIP I/RIP II
	ICMP
	ATM QoS
	SNMP v1 and v2c with MIB II support (RFC 1213)
	IP Multicasting IGMP v1 and v2
	IGMP Proxy
Management	Embedded Web Configurator
	Remote Firmware Upgrade
	Telnet
	Embedded FTP/TFTP Server for firmware upgrade and configuration file backup and restore
	CLI (Command Line Interpreter)
	SSH (Secure Shell function)
	Syslog
	TR-069
	TR-064

The following list, which is not exhaustive, illustrates the standards supported in the P-870HN-51D.

Table 94 Standards Supported

STANDARD	DESCRIPTION
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	Internet Group Management Protocol, Version 1 IGMP v1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 2236	Internet Group Management Protocol, Version 2 IGMP v2
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11n	Uses the 2.4 gigahertz (GHz) band

Table 94   Standards Supported (continued)

STANDARD	DESCRIPTION
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
ITU-T G.993.2 (VDSL2)	ITU standard that defines VDSL2.
TR-069	DSL Forum Standard for CPE Wan Management.
TR-064	DSL Forum LAN-Side DSL CPE Configuration

Network Troubleshooting

Overview

The three most basic utilities for troubleshooting network connection issues are: `ipconfig`, `ping` and `tracert`. This appendix gives a quick overview of them as well as some common usage examples. Moreover, three slightly more advanced utilities are also discussed: `arp`, `route`, and `netstat`.

Note: All command examples here use the Microsoft Windows operating system version of the commands.

Before Getting Started

Before using the commands described in this section, ensure that you have the TCP/IP networking component installed and properly configured for your network adapter.

Click **Start > Control Panel > Network Connections** and then open a **Local Area Connection** to display the following screen.

Figure 140 TCP/IP Networking Component
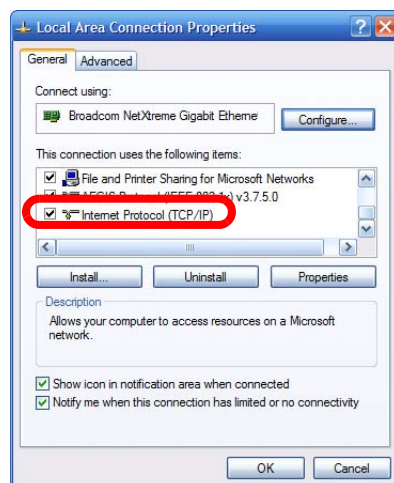
Note: Most operating systems ship with TCP/IP already installed and enabled. See your Windows documentation for details on installing or configuring TCP/IP.

The Command Line Interface

To open the Windows command line interface:

1 Click **Start > Run**.

2 In the **Run** dialog box, enter **cmd** then click **OK**.
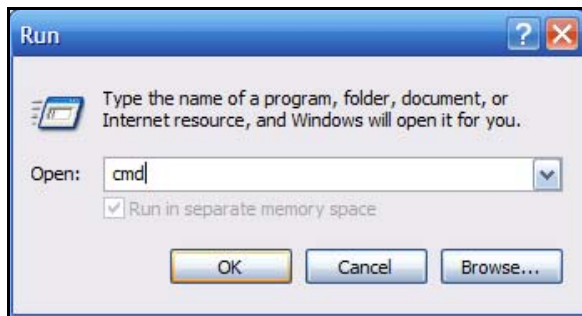
3 The **Command Prompt** window opens.
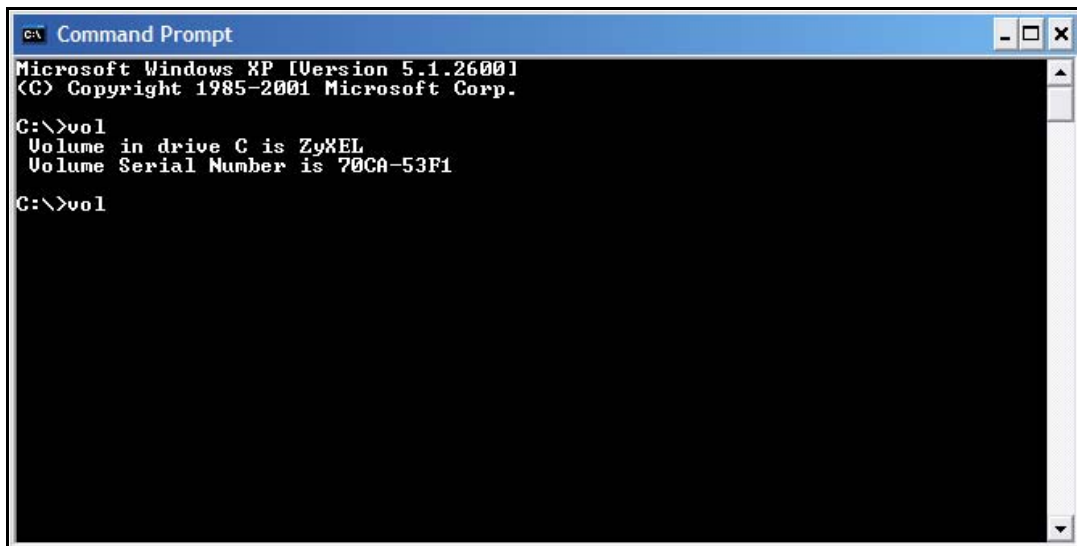
Command Syntax and Parameters

Command descriptions always indicate the default syntax you must use when entering them on the command line. Some commands require additional parameters in order to execute properly. Some may have optional parameters.

Parameters are displayed as follows: `command [parameter]`

For example, the `date` command has the optional `/t` and `date` parameters. If you do not use either of them and enter just `date` by itself, then the system shows you the date it is currently using and then prompts you to change it.

```
C:\>date
The current date is: 2009/10/21
Enter the new date: (mm-dd-yy)
```

However, if you use the `/t` parameter it just displays the date and nothing more.

```
C:\>date /t
2009/10/21

C:\>
```

To view the parameters for any given command, enter `help [command]`.

ipconfig

The `ipconfig` command line utility allows you to display current network (TCP/IP) configuration settings and, in some cases, adjust them. When you have network connectivity problems, the first thing you should do is run this command to ensure that your device or computer does in fact have an IP address as well as display the source of that IP address (such as a default gateway).

Syntax: `ipconfig`

Parameters: `ipconfig [/release] [/renew]`

There are other parameters, but these are the only ones you need to use for now.

The following examples show the typical output of this command:

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : example.com
        IP Address. . . . . . . . . . . : 192.168.1.1
        Subnet Mask . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 1.1.1.4

C:\>
```

Here you can see that the device has IP address of 1.1.1.1 and example.com is its Domain Name Server (DNS).

If the device is disconnected then you would see the following instead:

```
Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected
```

If the device is connected but cannot get an IP address then you would see:

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . :
```

In some cases, your computer may be properly connected to the network or the P-870HN-51D but it is not receiving an IP address for whatever reason. Use the `/release` parameter followed by `/renew`:

```
C:\>ipconfig /release

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . :

C:\>ipconfig /renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : zyxel.com
        IP Address. . . . . . . . . . . : 192.168.1.2
        Subnet Mask . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 2.2.2.4

C:\>
```

ping

The `ping` command line utility allows you to verify the connection and latency between your computer and either the P-870HN-51D or other devices on the network. If you cannot reach a target using this command, then it may indicate possible network trouble.

Syntax: `ping target`

The `target` can be an IP address or a host name.

Parameters: `ping [-w timeout] target`

The `timeout` parameter allows you to input the number of seconds (in milliseconds) that your computer waits for a reply.

The following examples show the typical output of this command:

```
C:\>ping www.zyxel.com

Pinging a1524.g.akamai.net [203.69.113.18] with 32 bytes of data:

Reply from 203.69.113.18: bytes=32 time=6ms TTL=56
Reply from 203.69.113.18: bytes=32 time=6ms TTL=56
Reply from 203.69.113.18: bytes=32 time=6ms TTL=56
Reply from 203.69.113.18: bytes=32 time=7ms TTL=48

Ping statistics for 203.69.113.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 7ms, Average = 6ms

>
```

The number of bytes here indicates packet size. As most data is broken up into smaller packets, this makes the ping test fairly representative of a typical network connection. The default packet size on Windows is 32 bytes.

Time is the number of milliseconds the data requires to make the roundtrip journey from your computer to the destination host and back again. The lower the number, the faster the connection between the two points.

Note: Some hosts are deliberately configured to not respond to ping requests. As such, we suggest pinging two or three hosts when performing your ping test.

If your ping test fails to get a response, then you may see a message like this:

```
C:\>ping www.example.com

Pinging www.example.com [192.0.32.10] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.0.32.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

When a request times out it may mean:

- your computer is not connected to the network

- your Internet access device is not connected to the network

- or the device which you are pinging is not connected to the network

If you think the destination is active but responding slowly, you can try increasing the ping timeout value from its default of 4 seconds (4000 milliseconds) to something like 8 seconds (or 8000 milliseconds).

```
C:\>ping -w 8000 www.example.com

Pinging www.example.com [192.0.32.10] with 32 bytes of data:

Reply from 192.0.32.10: bytes=32 time=157ms TTL=238
Reply from 192.0.32.10: bytes=32 time=154ms TTL=238
Reply from 192.0.32.10: bytes=32 time=152ms TTL=236
Reply from 192.0.32.10: bytes=32 time=162ms TTL=236

Ping statistics for 192.0.32.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 152ms, Maximum = 162ms, Average = 156ms

C:\>
```

A long `ping` response could indicate network problems:

- on your side of the connection

- between the start and end points of the connection

- on the receiving end

To determine where the slowdown is, you may need to use `traceroute`.

tracert

The `tracert` command line utility allows you to determine the network path between your computer and a host you specify. When you communicate with other devices on a network, the data is not often sent directly from point A to point B; rather, it moves through a series of intermediate servers, passed along until eventually the server closest to point B hands it off directly. This command can be useful for helping determine whether your connection issues are happening locally, somewhere in transit, or at the destination end.

- Each step in the chain of connections is called a 'hop'.
- The time it takes for a server at any given hop to pass the data packet is called 'latency' and is measured in milliseconds.

When a `tracert` command is run, it sends out a burst of three data packets per hop. The results table, therefore, always displays three values for latency in addition to the IP address and domain name (where available) of the server on that leg of the journey.

Syntax: `tracert` *target*

The `target` can be an IP address or a host name.

Parameters: `tracert` `[-d]` `[-h` *maximumhops* `]` *target*

There are other parameters but these are the only ones you need to use for now.

The following examples show the typical output of this command:

```
C:\>tracert www.example.com

Tracing route to www.example.com [192.0.32.10]
over a maximum of 30 hops:

  1     <1 ms     <1 ms     <1 ms  172.23.x.x
  2      5 ms      4 ms      5 ms  172.23.x.x
  3      4 ms      4 ms      4 ms  172.23.x.x
  4      5 ms      4 ms      6 ms  219-87-158-97.static.tfn.tw [219.87.158.97]
  5      6 ms      5 ms      4 ms  10.42.232.150
  6      5 ms      4 ms      4 ms  hc-c12r2.router.tw [220.128.7.86]
  7     10 ms      7 ms     10 ms  tp-s2-c12r12.router.tw [220.128.2.90]
  8      9 ms      7 ms      8 ms  pr03-s2.tp.tw [220.128.4.181]
  9      6 ms      6 ms      9 ms  220-128-3-249.NET-IP.tw [220.128.3.249]
 10    138 ms    137 ms    138 ms  r11-pa.NET-IP.net [211.72.108.129]
 11    138 ms    138 ms    138 ms  po4-0.core01.sjc04.atlas.com [154.54.11.129]
 12    128 ms    139 ms    140 ms  te9-2.mpd01.sjc04.atlas.com [154.54.0.173]
 13    140 ms    139 ms    136 ms  61.58.33.173
 14    154 ms    153 ms    137 ms  xe-0-0-0.r20.gin.ntt.net [129.250.16.161]
 15    154 ms    154 ms    137 ms  as-2.r21.tokyjp01.jp.ntt.net [129.250.4.81]
 16    562 ms    553 ms    553 ms  38.106.6.34
 17    554 ms    554 ms    553 ms  po-2.r00.lsanca19.us.ntt.net [129.250.6.42]
 18    254 ms    254 ms    248 ms  204.1.254.150
 19    154 ms    253 ms    154 ms  192.0.32.10

Trace complete.

C:\>
```

Here, the `tracert` to www.example.com took 18 hops to reach its destination. Looking at the latency data, you'll see the first slow down happens at hop 10.

The extremely low latency on the first few hops indicates a network local to the computer where the `tracert` command originated, such as a home or office LAN. The packets then move onto the local WAN (such as your Internet Service Provider's network). Because of the close proximity of those servers to your computer, the latency remains low.

Once the data packets move out of the regional network to the first international server (at hop 10 in this example), the latency increases. This is because of the distance between the regional and international servers - it physically takes longer for the response to get back to your computer.

Finally, on transition hop 15 from the server in Japan to the server in California, another latency spike occurs. If you were having connection problems, this would most likely be the source of it. For whatever reason, the server in Japan has a less than optimal connection with its counterpart in the United States.

In this example, we abridge the `tracert` results table to show only server IP addresses and not domain names by using the `-d` parameter. We also use the `-h` parameter to limit the number of hops to 5 to test local connections only.

```
C:\>tracert -d -h 5 www.zyxel.com

Tracing route to a1524.g.akamai.net [203.69.113.16]
over a maximum of 5 hops:

  1     <1 ms     <1 ms     <1 ms  172.23.31.254
  2      5 ms      4 ms      4 ms  172.23.6.113
  3      5 ms      5 ms      6 ms  172.23.6.253
  4     17 ms     16 ms     14 ms  218.160.188.254
  5     24 ms     25 ms     24 ms  10.42.232.150

Trace complete.

C:\>
```

arp

Local network transmission is based on MAC addresses. Data transmission between two networks is based on IP addresses.

Address Resolution Protocol (ARP) is a protocol that converts IP addresses into MAC addresses. Before a computer transmits data to an IP address on the same network, it will check whether the IP address exists in its ARP table. If it does, the computer then sends the data directly to the mapped MAC address. If it does not, the computer broadcasts an ARP request to the network. The host whose MAC address maps to the IP address responds.

When you use `ping` to check the connection to a computer, no response does not mean the computer is not alive on the network. The destination computer may be configured not to respond to any ping requests. However, you can use the `arp -a` command line utility to check the IP addresses and MAC addresses of your neighboring computers or devices.

Syntax: `arp -a`

Parameters: `arp [-d` *inet_addr*`] [-s` *inet_addr eth_addr*`]`

The `-d` parameter can be use alone to remove all entries from an arp table or in conjunction with an IP address to remove just that IP address (*inet_addr*). The `-s` parameter allows you to add entries based on IP address (*inet_addr*) and/or MAC address (*eth_addr*).

There are other parameters but these are the only ones you need to use for now.

261

To check the ARP table on a Windows XP computer:

1 Click **Start** > **Programs** > **Accessories** > **Command Prompt**. The **Command Prompt** screen appears.

2 Type `arp -a` and press `[Enter]`.

The following examples show the typical output of this command:

```
C:\>arp -a
Interface: 172.16.1.28 on Interface 0x1000003
  Internet Address      Physical Address      Type
  172.16.1.5            00-00-aa-19-07-38     dynamic
  172.16.1.25           00-18-f3-f0-aa-34     dynamic
  172.16.1.44           00-0e-a6-2c-60-10     dynamic
  172.16.1.210          00-19-cb-e9-66-33     dynamic
  172.16.1.254          00-04-80-4c-a8-05     dynamic
```

In this example, the **Physical Address** indicates the associated MAC address. A **Type** entry with **dynamic** means it was dynamically learned through an ARP response. Use the `arp -s [inet_addr eth_addr]` to manually add an ARP entry if you want your computer to connect to the host with the specified MAC address when you access the specified IP address.

You can additionally check whether the MAC address associated with the IP address that you are looking for is correct. In some circumstances, your ARP table may keep a wrong MAC address until the entry expires. You can then manually update the ARP table.

To update the ARP table:

1 Type `arp -d [inet_addr]` or just use `arp -d` to remove all entries in the ARP table. For example, type `arp -d 172.16.1.5`.

2 Type `ping 172.16.1.5` and press `[Enter]`.

3 Next, use the `arp -a` command again to check whether the MAC address matches what you expected. If it does not, another computer may be using a duplicate IP address on the network. Change the IP address on either computer to an unused one to fix this problem.

route

The `route` command line utility allows you to display or adjust your computer's network table. The routing table on your computer contains the default gateway

and other route information. When your computer wants to access an IP address on another network, it references this table.

Syntax: `route print`

Parameters: For the purposes of this section, the *print* parameter is the most important. If you enter `route` by itself, the command's help page displays.

The following example shows the typical output of this command:

```
C:\>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 02 e3 a1 b2 c3 ...... Broadcom NetXtreme Gigabit Ethernet
Driver

===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     172.16.1.254     172.16.1.32       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
       172.16.1.0    255.255.255.0     172.16.1.32     172.16.1.32       1
      172.16.1.32  255.255.255.255        127.0.0.1       127.0.0.1       1
   172.16.255.255  255.255.255.255     172.16.1.32     172.16.1.32       1
        224.0.0.0        224.0.0.0     172.16.1.32     172.16.1.32       1
  255.255.255.255  255.255.255.255     172.16.1.32     172.16.1.32       1
Default Gateway:      172.16.1.254
===========================================================================
Persistent Routes:
  None
```

The following table describes labels shown in the command output:

Table 95   route print Command Output

OUTPUT	DESCRIPTION
Active Routes	This section lists all available routes that are automatically learned from the network.
Network Destination	The destination IP address of packets that this route entry is to route. The destination can be an IP address for a network or host, 0.0.0.0 for the default route or 127.0.0.0 for the loopback interface which is used mainly for self-test.
	The destination 224.0.0.0 is for multicasting packets or reserved for testing. But if you are not using multicast applications, just ignore it.
	The destination 255.255.255.255 is used to find computers when an IP address is not known. For example, before the DHCP IP address of your computer is determined, your computer sends packets with the destination looking for DHCP servers on the network.

Table 95 route print Command Output

OUTPUT	DESCRIPTION
Netmask	The destination subnet mask of packets that this route entry is to route. The subnet mask can be the apropriate subnet mask for a network, 255.255.255.255 for a host, or 0.0.0.0 for the default route.
Gateway	The IP address of the gateway through which this computer should send the matched packets.
Interface	The IP address of an physical interface on this computer used to send the matched packets for this route entry.
Metric	The metric (hop count) of this route. Normally, the lower the number, the faster to a destination.
Default Gateway	The IP address of the gateway through which this computer sends all the rest packets if this computer cannot find any other matched routes for the packets.
Persistent Routes	This section lists all routes that are manually configured.

In this example, the 172.16.1.0 is the network address. The 172.16.1.32 is the address of the local computer. 172.16.1.255 is the network broadcast address which sends broadcast packets to all computers on the 172.16.1.x network. 172.16.1.254 is the default gateway.

You may have more than one 0.0.0.0 entry if your computer has two or more network cards installed. This may casue packets to be routed somewhere unexpected. Delete all 0.0.0.0 entries except the one that you want to use for the default gateway. In the following example, the computer uses the first 0.0.0.0 entry for the default gateway.

```
Network Destination        Netmask          Gateway       Interface  Metric
        0.0.0.0          0.0.0.0     192.168.1.254    192.168.1.33        1
        0.0.0.0          0.0.0.0      172.16.1.254     172.16.1.32        1
```

• To delete the route to the default route with the gateway of 192.168.1.254, type: `route delete 0.0.0.0 mask 0.0.0.0 192.168.1.254`.

• To add a route to the destination 172.16.2.0 with the subnet mask of 255.255.255.0, the next hop address of 172.16.1.250, and the cost metric of 7, type: `route add 172.16.2.0 mask 255.255.255.0 172.16.1.250 metric 7`.

• To add a persistent route to the destination 172.16.3.0 with the subnet mask of 255.255.255.0 and the next hop address of 172.16.1.252, type: `route -p add 172.16.3.0 mask 255.255.255.0 172.16.1.252`.

Note that the metric will be set to 1 if you do not specify any.

netstat

The netstat command line utility is used to show Ethernet statistics and current TCP/IP network connections.

Syntax: netstat

With no parameters, this command simply displays only active statistics for ports that are currently in use by one process or another.

Parameter: netstat [-a] [-e]

The -a parameter displays all available listening ports and connections whether they are active or not, while the -e parameter displays Ethernet statistics.

There are other parameters but these are the only ones you need to use for now.

The following examples show the typical output of this command:

```
C:\>netstat

Active Connections

  Proto   Local Address            Foreign Address          State
  TCP     COMPUTERA:1056           localhost:5091           ESTABLISHED
  TCP     COMPUTERA:1091           localhost:27015          ESTABLISHED
  TCP     COMPUTERA:1120           localhost:40000          ESTABLISHED
  TCP     COMPUTERA:3243           localhost:3244           ESTABLISHED
  TCP     COMPUTERA:3244           localhost:3243           ESTABLISHED
  TCP     COMPUTERA:3246           localhost:3247           ESTABLISHED
  TCP     COMPUTERA:3247           localhost:3246           ESTABLISHED
  TCP     COMPUTERA:5091           localhost:1056           ESTABLISHED
  TCP     COMPUTERA:5152           localhost:3245           CLOSE_WAIT
  TCP     COMPUTERA:27015          localhost:1091           ESTABLISHED
  TCP     COMPUTERA:40000          localhost:1120           ESTABLISHED
  TCP     COMPUTERA:3229           172.20.0.201:http        CLOSE_WAIT
  TCP     COMPUTERA:3234           172.16.1.29:1155         ESTABLISHED
  TCP     COMPUTERA:3237           172.16.1.29:1155         ESTABLISHED
  TCP     COMPUTERA:3240           172.16.1.29:1155         ESTABLISHED

C:\>
```

Use the -a parameter to display all possible connections to your device, not just the ones that are currently in use:

```
C:\>netstat -a
Active Connections

  Proto  Local Address          Foreign Address          State
  TCP    COMPUTERA:http         COMPUTERA:0              LISTENING
  TCP    COMPUTERA:http         172.16.x.x:4036          ESTABLISHED
  TCP    COMPUTERA:2744         NAS:microsoft-ds         ESTABLISHED
  TCP    COMPUTERA:5152         172.16.x.x.ZyXEL.com:0   LISTENING
  TCP    COMPUTERA:5152         localhost:4067           CLOSE_WAIT
  TCP    COMPUTERA:5354         172.16.x.x.ZyXEL.com:0   LISTENING
  TCP    COMPUTERA:27015        172.16.x.x.ZyXEL.com:0   LISTENING
  TCP    COMPUTERA:40000        localhost:0              LISTENING
  TCP    COMPUTERA:40000        localhost:1120           ESTABLISHED
  TCP    COMPUTERA:netbios-ssn  172.16.x.x.ZyXEL.com:0   LISTENING
  TCP    COMPUTERA:4177         172.16.x.x:1155          ESTABLISHED
  TCP    COMPUTERA:4178         172.16.x.x:1155          ESTABLISHED
  TCP    COMPUTERA:4180         172.16.x.x:1155          ESTABLISHED
  TCP    COMPUTERA:4182         172.16.x.x:1025          ESTABLISHED
  TCP    COMPUTERA:4317         NAS:microsoft-ds         ESTABLISHED
  TCP    COMPUTERA:4539         NAS:microsoft-ds         TIME_WAIT
  TCP    COMPUTERA:netbios-ssn  172.16.x.x:0             LISTENING
  TCP    COMPUTERA:netbios-ssn  172.16.x.x:0             LISTENING

C:\>
```

The following table describes the three entries in the output example above:

Table 96   netstat -a Command Output

OUTPUT	DESCRIPTION
TCP COMPUTERA:http COMPUTERA:0 LISTENING	A web server is available on **COMPUTERA** as an HTTP service is in a **LISTENING** state.
TCP COMPUTERA:http 172.16.1.29:4036 ESTABLISHED	A computer with an IP address of 172.16.1.29 is accessing the web service on the **COMPUTERA**.
TCP COMPUTERA:2744 NAS:microsoft-ds ESTABLISHED	**COMPUTERA** has established a TCP/IP NETBIOS connection (**microsoft-ds**) with a NAS device.

Additionally, you can use `netstat -e` to display Ethernet statistics as the following example.

```
C:\ >netstat -e
Interface Statistics

                        Received            Sent

Bytes                  25250033         7060325
Unicast packets           38838           34744
Non-unicast packets       38227             175
Discards                      0               0
Errors                        0              35
Unknown protocols           787
```

B

Setting Up Your Computer's IP Address

Note: Your specific P-870HN-51D may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

- *Windows XP/NT/2000* on *page 269*
- *Windows Vista* on *page 273*
- *Windows 7* on *page 277*
- *Mac OS X: 10.3 and 10.4* on *page 281*
- *Mac OS X: 10.5 and 10.6* on *page 285*
- *Linux: Ubuntu 8 (GNOME)* on *page 288*
- *Linux: openSUSE 10.3 (KDE)* on *page 293*

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

Figure 141 Windows XP: Start Menu
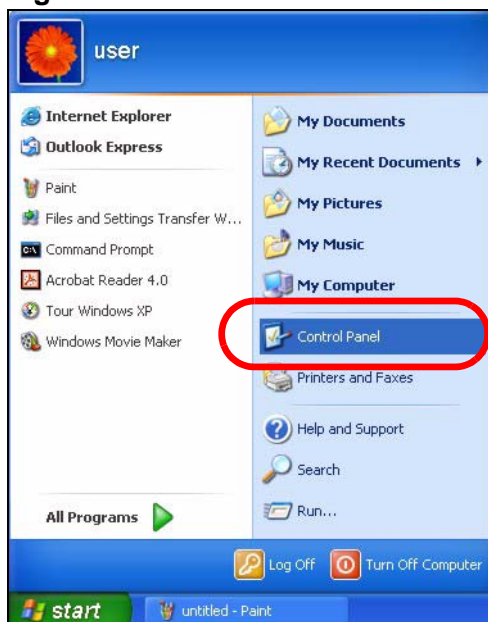
2 In the **Control Panel**, click the **Network Connections** icon.

Figure 142 Windows XP: Control Panel

3 Right-click **Local Area Connection** and then select **Properties**.

Figure 143 Windows XP: Control Panel > Network Connections > Properties
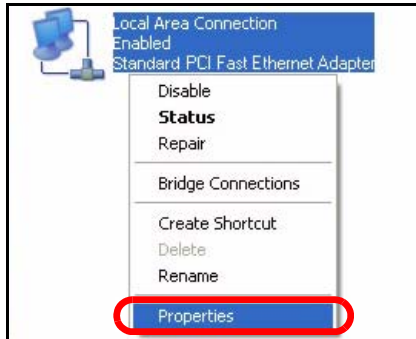
4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 144 Windows XP: Local Area Connection Properties
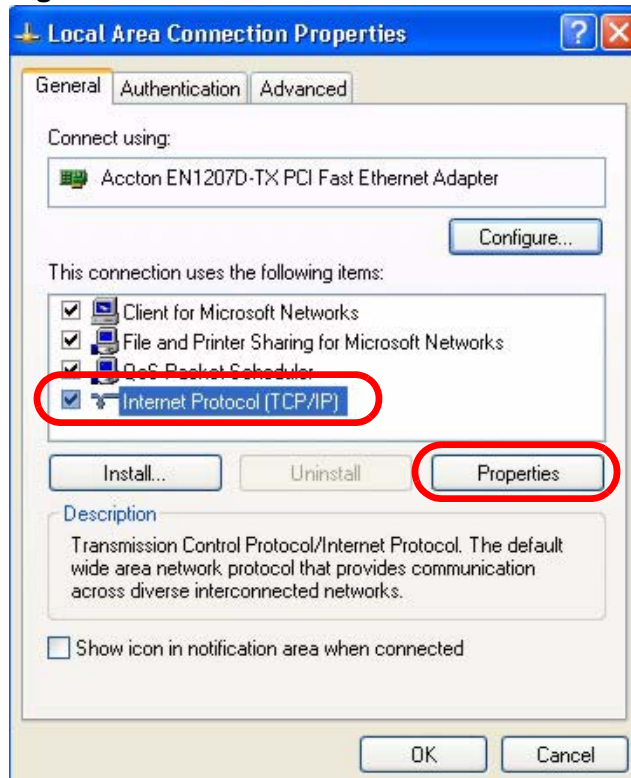
5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 145 Windows XP: Internet Protocol (TCP/IP) Properties
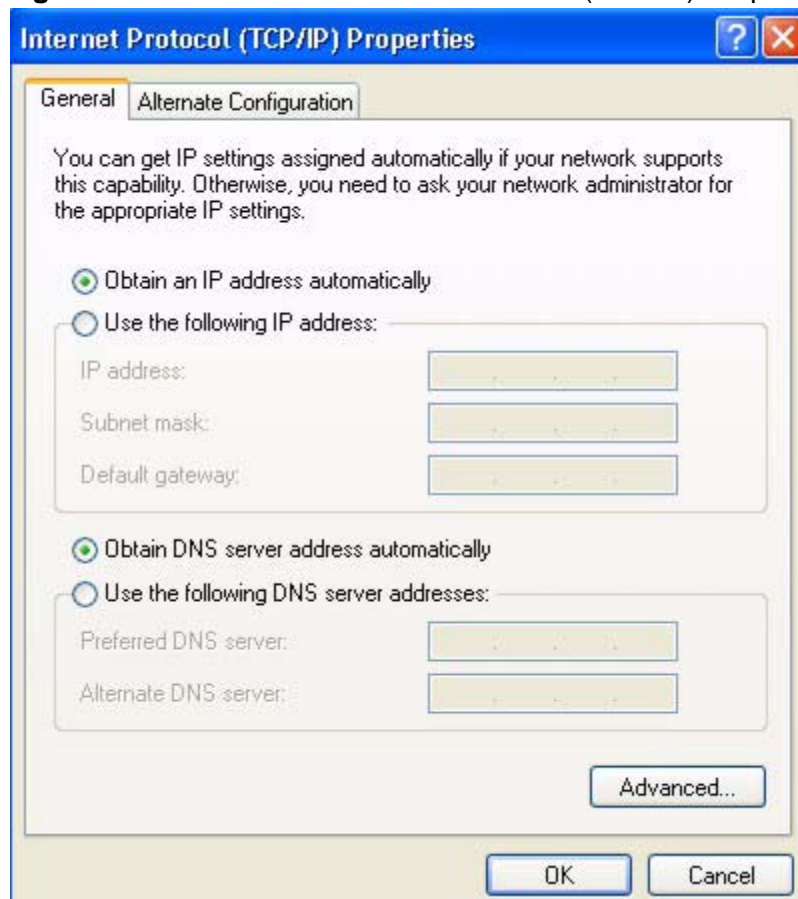
6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

1 Click **Start** > **Control Panel**.

Figure 146 Windows Vista: Start Menu
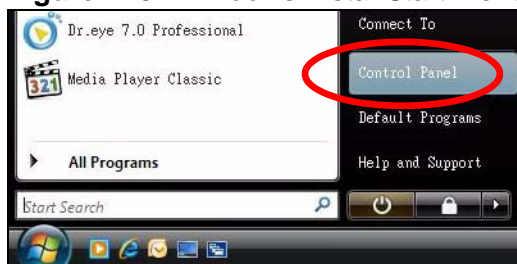
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 147 Windows Vista: Control Panel
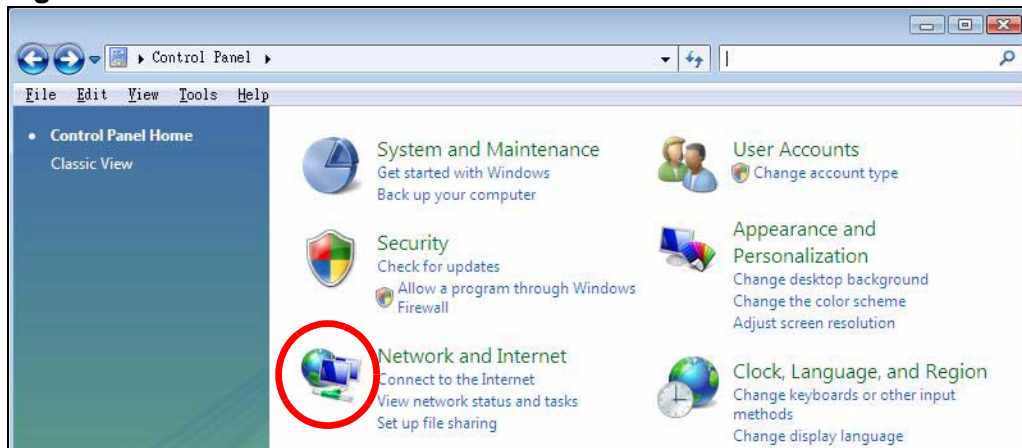
3 Click the **Network and Sharing Center** icon.

Figure 148 Windows Vista: Network And Internet

4 Click **Manage network connections**.

Figure 149 Windows Vista: Network and Sharing Center
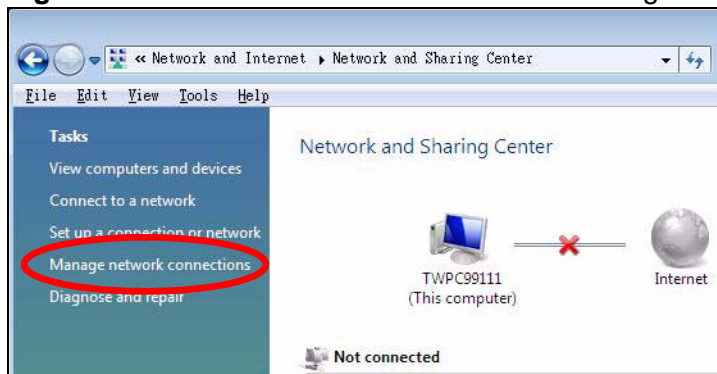
5 Right-click **Local Area Connection** and then select **Properties**.

Figure 150 Windows Vista: Network and Sharing Center
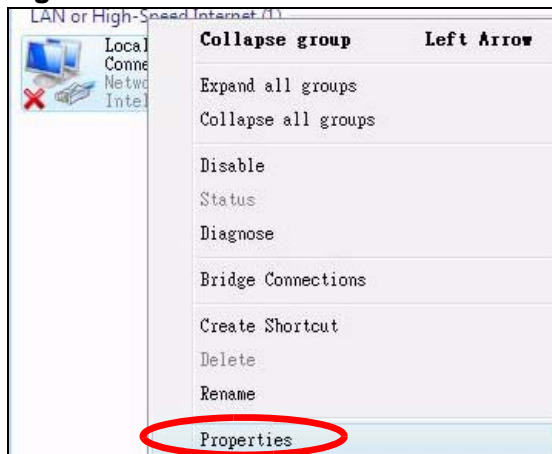
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 151 Windows Vista: Local Area Connection Properties
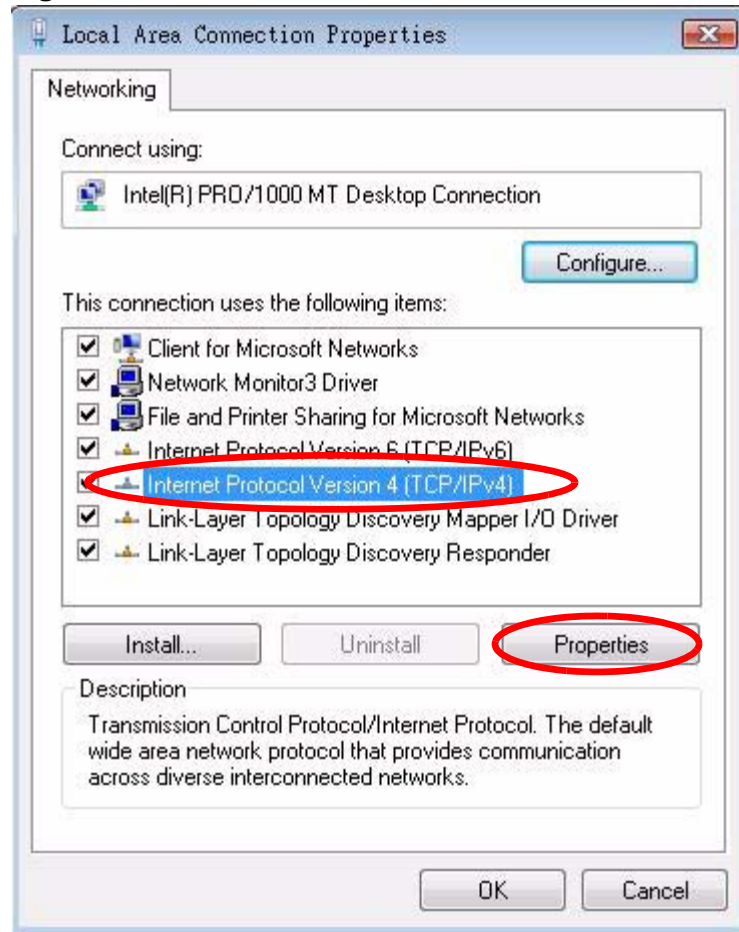
7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 152 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties
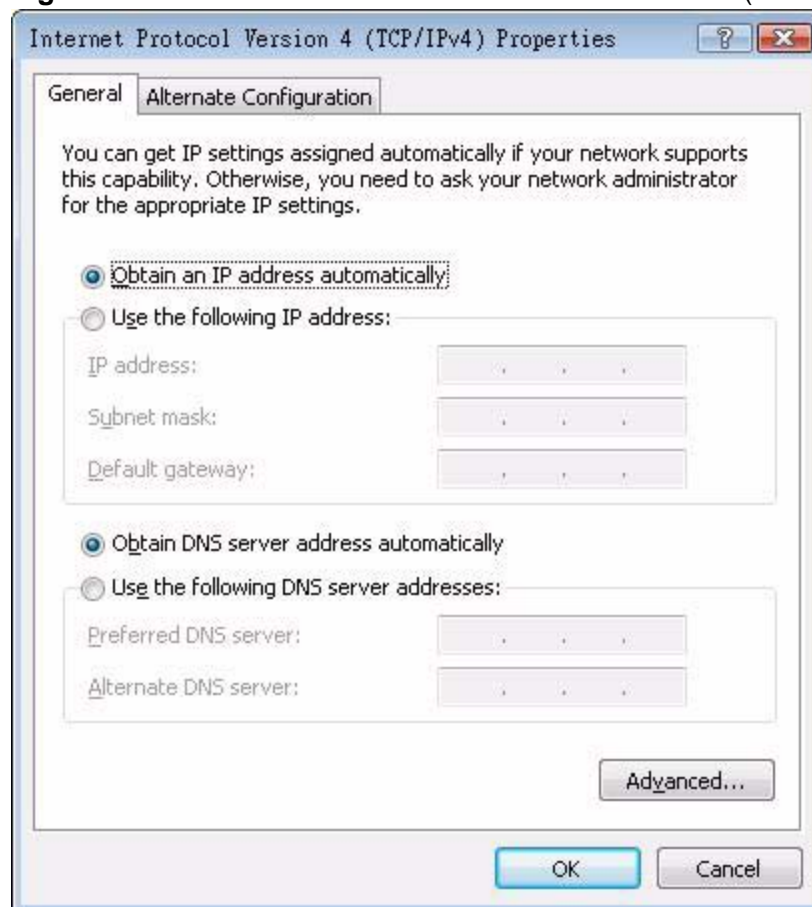
8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2   In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows 7

This section shows screens from Windows 7 Enterprise.

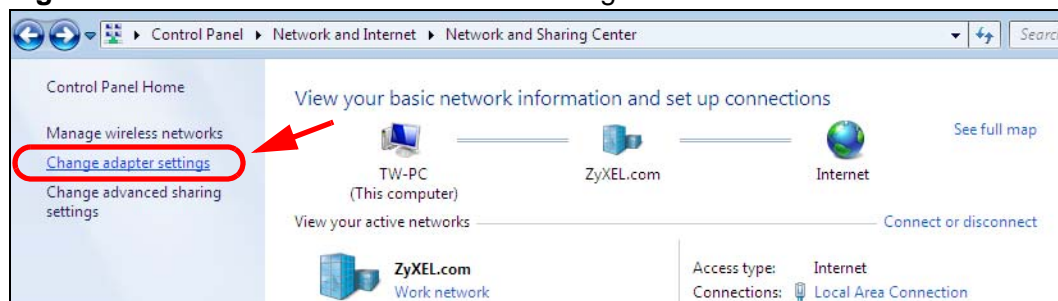1   Click **Start** > **Control Panel**.

Figure 153 Windows 7: Start Menu
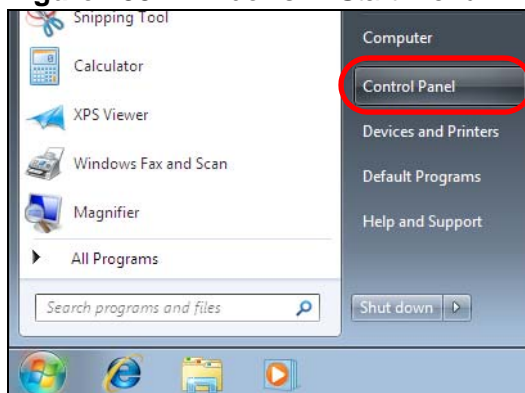
2   In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

Figure 154 Windows 7: Control Panel
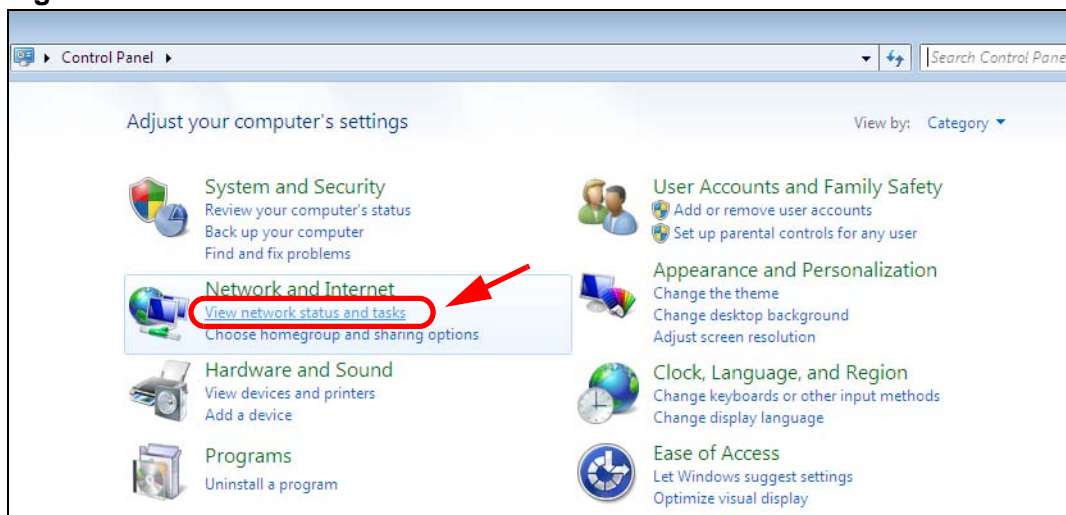
3 Click **Change adapter settings**.

Figure 155 Windows 7: Network And Sharing Center

4 Double click **Local Area Connection** and then select **Properties**.

Figure 156 Windows 7: Local Area Connection Status
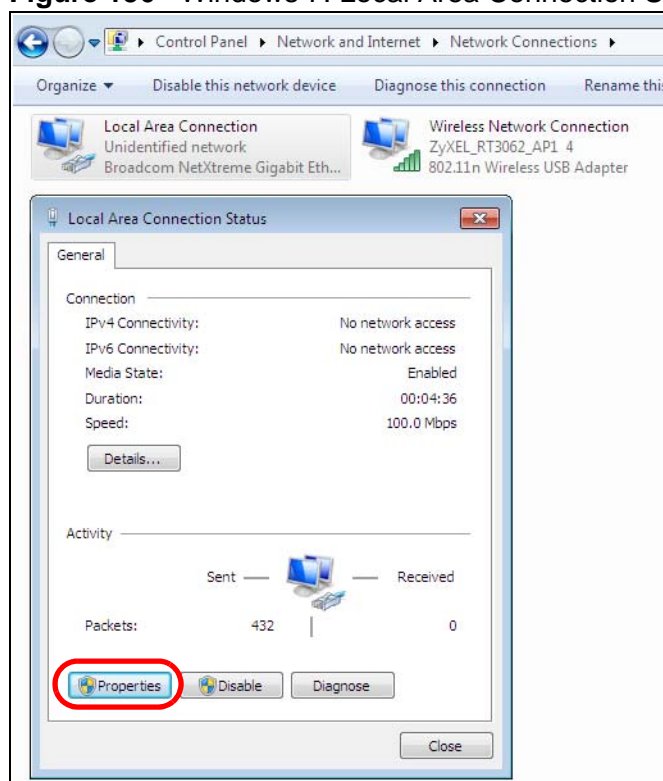
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.
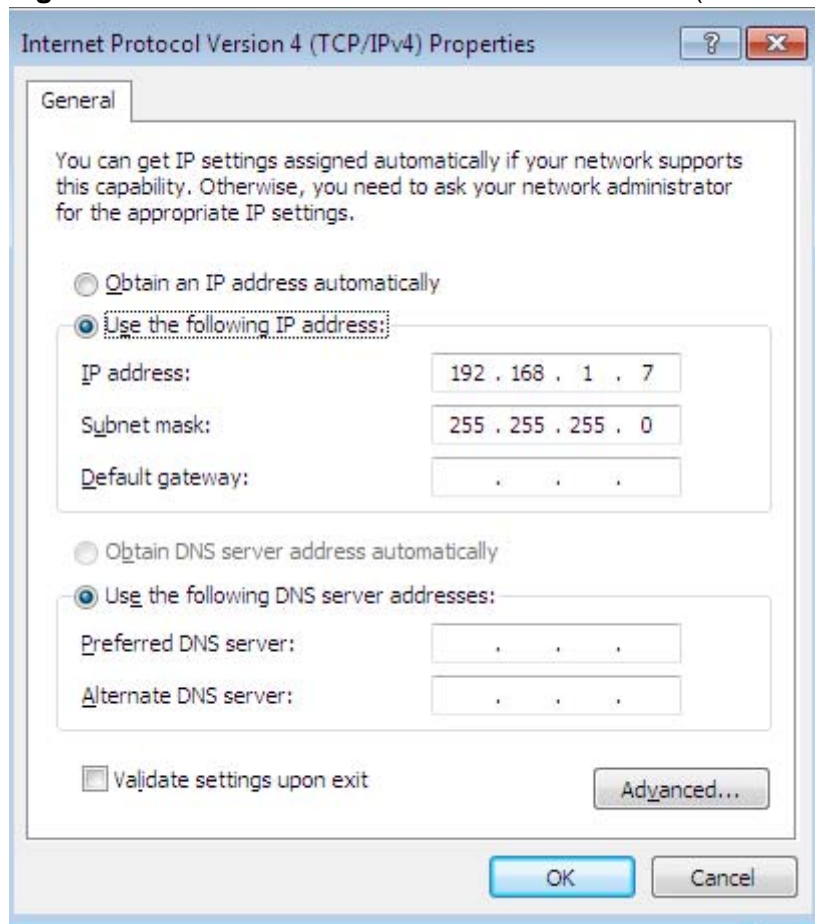
5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 157 Windows 7: Local Area Connection Properties
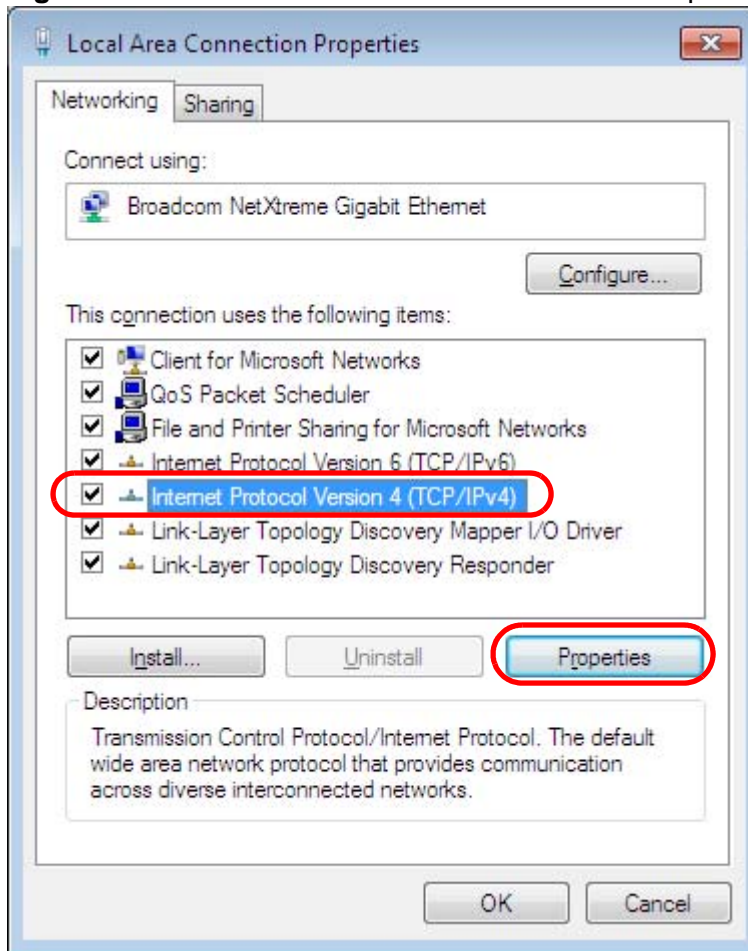
6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 158 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties

7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

3 The IP settings are displayed as follows.

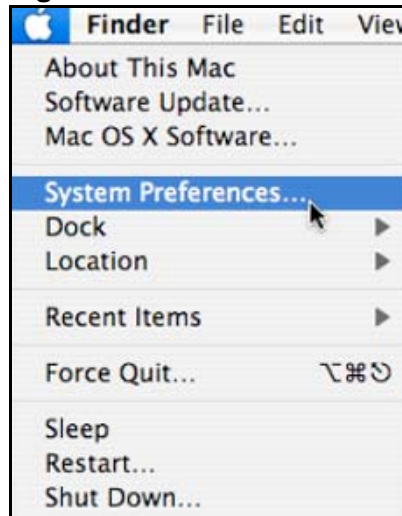**Figure 159** Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties

```
C:\WINNT\system32\cmd.exe                          _ □ ×

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.7
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\>_
```
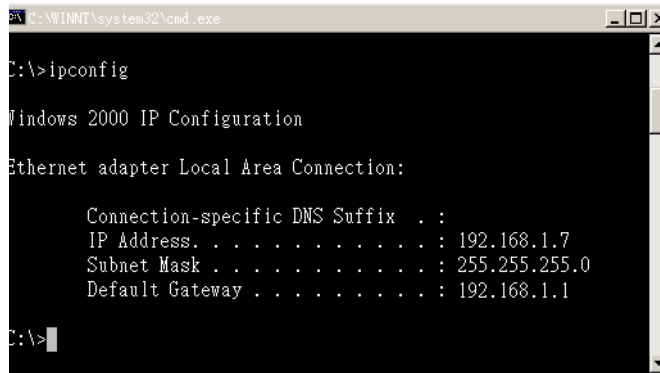
Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

Figure 160 Mac OS X 10.4: Apple Menu

```
🍎  Finder  File  Edit  View

  About This Mac
  Software Update...
  Mac OS X Software...

  System Preferences...
  Dock                        ▶
  Location                    ▶

  Recent Items                ▶

  Force Quit...           ⌥⌘⏏

  Sleep
  Restart...
  Shut Down...
```

2 In the **System Preferences** window, click the **Network** icon.

Figure 161 Mac OS X 10.4: System Preferences

3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

Figure 162 Mac OS X 10.4: Network Preferences
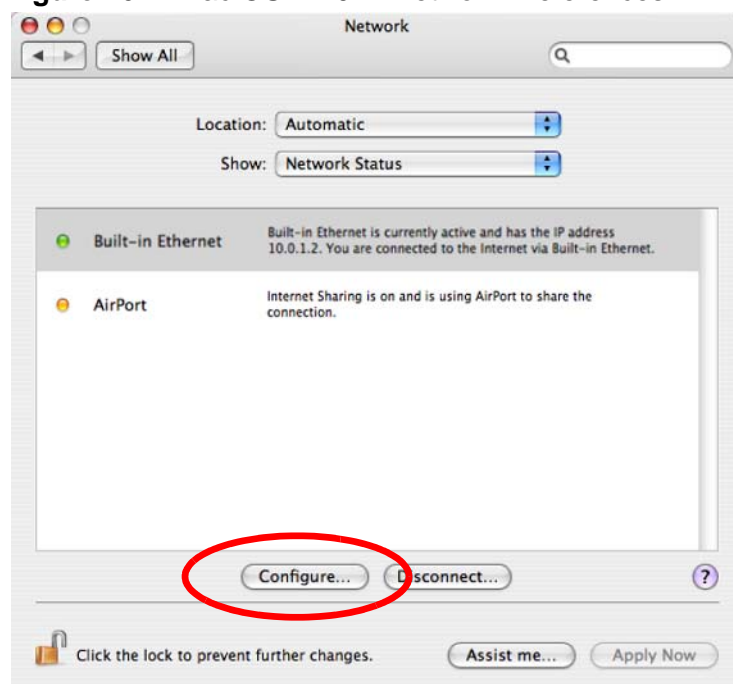
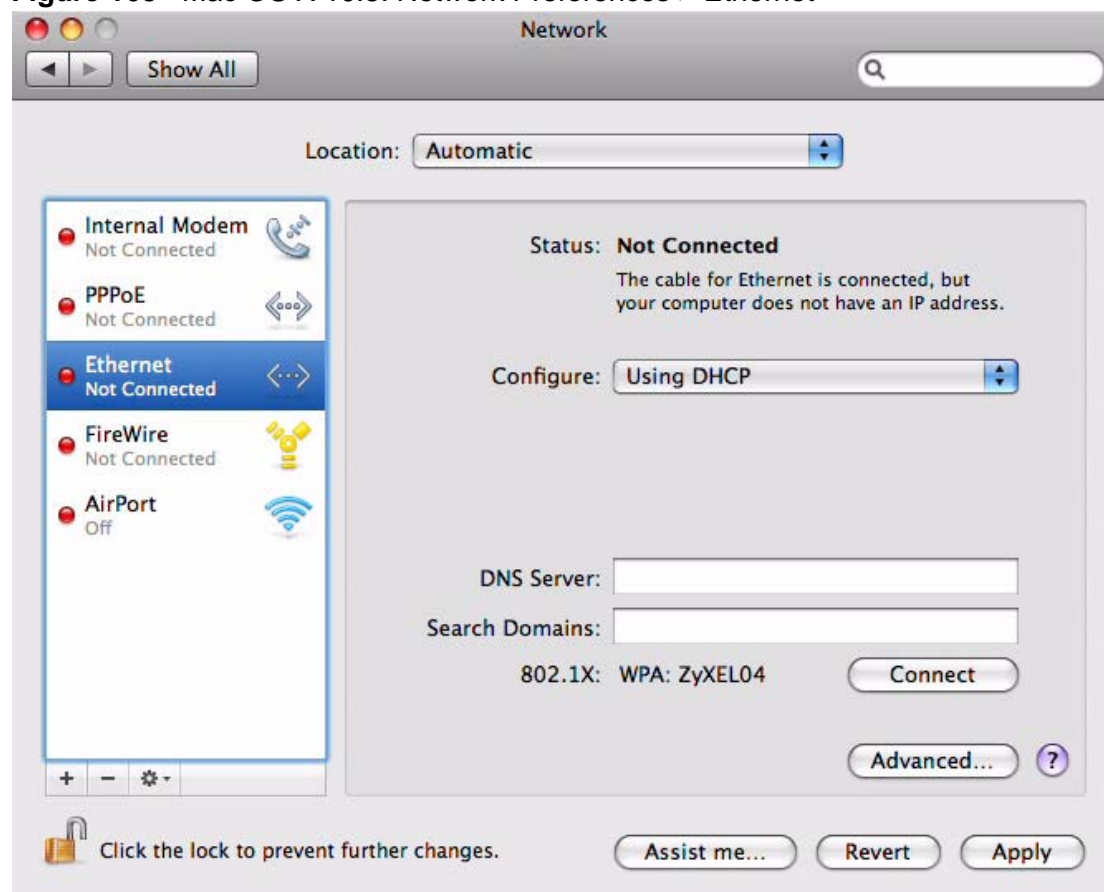**4** For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 163 Mac OS X 10.4: Network Preferences > TCP/IP Tab.
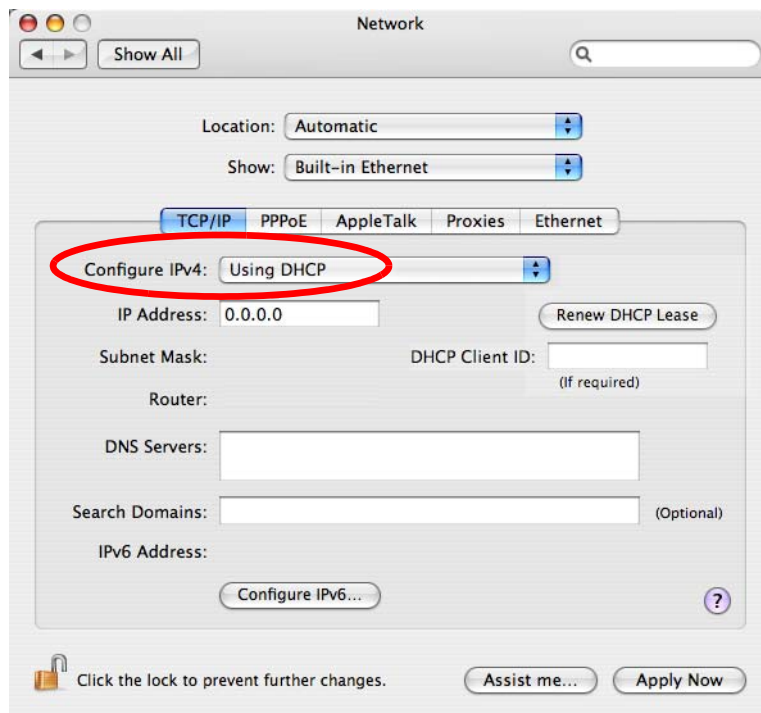
5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.

• In the **Router** field, type the IP address of your device.

Figure 164 Mac OS X 10.4: Network Preferences > Ethernet
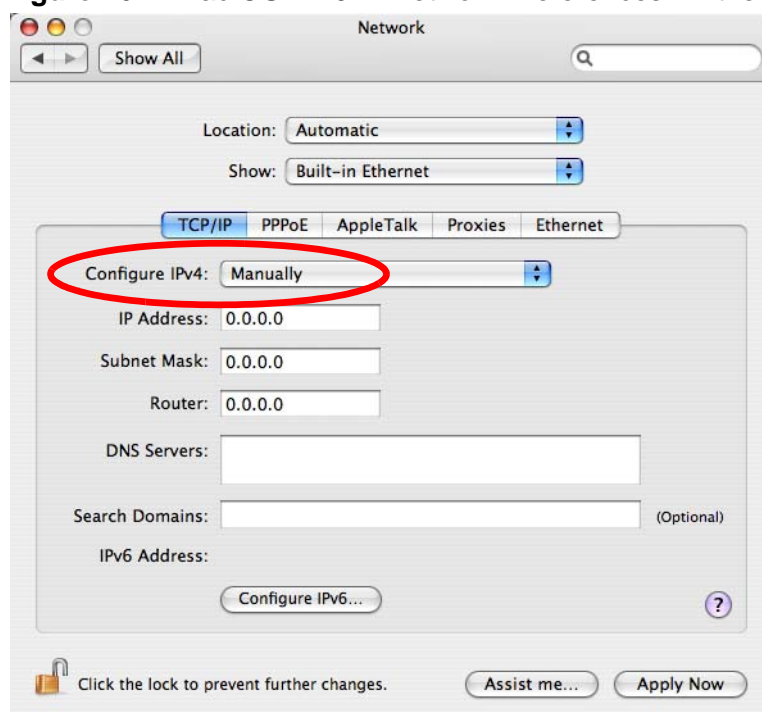
6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 165 Mac OS X 10.4: Network Utility
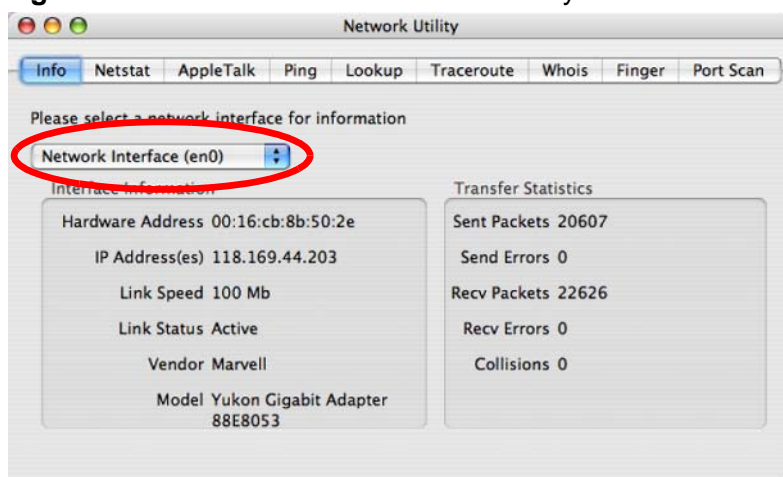
Mac OS X: 10.5 and 10.6

The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

1 Click **Apple** > **System Preferences**.

Figure 166 Mac OS X 10.5: Apple Menu
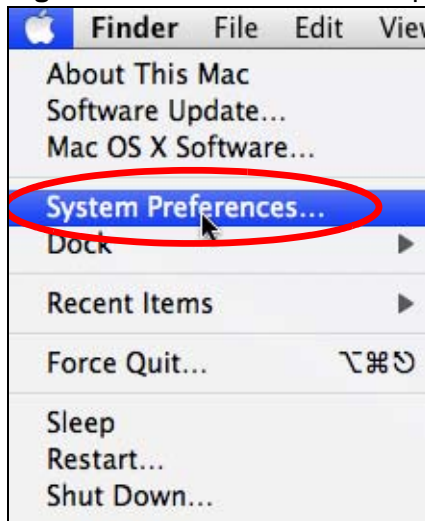
2 In **System Preferences**, click the **Network** icon.

Figure 167 Mac OS X 10.5: Systems Preferences

285

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

Figure 168 Mac OS X 10.5: Network Preferences > Ethernet

4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.

- In the **Router** field, enter the IP address of your P-870HN-51D.

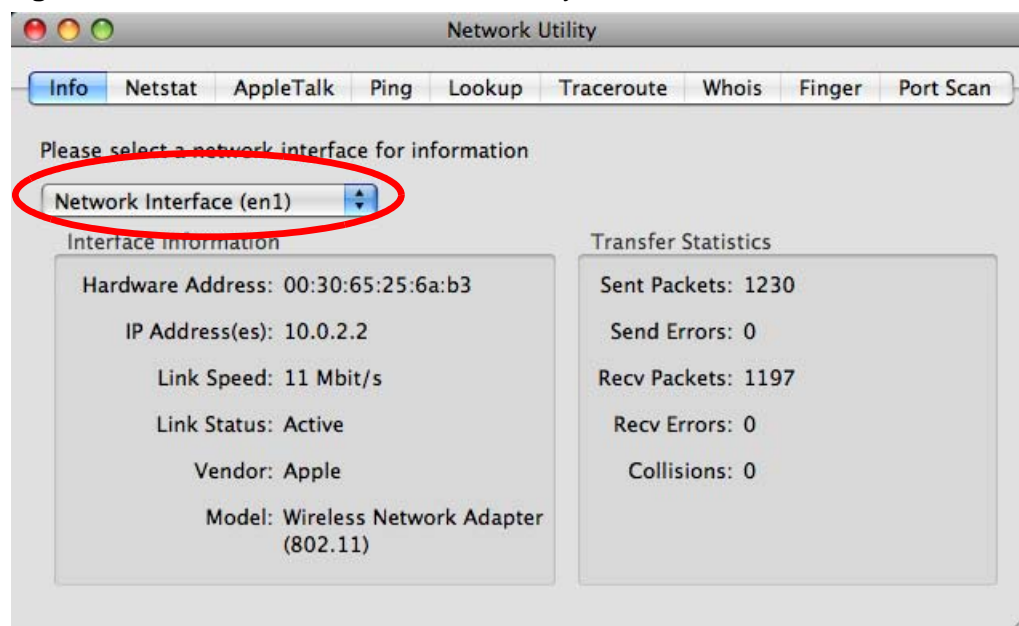**Figure 169**   Mac OS X 10.5: Network Preferences > Ethernet
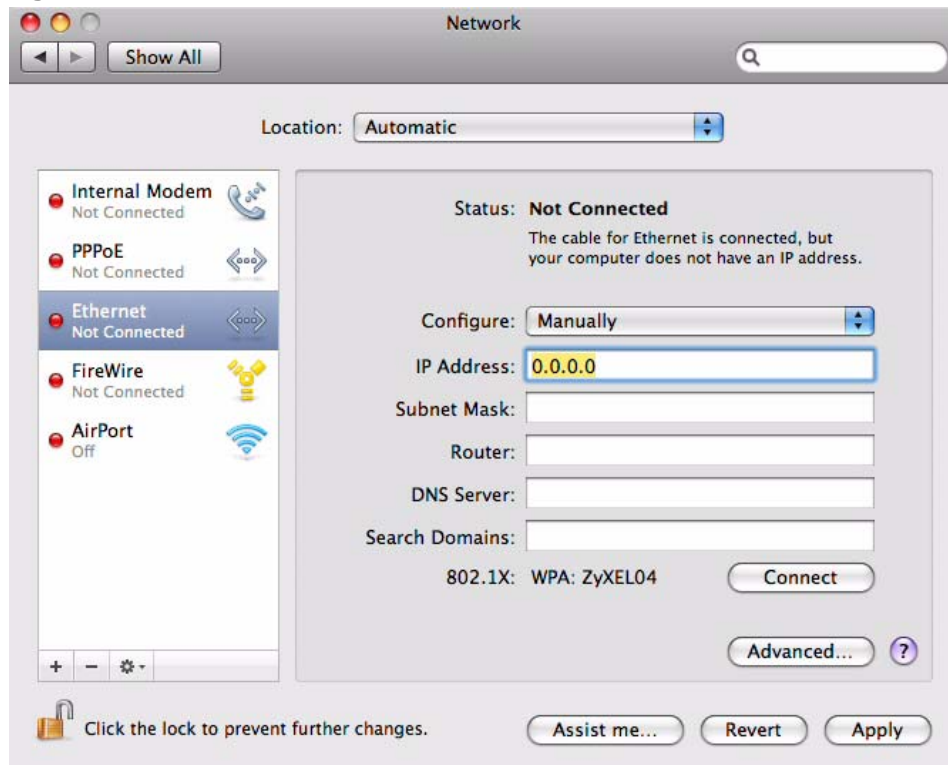
6   Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

**Figure 170**   Mac OS X 10.5: Network Utility

Linux: Ubuntu 8 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

1 Click **System** > **Administration** > **Network**.

Figure 171   Ubuntu 8: System > Administration Menu
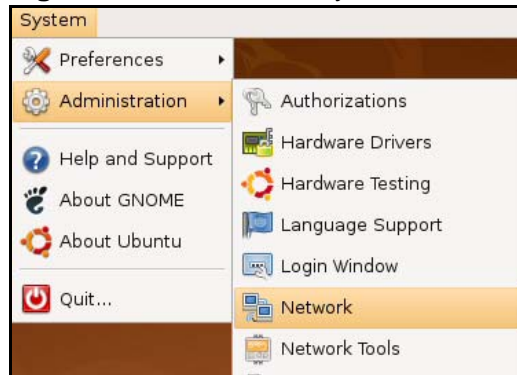
2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 172   Ubuntu 8: Network Settings > Connections
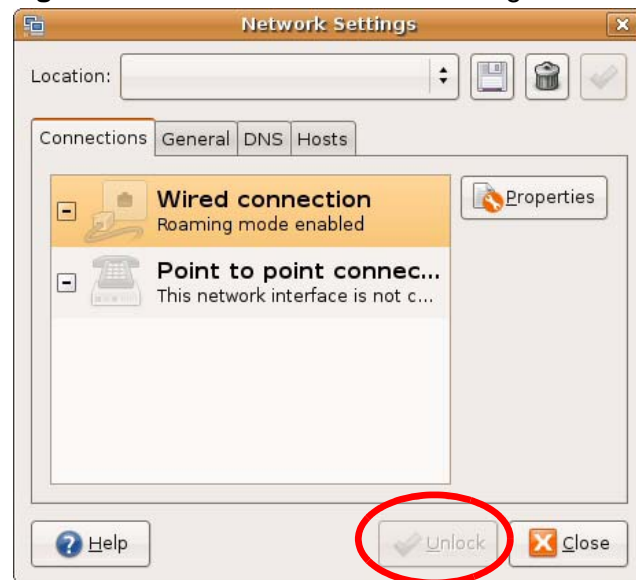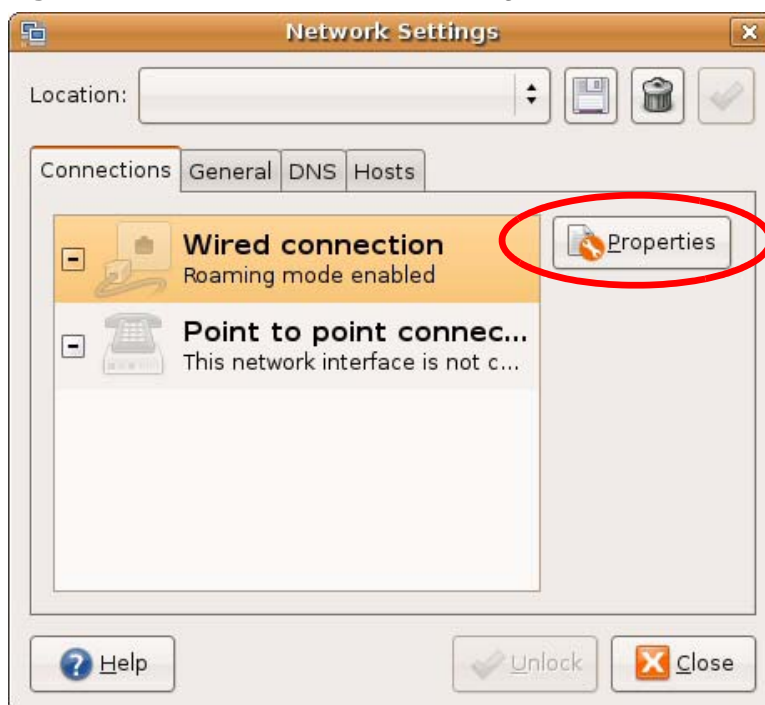
3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 173 Ubuntu 8: Administrator Account Authentication

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 174 Ubuntu 8: Network Settings > Connections

5 The **Properties** dialog box opens.

Figure 175 Ubuntu 8: Network Settings > Properties

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 176 Ubuntu 8: Network Settings > DNS
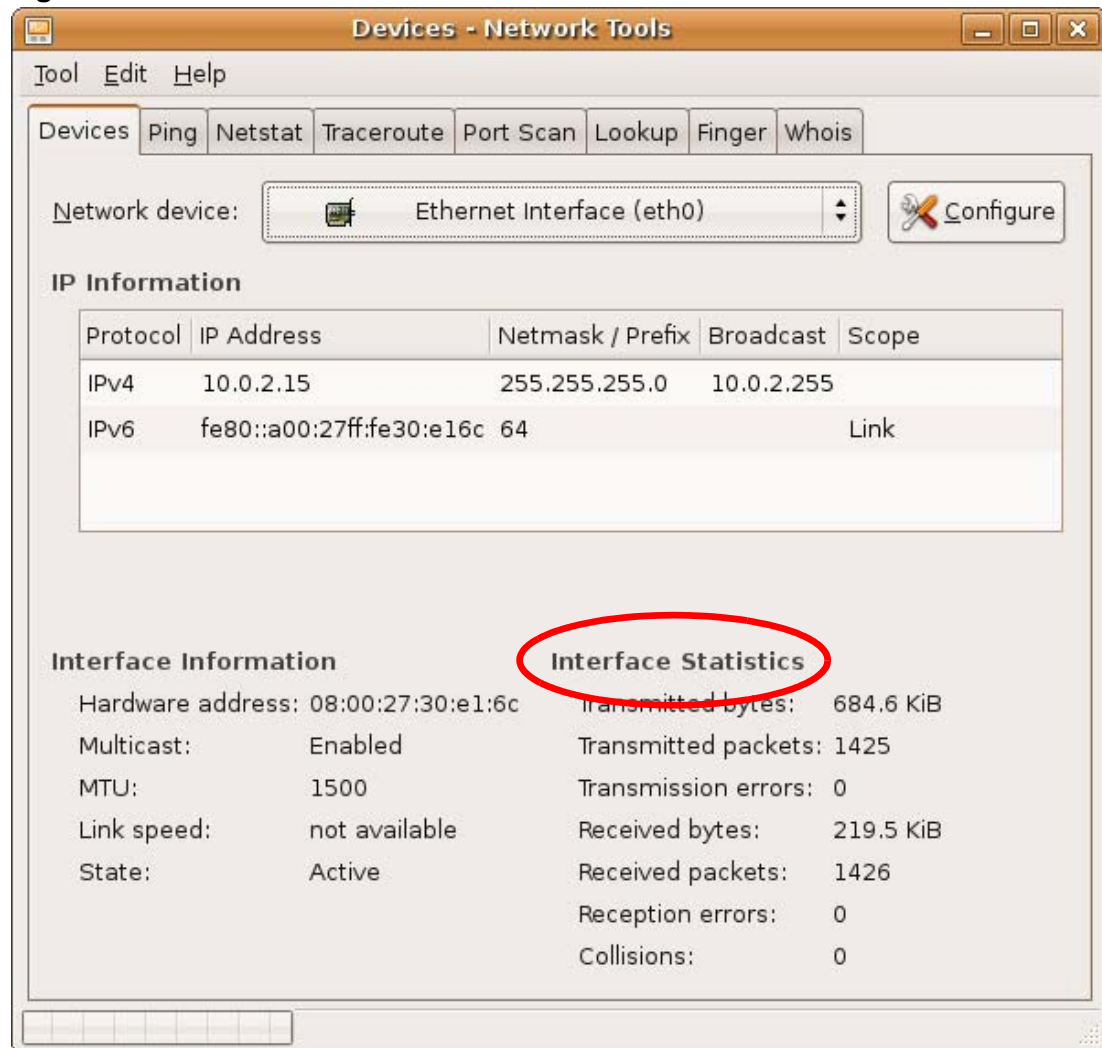

8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices**

tab. The **Interface Statistics** column shows data if your connection is working properly.

**Figure 177** Ubuntu 8: Network Tools

Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu** > **Computer** > **Administrator Settings (YaST)**.

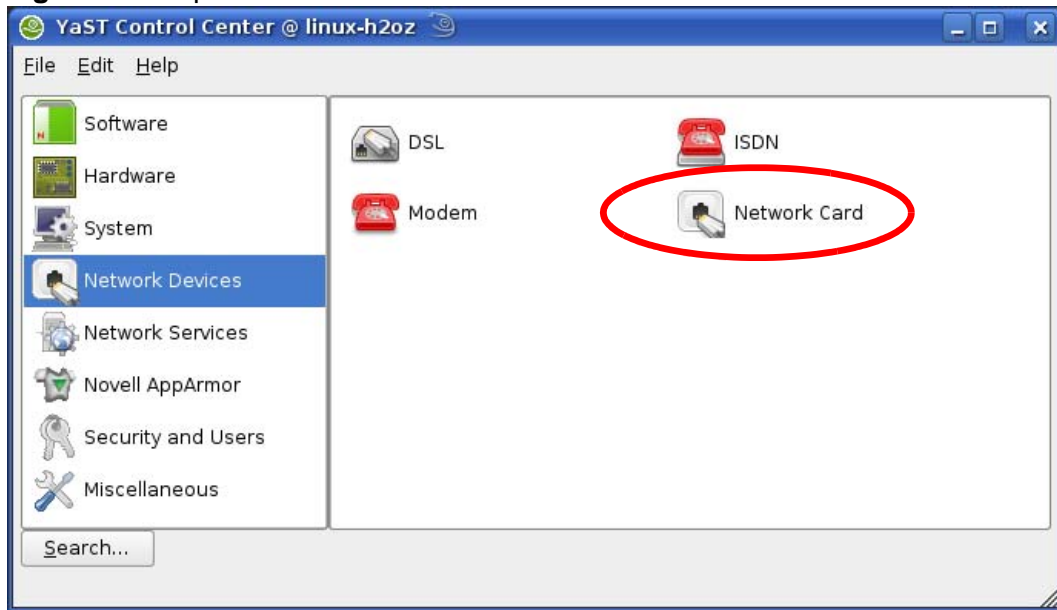**Figure 178**   openSUSE 10.3: K Menu > Computer Menu
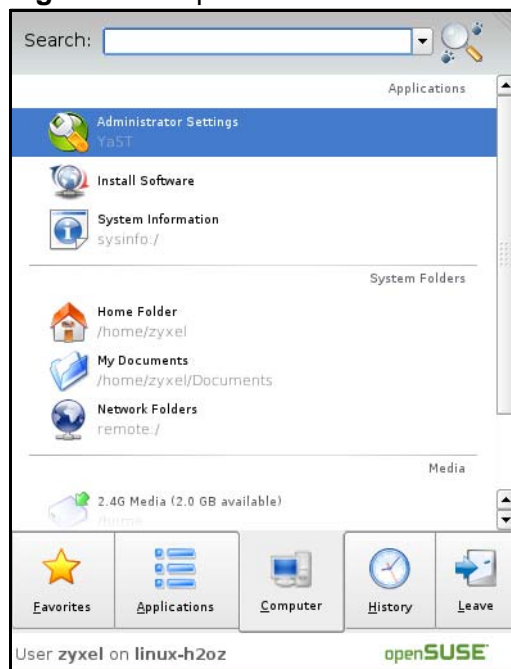
2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 179   openSUSE 10.3: K Menu > Computer Menu
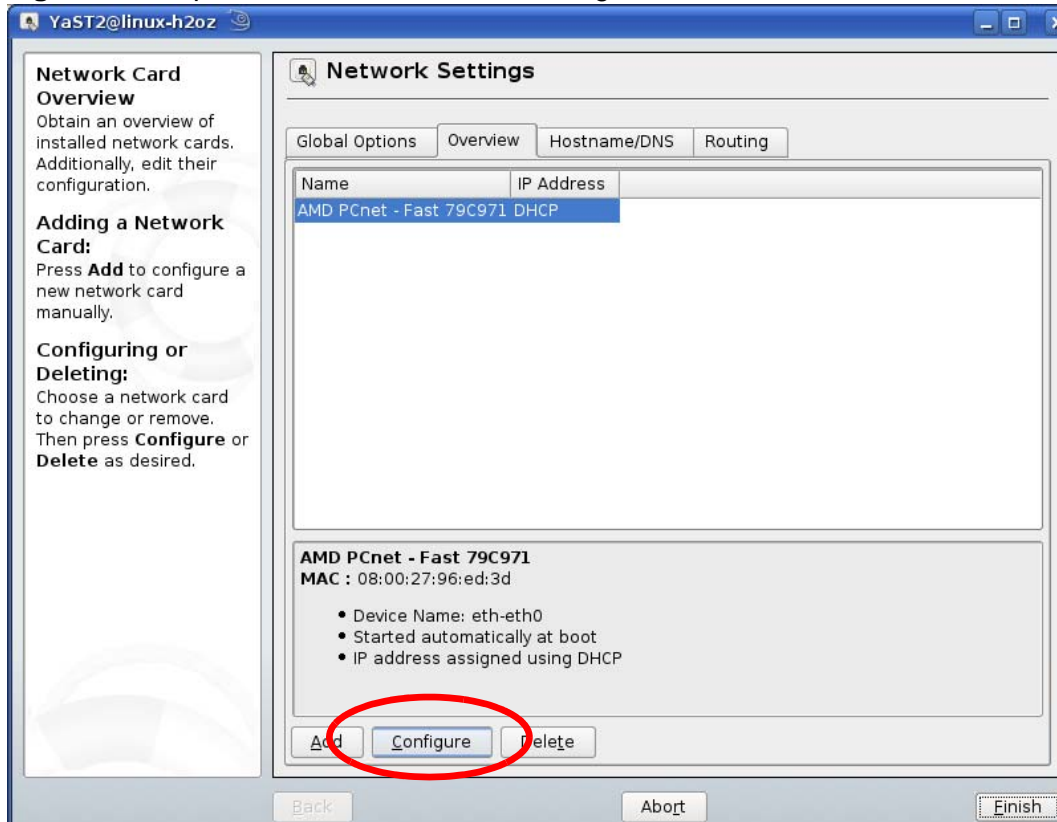
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.
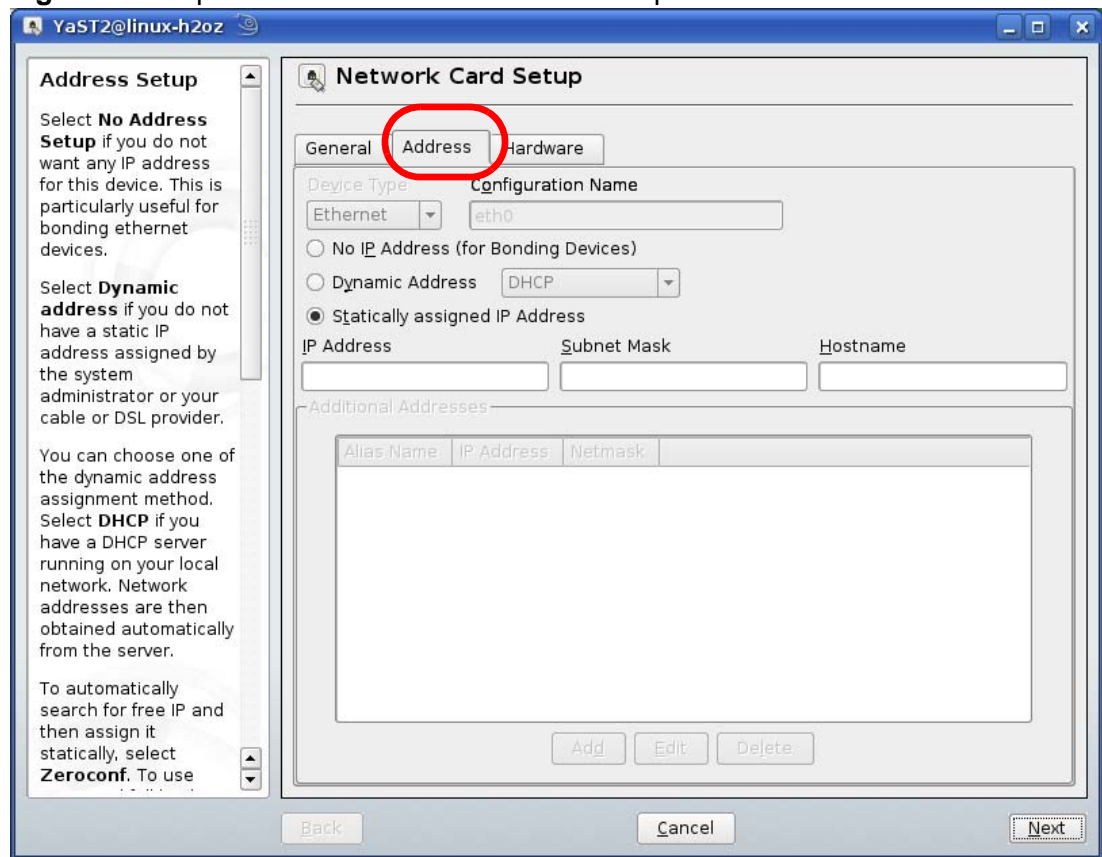
Figure 180 openSUSE 10.3: YaST Control Center

4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 181 openSUSE 10.3: Network Settings

5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 182   openSUSE 10.3: Network Card Setup

6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.
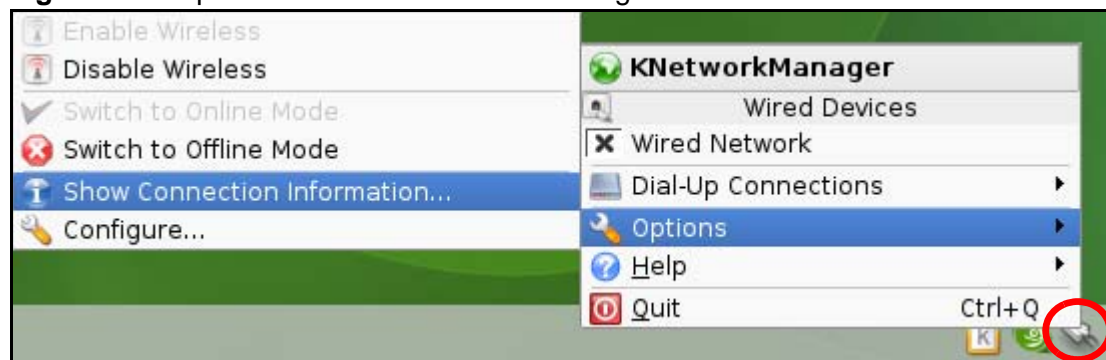
Figure 183 openSUSE 10.3: Network Settings
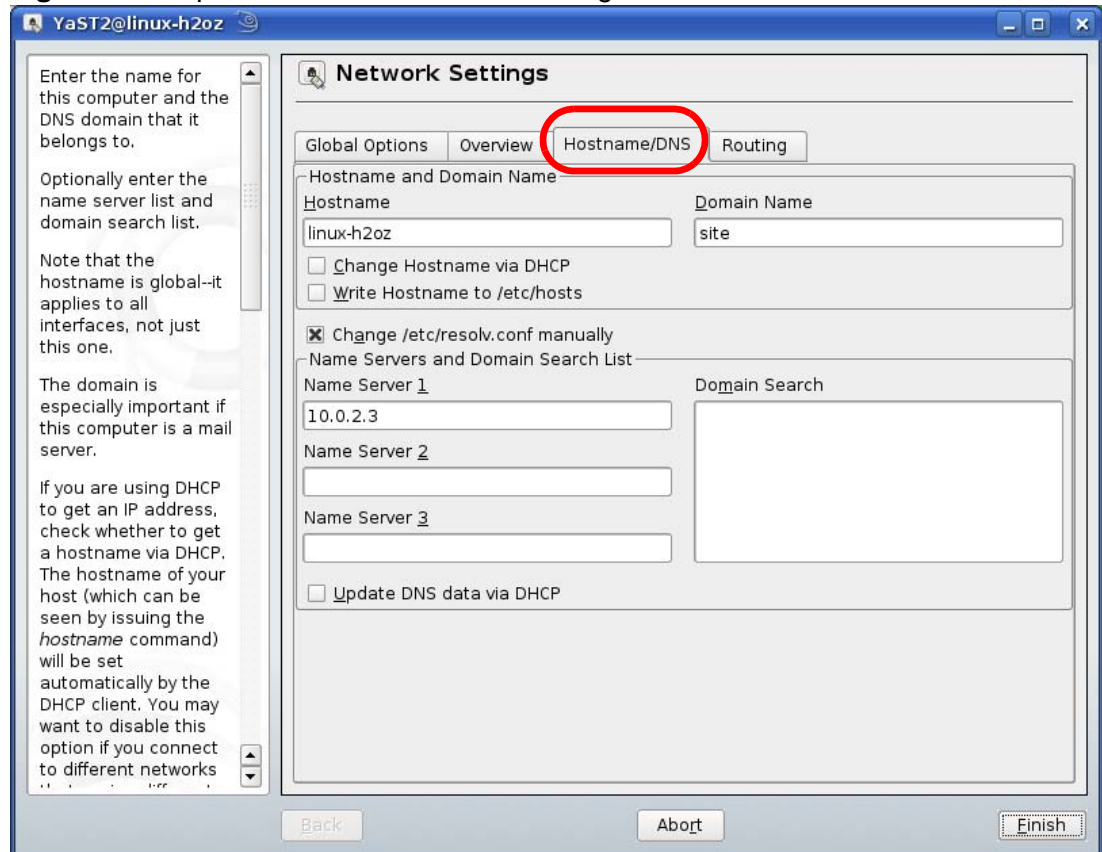
9 Click **Finish** to save your settings and close the window.

Verifying Settings

Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 184 openSUSE 10.3: KNetwork Manager

When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 185 openSUSE: Connection Status - KNetwork Manager
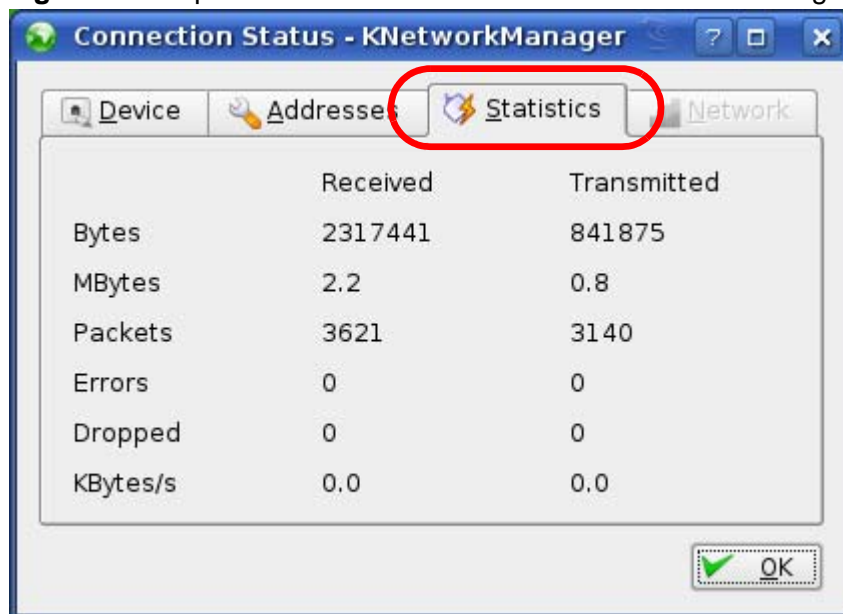
Pop-up Windows, JavaScripts and Java Permissions

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.
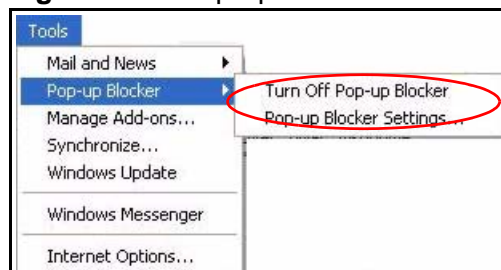
Internet Explorer Pop-up Blockers

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 186 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 187 Internet Options: Privacy

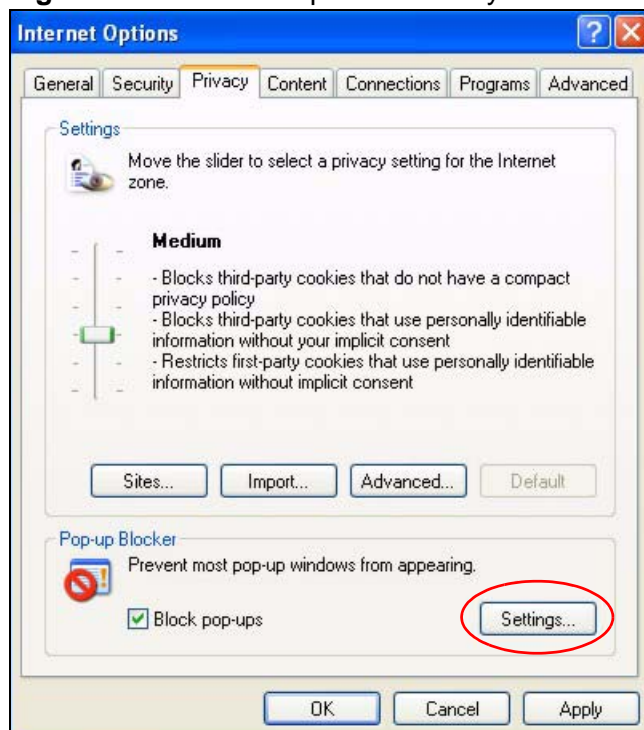**3** Click **Apply** to save this setting.

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.

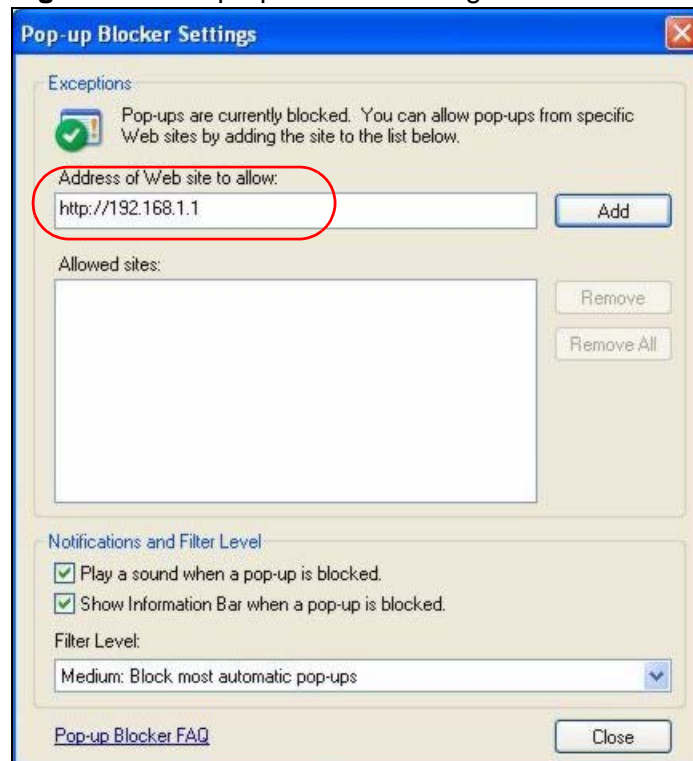**2** Select **Settings…** to open the **Pop-up Blocker Settings** screen.

Figure 188 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://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

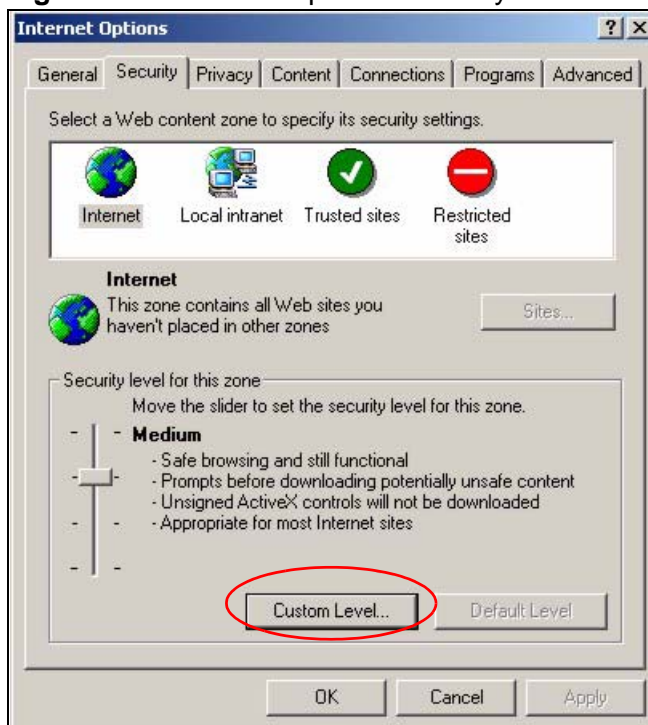**Figure 189**   Pop-up Blocker Settings

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 190 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 191 Security Settings - Java Scripting
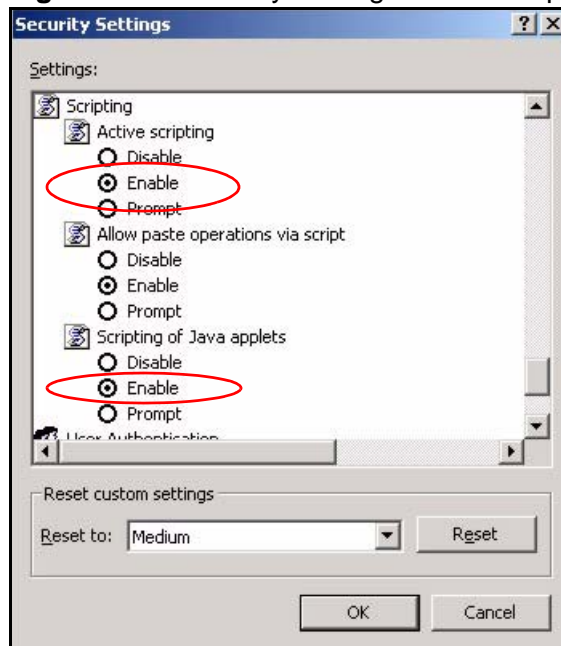
Java Permissions

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 192 Security Settings - Java
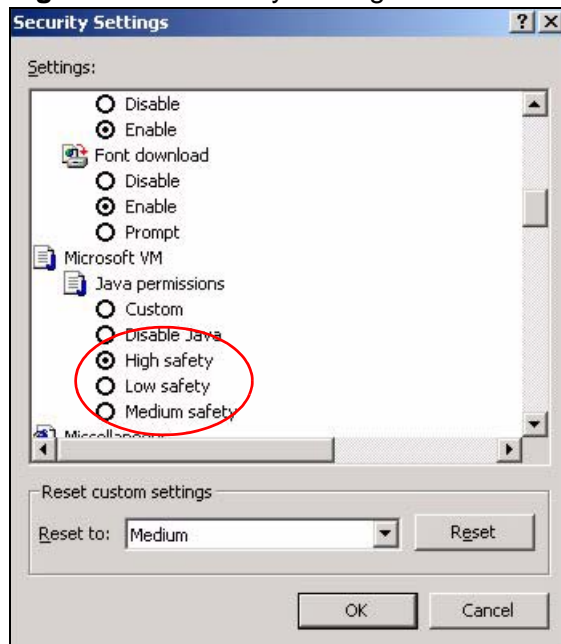
JAVA (Sun)

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 193   Java (Sun)
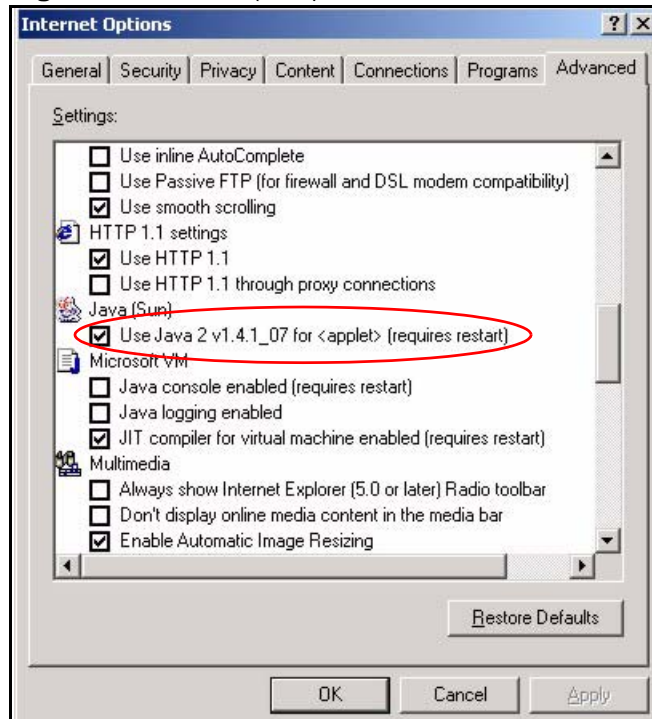
Mozilla Firefox

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 194   Mozilla Firefox: Tools > Options

Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 195 Mozilla Firefox Content Security

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

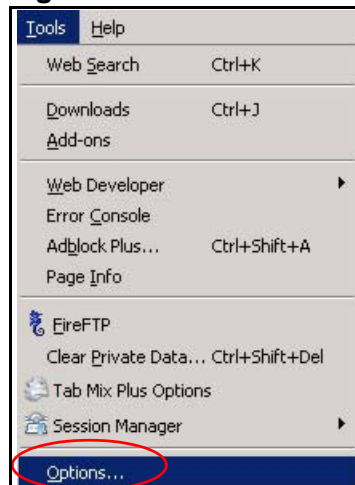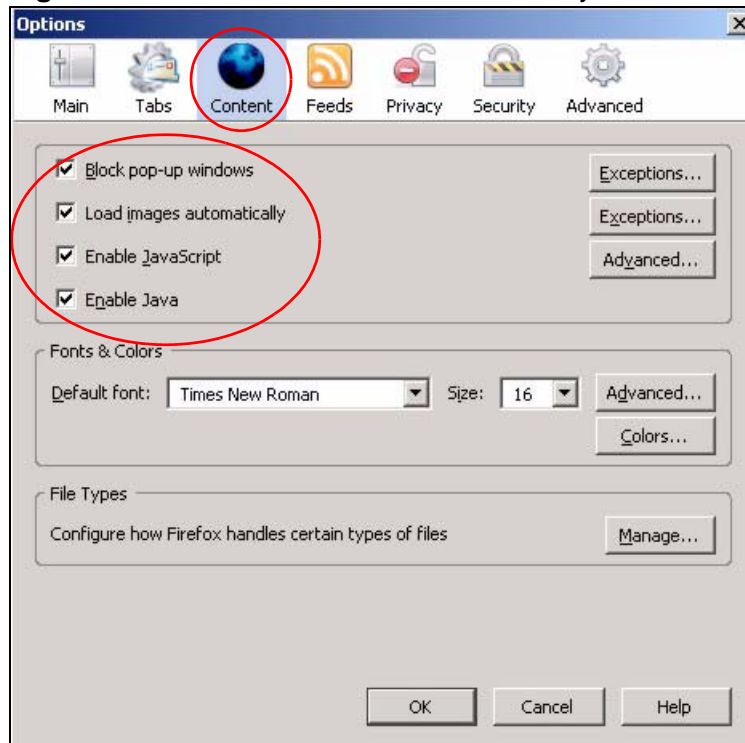IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

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 196 Network Number and Host ID
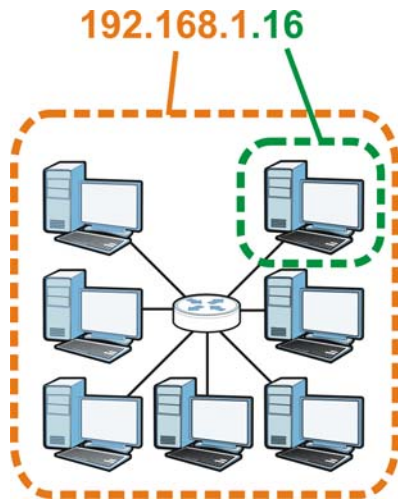
How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

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 97 IP Address Network Number and Host ID Example

	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 98   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 99   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 100 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 197** Subnetting Example: Before Subnetting
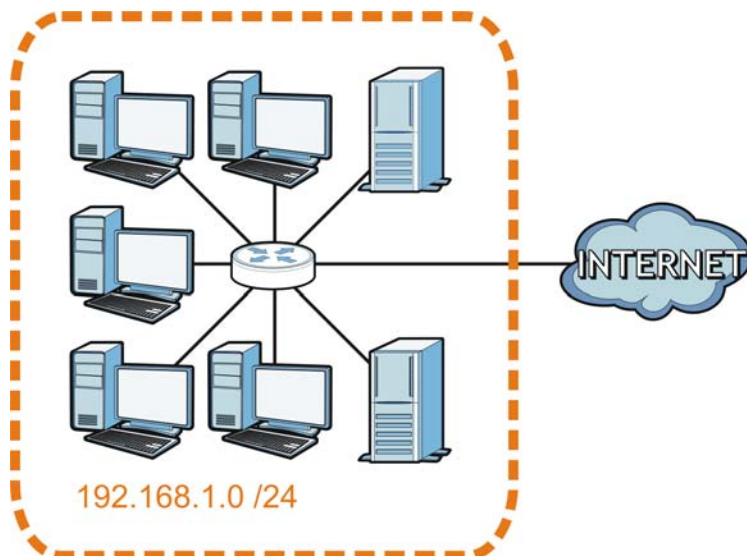
You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 198 Subnetting Example: After Subnetting
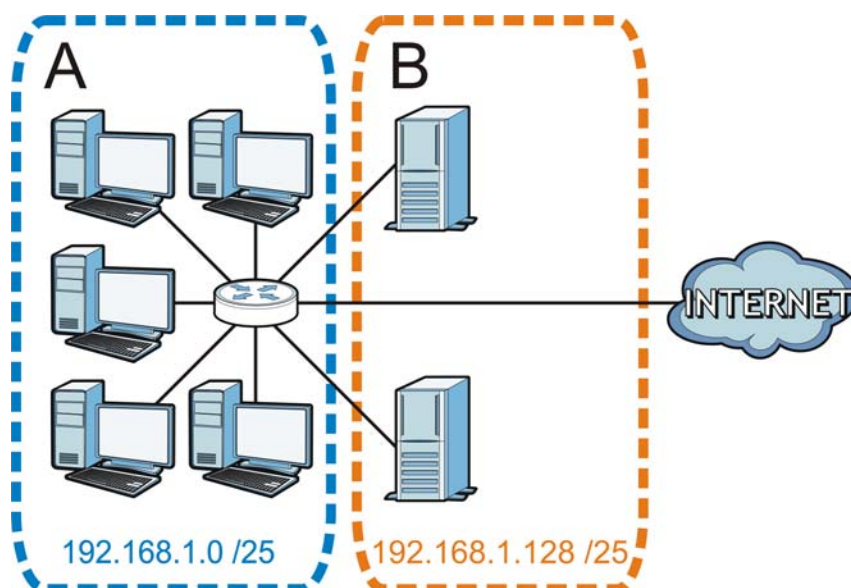
In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of 2^7 – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

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 101 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 102 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 103 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 104 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 105 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
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 106 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 107 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP

addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the P-870HN-51D.

Once you have decided on the network number, pick an IP address for your P-870HN-51D that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your P-870HN-51D will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the P-870HN-51D 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.
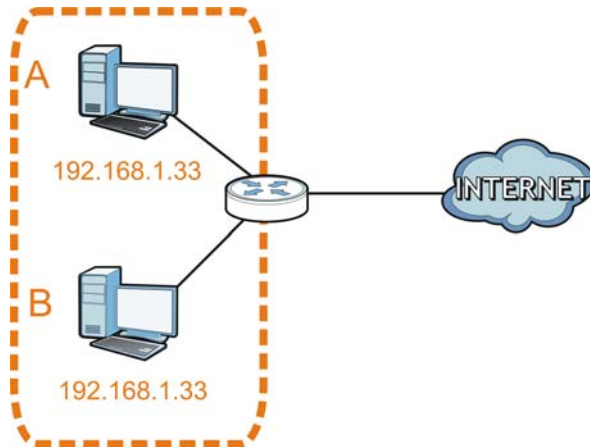
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

Figure 199   Conflicting Computer IP Addresses Example

Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the

following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

Figure 200 Conflicting Router IP Addresses Example
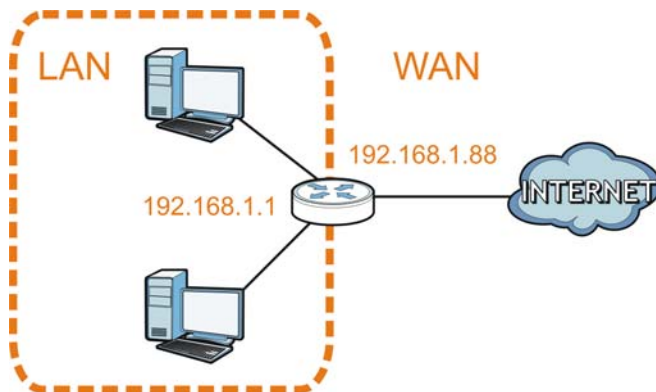
Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 201 Conflicting Computer and Router IP Addresses Example

E
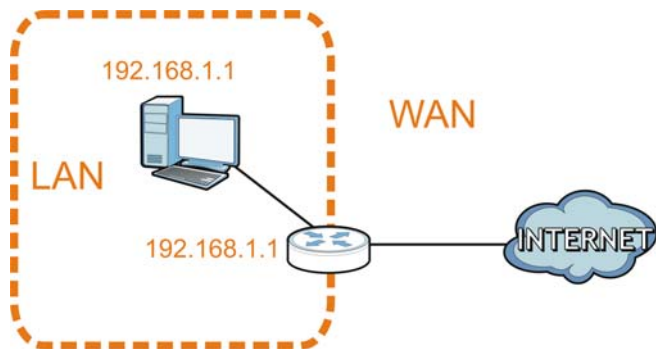
Wireless LANs

Note: Your specific P-870HN-51D may not support all of the wireless security types described in this appendix. See the product specifications for more information about which wireless security types are supported.

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 202   Peer-to-Peer Communication in an Ad-hoc Network
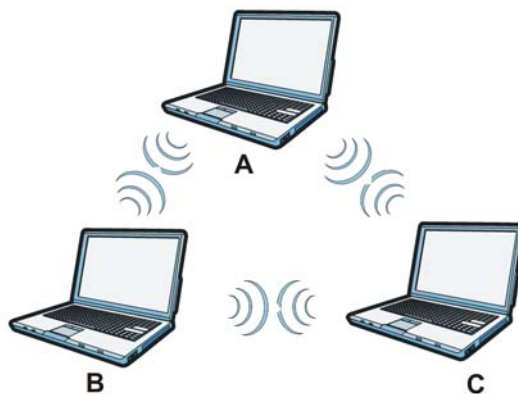
BSS

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 203 Basic Service Set
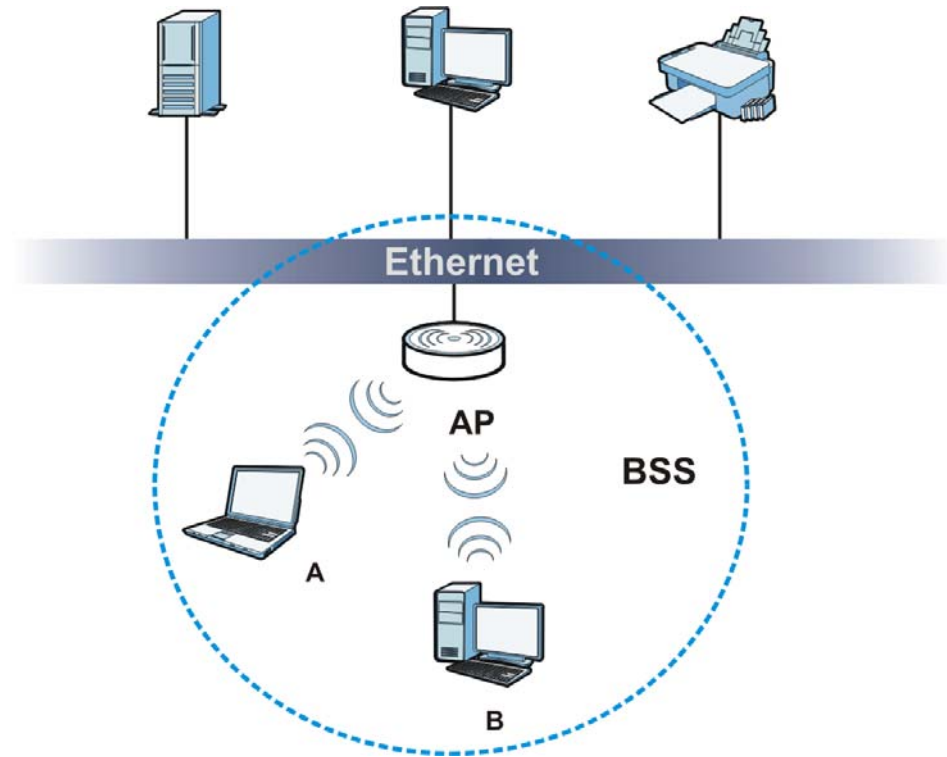
ESS

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 204 Infrastructure WLAN
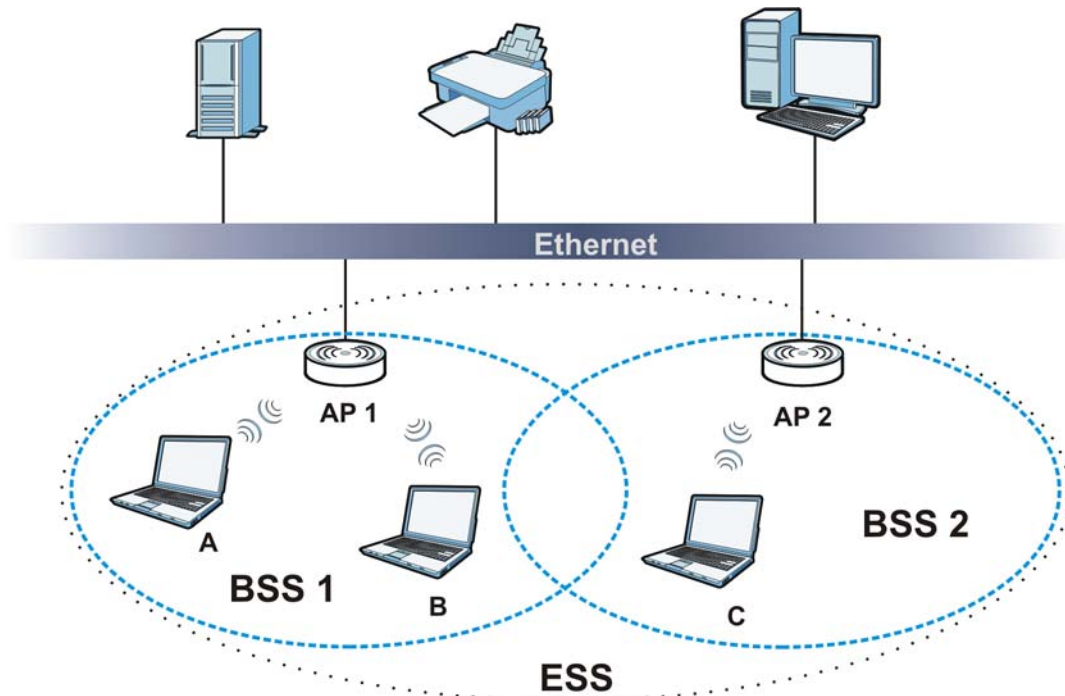
Channel

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 205   RTS/CTS
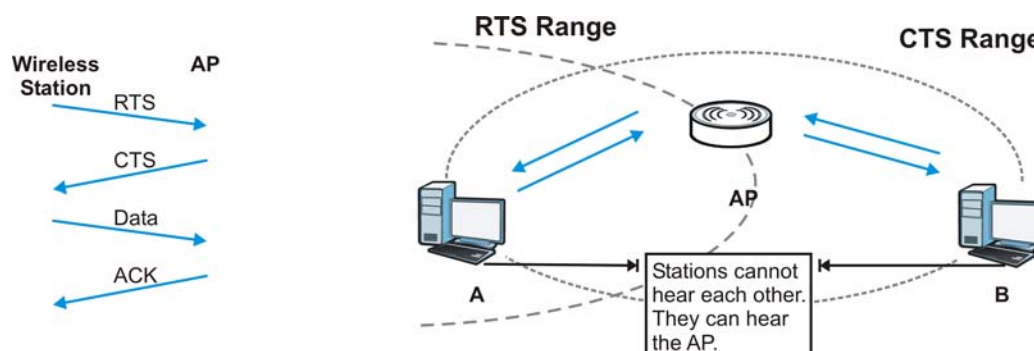
When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

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.

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 P-870HN-51D uses long preamble.

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

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 108 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 P-870HN-51D are data encryption, wireless client authentication, restricting access by device MAC address and hiding the P-870HN-51D identity.

The following figure shows the relative effectiveness of these wireless security methods available on your P-870HN-51D.

Table 109 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 P-870HN-51D 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 110 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 206 WPA(2) with RADIUS Application Example
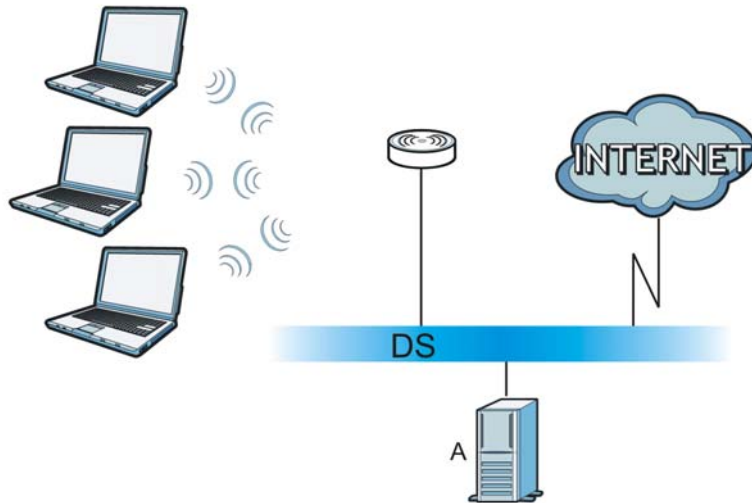
WPA(2)-PSK Application Example

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.

333

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 207 WPA(2)-PSK Authentication
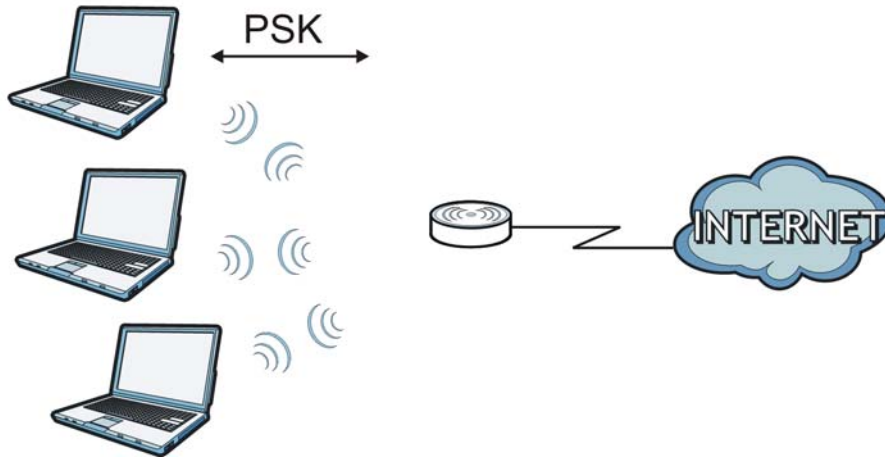
Security Parameters Summary

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 111 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.

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/ code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **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**. Please refer to RFC 1700 for further information about port numbers.

  - 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 112   Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
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	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.

Table 112 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, 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 or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management 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.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
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).

Table 112 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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	Simple File Transfer Protocol.
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.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
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.
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.

Table 112 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

Open Software Announcements

End-User License Agreement for "P-870HN-51D"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED.

1 Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2 Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3 Copyright

The Software and Documentation contain material that is protected by International Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation

4 Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL listed in the below Table (collectively the "Open-Sourced Components") You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components, which have been provided on the License Notice as below for the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the Software, and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5 Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms

and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6 No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7 Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8 Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND

DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9 Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10 Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11 General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

Note: Some components of this product incorporate source code covered under the open source code licenses. To obtain the source code covered under those Licenses, please check ZyXEL Technical Support (support@zyxel.com.tw) to get it.

344

Open-Source Packages for "P-870HN-51D"

3RD PARTY SOFTWARE	VERSION	WEB ADDRESS OF THE SOFTWARE LICENSE TERM
MIPS Linux kernel	2.6.21.5	http://www.linux-mips.org
Bridge-Utils	1.2	http://bridge.sourceforge.net
bftpd	1.0.24	http://www.bftpd.org/
busybox	1'00	http://www.busybox.net/
Dnsmasq	2.48	http://www.thekelleys.org.uk/dnsmasq/
ebtables	2.0.6	http://ebtables.sourceforge.net
iproute2	2.4.7	http://www.linuxgrill.com/anonymous/iproute2
iptables	1.3.8	http://www.netfilter.org
NTFS-3G	1.231	http://www.ntfs-3g.org
openSSL: openSSL library	0.9.7f	http://www.openssl.org/source/license.html
PPP	2.4.1	http://ppp.samba.org/
SSH server: dropbear	0.46	http://www.opensource.org/licenses/mit-license.php
Samba	3.0.34	http://www.samba.org
udhcp	0.9.6	http://udhcp.busybox.net/
zebra	0.93a	http://www.zebra.org/

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Bridge-utils 1.2, Busybox 1.0.0, Bftpd 1.0.24, Dnsmasq 2.48, Ebtables 2.0.6, Iproute2 2.4.7, Iptables 1.3.8, MIPS linux kernel 2.6.21.5, NTFS-3G 1.231, Ppp 2.4.1, Samba 3.0.34, Udhcp 0.9.6 and zebra 0.93a under below GPL license

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain

patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions,

and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same

place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/ OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN

IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes Ssh server dropbear v0.46 under the MIT-Style License.

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

This Product includes OpenSSL v0.9.7f under the OpenSSL License.

OpenSSL License

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

H

Legal Information

Copyright

Copyright © 2010 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

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.

Your use of the P-870HN-51D is subject to the terms and conditions of any related service providers.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IMPORTANT NOTE

Device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems; users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

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

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

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

362