P-320W v3

DRAFT

802.11g Wireless Firewall Router

User's Guide

Default Login Details

IP Address	http://192.168.1.1
Password	1234

Firmware Version 1.0
Edition 1, 3/2009

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the P-320W v3 using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

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.

- Supporting Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See http://www.zyxel.com/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.

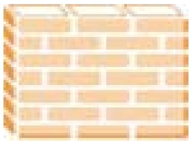
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-320W v3 may be referred to as the “P-320W v3”, the “device”, the “product” or the “system” 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.

P-320W v3 	Computer 	Notebook computer
Server 	Modem 	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 power outlet.
- 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.
- 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

PART I
Introduction

1

Getting to Know Your P-320W v3

1.1 Overview

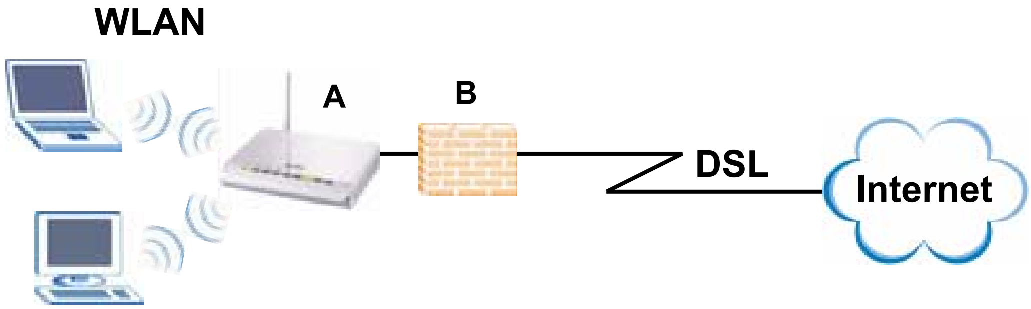
This chapter introduces the main features and applications of the P-320W v3.

The P-320W v3 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

It acts as a secure broadband router for all data passing between the Internet and your local network. You can set up a wireless network with other IEEE 802.11b/g compatible devices.

The following figure shows computers in a WLAN connecting to the P-320W v3 (**A**), which has a DSL connection to the Internet. The P-320W v3 has a built-in firewall (**B**) to protect the network. It also has the Network Address Translation (NAT) feature enabled by default.

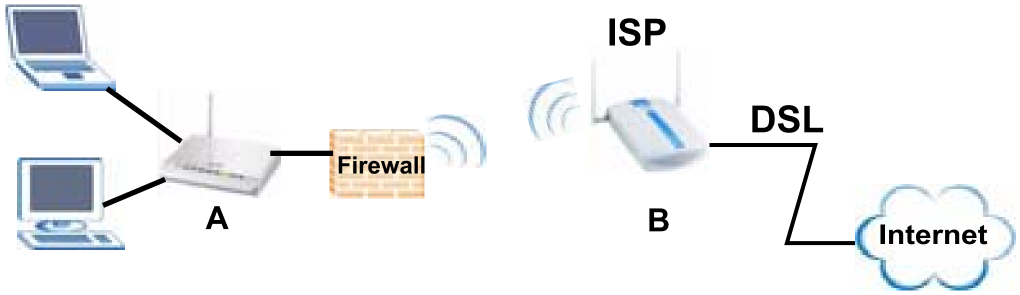
Figure 1 Secure Wireless Internet Access in Router Mode



The P-320W v3 can also serve as a wireless client enabling network devices to connect to an existing wired or wireless network. Features, such as firewall and NAT, are available. Networking devices cannot connect wirelessly to the P-320W v3 when it is acting as a wireless client.

In the following figure, the P-320W v3 (**A**) enables the wired computers to connect to the access point (**B**) and gain access to LAN/Internet.

Figure 2 Using the P-320W v3 as a Wireless Client



1.2 Ways to Manage the P-320W v3

Use any of the following methods to manage the P-320W v3.

- **Web Configurator**. This is recommended for everyday management of the P-320W v3 using a (supported) web browser.
- **SNMP**. Simple Network Management Protocol is a communication protocol for collecting information from devices on the network.

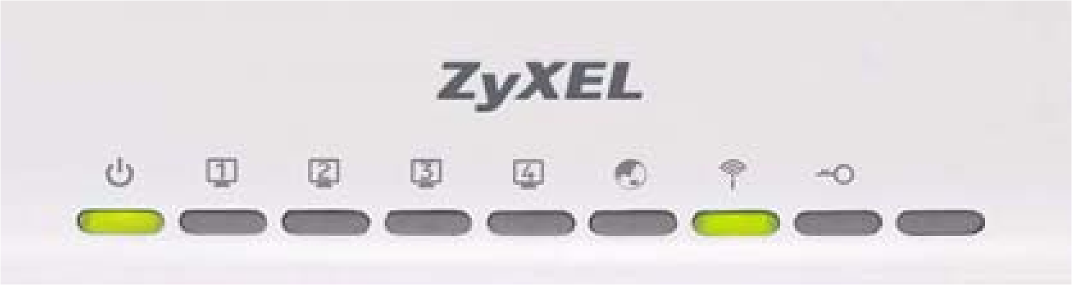
1.3 Good Habits for Managing the P-320W v3

Do the following things regularly to make the P-320W v3 more secure and to manage the P-320W v3 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-320W v3 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the P-320W v3. You could simply restore your last configuration.

1.4 LEDs

Figure 3 Front Panel



The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The P-320W v3 is receiving power and functioning properly.
		Off	The P-320W v3 is not receiving power.
LAN 1-4	Green	On	The P-320W v3 has a successful 10MB Ethernet connection.
		Blinking	The P-320W v3 is sending/receiving data.
	Amber	On	The P-320W v3 has a successful 100MB Ethernet connection.
		Blinking	The P-320W v3 is sending/receiving data.
		Off	The LAN is not connected.
WAN	Green	On	The P-320W v3 has a successful 10MB WAN connection.
		Blinking	The P-320W v3 is sending/receiving data.
	Amber	On	The P-320W v3 has a successful 100MB Ethernet connection.
		Blinking	The P-320W v3 is sending/receiving data.
		Off	The WAN connection is not ready, or has failed.
WLAN	Green	On	The P-320W v3 is ready, but is not sending/ receiving data through the wireless LAN.
		Blinking	The P-320W v3 is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
WPS	Green	On	WPS (WiFi Protected Setp) is configurered on your device.
		Blinking	The P-320W v3 is negotiating WPS.
		Off	WPS is disabled on your device.

CHAPTER 2

Introducing the Web Configurator

This chapter describes how to access the P-320W v3 web configurator and provides an overview of its screens.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy setup and management of the P-320W v3 via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions or Safari 2.0 or 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).

Refer to the Troubleshooting chapter to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

1 Make sure your P-320W v3 hardware is properly connected and prepare your computer or computer network to connect to the P-320W v3 (refer to the Quick Start Guide).

2 Launch your web browser.

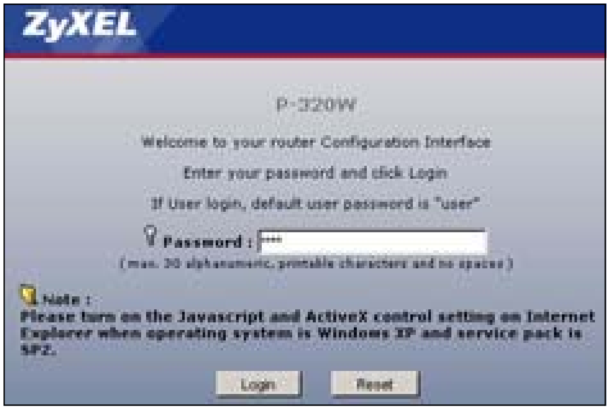
3 Type "http://192.168.1.1" as the website address.

Your computer must be in the same subnet in order to access this website address.

Note: Enable the DHCP Server. The P-320W v3 assigns your computer an IP address on the same subnet.

4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

Figure 4 Change Password Screen



P-320W

Welcome to your router Configuration Interface

Enter your password and click Login

If User login, default user password is "user"

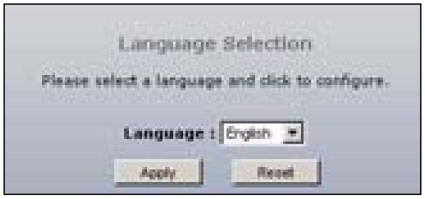
Password : ****

(max. 30 alphanumeric, printable characters and no spaces)

Note :
Please turn on the Javascript and ActiveX control setting on Internet Explorer when operating system is Windows XP and service pack is SP2.

5 Select your language in the screen that follows and click **Apply** or click **Reset**.

Figure 5 Language Selection



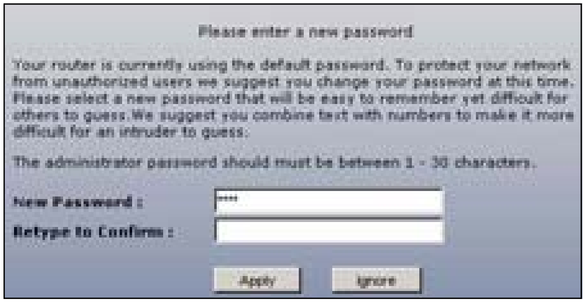
Language Selection

Please select a language and click to configure.

Language : English

6 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 6 Change Password Screen



Please enter a new password

Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess.We suggest you combine text with numbers to make it more difficult for an intruder to guess.

The administrator password should must be between 1 - 30 characters.

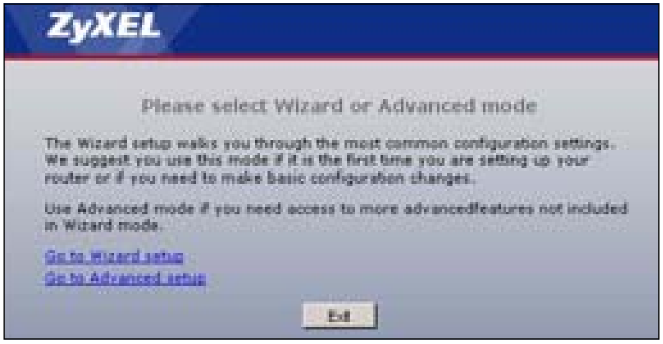
New Password : ****

Retype to Confirm :

7 Click **Go to Wizard Setup** to use the Configuration Wizard for basic Internet and Wireless setup.

8 **Click Go to Advanced Setup** to view and configure all the P-320W v3's settings.

Figure 7 Choose Your Setup Mode.



Please select Wizard or Advanced mode

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.

Use Advanced mode if you need access to more advancedfeatures not included in Wizard mode.

Go to Wizard setup
Go to Advanced setup

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the P-320W v3 if this happens.

2.3 Resetting the P-320W v3

If you forget your password or IP address, or you cannot access the web configurator, you will need to use the **RESET** button at the back of the P-320W v3 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "1234" and the IP address will be reset to "192.168.1.1".

2.3.1 Procedure to Use the Reset Button

1 Make sure the power LED is on.

2 Press the **RESET** button for longer than 1 second to restart/reboot the P-320W v3.

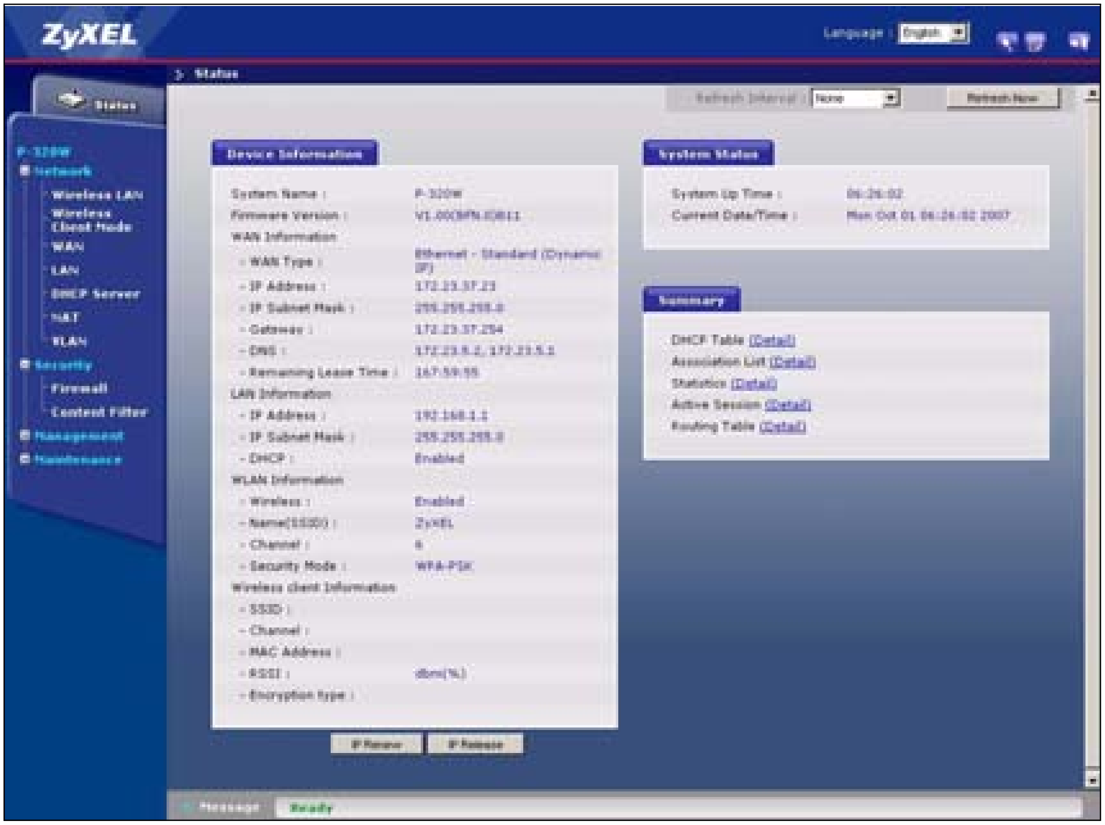
3 Press the **RESET** button for longer than five seconds to set the P-320W v3 back to its factory-default configurations.

2.4 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Status** screen.

Click on **Status**. The screen below shows the status screen.

Figure 8 Web Configurator Status Screen



System Name : P-320W
Firmware Version : V1.00(BFN.0)B11
WAN Information
- WAN Type : Ethernet - Standard (Dynamic IP)
- IP Address : 172.23.37.23
- IP Subnet Mask : 255.255.255.0
- Gateway : 172.23.37.254
- DNS : 172.23.5.2, 172.23.5.1
- Remaining Lease Time : 167:59:55
LAN Information
- IP Address : 192.168.1.1
- IP Subnet Mask : 255.255.255.0
- DHCP : Enabled
WLAN Information
- Wireless : Enabled
- Name(SSID) : ZyXEL
- Channel : 6
- Security Mode : WPA-PSK
Wireless client Information
- SSID :
- Channel :
- MAC Address :
- RSSI : dbm(%)
- Encryption type :

System Up Time : 06:26:02
Current Date/Time : Mon Oct 01 06:26:02 2007

DHCP Table (Detail)
Association List (Detail)
Statistics (Detail)
Active Session (Detail)
Routing Table (Detail)

Ready

The following table describes the icons shown in the **Status** screen.

Table 2 Status Screen Icon Key

ICON	DESCRIPTION
Language : English	Select a language from the drop-down list box to have the web configurator display in that language.
	Click this icon to open the setup wizard.
	Click this icon to view copyright and a link for related product information.
	Click this icon at any time to exit the web configurator.
Refresh Interval: 20 seconds	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
Refresh Now	Click this button to refresh the status screen statistics.

The following table describes the labels shown in the **Status** screen.

Table 3 Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
WAN Information	
WAN Type	This shows the P-320W v3's WAN type or how it acquires its WAN IP address.
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- Gateway	This shows the gateway address of the WAN connection.
- DNS	This shows the Domain Name System (DNS) addresses of the WAN connection.
- Remaining Lease Time	This shows how long the P-320W v3 can use the current WAN IP address.
LAN Information	
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP is enabled.
WLAN Information	
- Wireless	This shows if the wireless LAN is enabled.
- Name(SSID)	This shows a descriptive name used to identify the P-320W v3 in the wireless LAN.
- Channel	This shows the channel number which you select manually. Note: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.
- Security Mode	This shows the level of wireless security the P-320W v3 is using.
Wireless client Information	
- SSID	This shows a descriptive name used to identify the P-320W v3 in the guest WLAN network.
- Channel	This shows the channel number which you select manually. Note: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.
- MAC Address	This shows the wireless adapter MAC Address of guest WLAN on your device.
- RSSI	This shows the IP address for guest WLAN network.
- Encryption Type	This shows the subnet mask for guest WLAN network.

Table 3 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
System Status	
- System Up Time	This is the total time the P-320W v3 has been on.
- Current Date/Time	This field displays your P-320W v3's present date and time.
Summary	
- DHCP Table	Use this screen to view current DHCP client information.
- Association List	Use this screen to view the a list of devices the P-320W v3 is currently associated with.
- Statistics	Use this screen to view port status and packet specific statistics.
- Active Session	Use this screen to view a list of wireless clients currently connected to the P-320W v3.
- Routing Table	Use this screen to view a list of the traffic routes used by the P-320W v3.
IP Renew	Click this to renew the P-320W v3's IP address.
IP Release	Click this to release the P-320W v3's IP address.

2.4.1 Navigation Panel

Use the sub-menus on the navigation panel to configure P-320W v3 features.

The following table describes the sub-menus.

Table 4 Sub-menus

LINK	TAB	FUNCTION
Status		This screen shows the P-320W v3's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the P-320W v3 to block access to devices or block the devices from accessing the P-320W v3.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add stations to the wireless network via the Push Button.
	Advanced	This screen allows you to configure advanced wireless settings.
Wireless Client Mode		This screen allows you to use your P-320W v3 as a wireless client and connect to a wireless access point.
WAN	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
	Advanced	Use this screen to configure other advanced properties.
	Traffic Redirect	Use this screen to enable a backup gateway IP address for the P-320W v3.

Table 4 Sub-menus

LINK	TAB	FUNCTION
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
DHCP Server	General	Use this screen to enable the P-320W v3's DHCP server.
	Static DHCP	Use this screen to assign permanent IP addresses to specific devices.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to configure servers behind the P-320W v3.
	Trigger Port	Use this screen to change your P-320W v3's port triggering settings.
VLAN	VLAN Setup	Use this screen to assign VLAN IDs to the physical ports of the P-320W v3.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
Content Filter	Filter	Use this screen to block certain web features and sites containing certain keywords in the URL.
Management		
IP Static Route	IP Static Route	Use this screen to configure IP static routes.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the P-320W v3.
	SNMP	Use this screen to configure SNMP in your P-320W v3.
	Security	Use this screen to set your P-320W v3 to not respond to ping from WAN.
UPnP	General	Use this screen to enable UPnP on the P-320W v3.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Dynamic DNS	Use this screen to enable dynamic DNS.
	Time Setting	Use this screen to change your P-320W v3's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your P-320W v3's log settings.

Table 4 Sub-menus

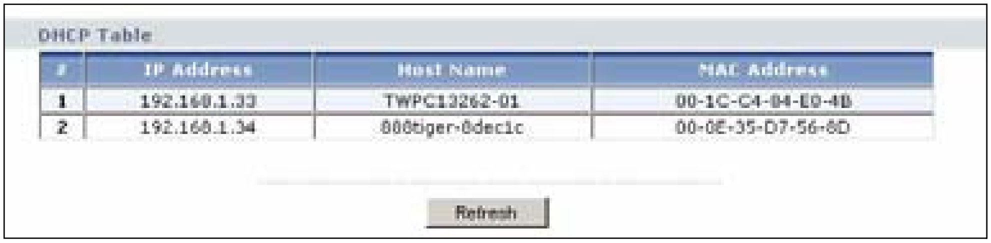
LINK	TAB	FUNCTION
Tools	Firmware	Use this screen to upload firmware to your P-320W v3.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your P-320W v3.
	Restart	This screen allows you to reboot the P-320W v3 without turning the power off.

2.4.2 Summary: DHCP Table

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-320W v3's LAN and/or Guest WLAN as DHCP server(s) or disable them. When configured as a server, the P-320W v3 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on that network, or else the computer must be manually configured.

Click the **DHCP Table (Details...)** hyperlink in the **Status** screen. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the P-320W v3's DHCP server.

Figure 9 Summary: DHCP Table



DHCP Table

#	IP Address	Host Name	MAC Address
1	192.168.1.33	TWPC13262-01	00-1C-C4-84-E0-4B
2	192.168.1.34	888tiger-0dec1c	00-0E-35-D7-56-8D

The following table describes the labels in this screen.

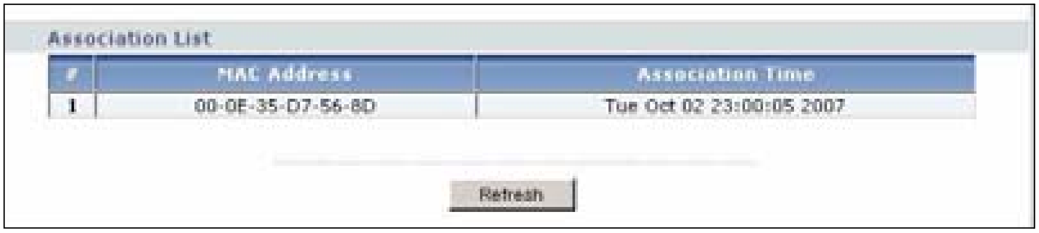
Table 5 Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the client.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click **Refresh** to renew the screen.

2.4.3 Summary: Association List

Click the **Association List (Details...)** hyperlink in the **Status** screen. Read-only information here includes the MAC address of a device and its time of association with the P-320W v3. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Figure 10 Summary: Association List



Association List

#	MAC Address	Association Time
1	00-0E-35-D7-56-8D	Tue Oct 02 23:00:05 2007

The following table describes the labels in this screen.

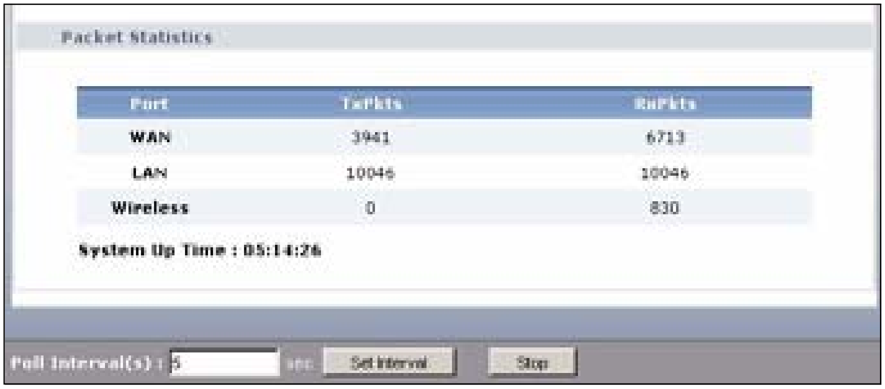
Table 6 Summary: Association List

LABEL	DESCRIPTION
#	This is the index number of the client.
MAC Address	This shows the MAC address of the device associated with the P-320W v3.
Association Time	This shows the date and time when the association with a device is made.
Refresh	Click **Refresh** to renew the screen.

2.4.4 Summary: Statistics

Click the **Statistics (Details...)** hyperlink in the **Status** screen. Read-only information here includes port status, packet specific statistics and the "system up time". The **Poll Interval(s)** field is configurable and is used for refreshing the screen.

Figure 11 Summary: Statistics



Packet Statistics

Port	TxPkts	RxPkts
WAN	3941	6713
LAN	10046	10046
Wireless	0	830

System Up Time : 05:14:26

Poll Interval(s) : 5 sec

The following table describes the labels in this screen.

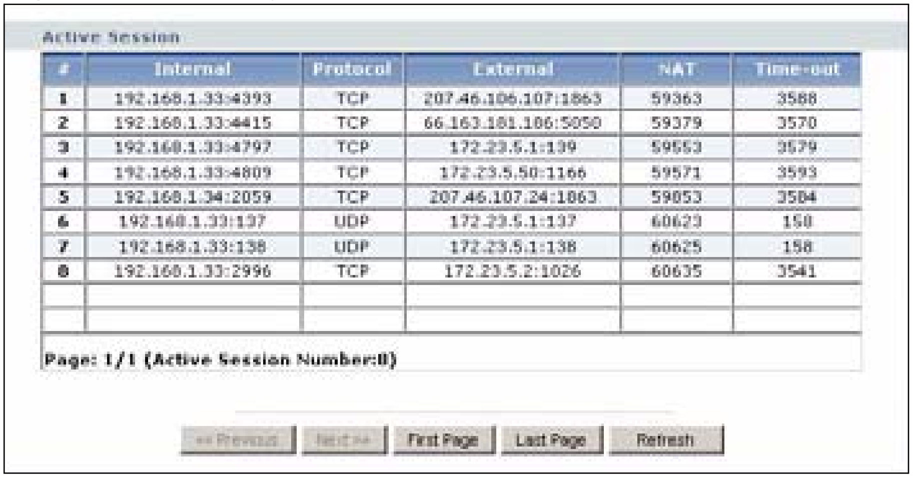
Table 7 Summary: Statistics

LABEL	DESCRIPTION
Port	This is the P-320W v3's port type.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
System Up Time	This is the total time the P-320W v3 has been on.
Poll Interval(s)	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 **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

2.4.5 Summary: Active Session

Click the **Active Session (Details...)** hyperlink in the **Status** screen. View a list of devices that are currently associated to the P-320W v3 and read-only information such as internal/external IP addresses and Time-out.

Figure 12 Summary: Active Session



Active Session

#	Internal	Protocol	External	NAT	Time-out
1	192.168.1.33:4393	TCP	207.46.106.107:1863	59363	3588
2	192.168.1.33:4415	TCP	66.163.181.186:5050	59379	3570
3	192.168.1.33:4797	TCP	172.23.5.1:139	59553	3579
4	192.168.1.33:4809	TCP	172.23.5.50:1166	59571	3593
5	192.168.1.34:2059	TCP	207.46.107.24:1863	59853	3584
6	192.168.1.33:137	UDP	172.23.5.1:137	60623	158
7	192.168.1.33:138	UDP	172.23.5.1:138	60625	158
8	192.168.1.33:2996	TCP	172.23.5.2:1026	60635	3541

Page: 1/1 (Active Session Number:8)

The following table describes the labels in this screen.

Table 8 Summary: Active Sessiont

LABEL	DESCRIPTION
#	This is the index number of the active session.
Internal	This is the internal IP address of the device.
Protocol	This is the transfer protocol used.
External	This is the external IP address of the device.
NAT	This is the numerical tag for the NAT entry.
Time out	This is the time out value (in minutes) of the NAT entry.

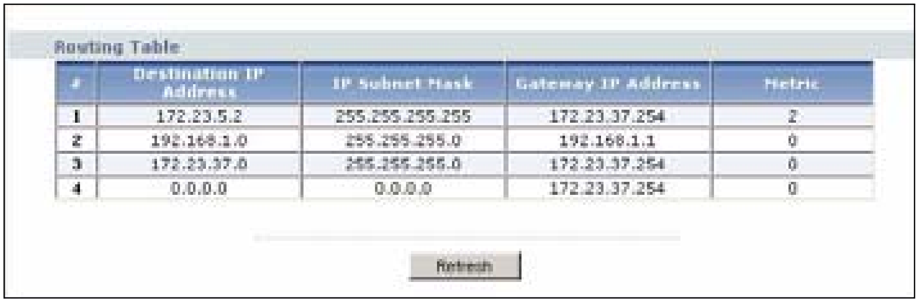
Table 8 Summary: Active Sessiont

LABEL	DESCRIPTION
Page... (Active Session Number)	This shows the current page you are looking at as well as the total number of pages of the association list.
Previous	Click this to go to the previous page.
Next	Click this to go to the next page.
First Page	Click this to go to the first page.
Last Page	Click this to go to the last page.
Refresh	Click **Refresh** to renew the screen.

2.4.6 Summary: Routing Table

Click the **Routing Table (Details...)** hyperlink in the **Status** screen. View a list of the static routes configured in the P-320W v3.

Figure 13 Summary: Routing Table



Routing Table

#	Destination IP Address	IP Subnet Mask	Gateway IP Address	Metric
1	172.23.5.2	255.255.255.255	172.23.37.254	2
2	192.168.1.0	255.255.255.0	192.168.1.1	0
3	172.23.37.0	255.255.255.0	172.23.37.254	0
4	0.0.0.0	0.0.0.0	172.23.37.254	0

The following table describes the labels in this screen.

Table 9 Summary: Routing Table

LABEL	DESCRIPTION
#	This is the index number of the routing entry.
Destination IP Address	This is the destination IP address of the outgoing traffic.
IP Subnet Mask	This is teh IP subnet mask of the traffic.
Gateway IP Address	This is the gateway IP address of the host computer.
Metric	This is the numerical tag for the routing entry.
Refresh	Click **Refresh** to renew the screen.

3

Connection Wizard

This chapter provides information on the wizard setup screens in the web configurator.

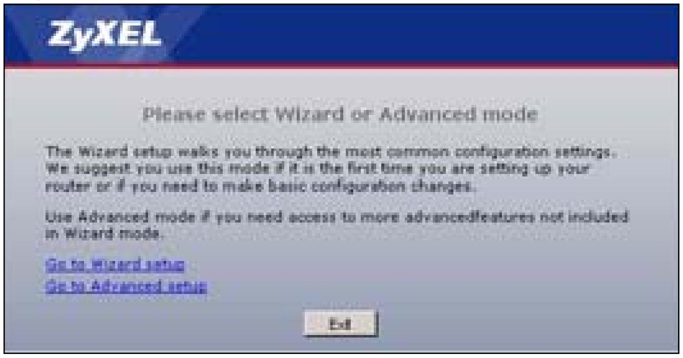
3.1 Wizard Setup

The web configurator's wizard setup helps you configure your device to access the Internet. Refer to your ISP (Internet Service Provider) checklist in the Quick Start Guide to know what to enter in each field. Leave a field blank if you don't have that information.

1 After you access the P-320W v3 web configurator, click the **Go to Wizard setup** hyperlink.

You can click the **Go to Advanced setup** hyperlink to skip this wizard setup and configure advanced features accordingly.

Figure 14 Select Wizard or Advanced Mode



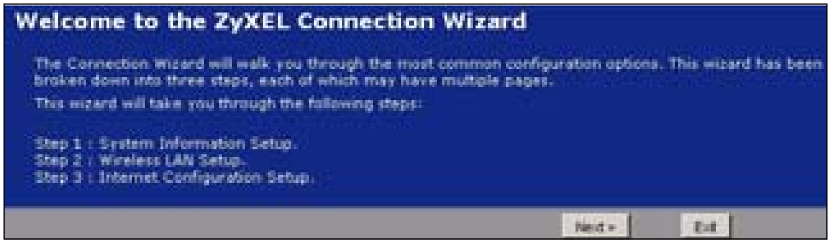
Please select Wizard or Advanced mode

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.

Use Advanced mode if you need access to more advancedfeatures not included in Wizard mode.

2 Read the on-screen information and click **Next**.

Figure 15 Welcome to the Connection Wizard



Welcome to the ZyXEL Connection Wizard

The Connection Wizard will walk you through the most common configuration options. This wizard has been broken down into three steps, each of which may have multiple pages.

This wizard will take you through the following steps:

Step 1 : System Information Setup.
Step 2 : Wireless LAN Setup.
Step 3 : Internet Configuration Setup.

3.2 Connection Wizard: STEP 1: System Information

System Information contains administrative and system-related information.

3.2.1 System Name

System Name is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

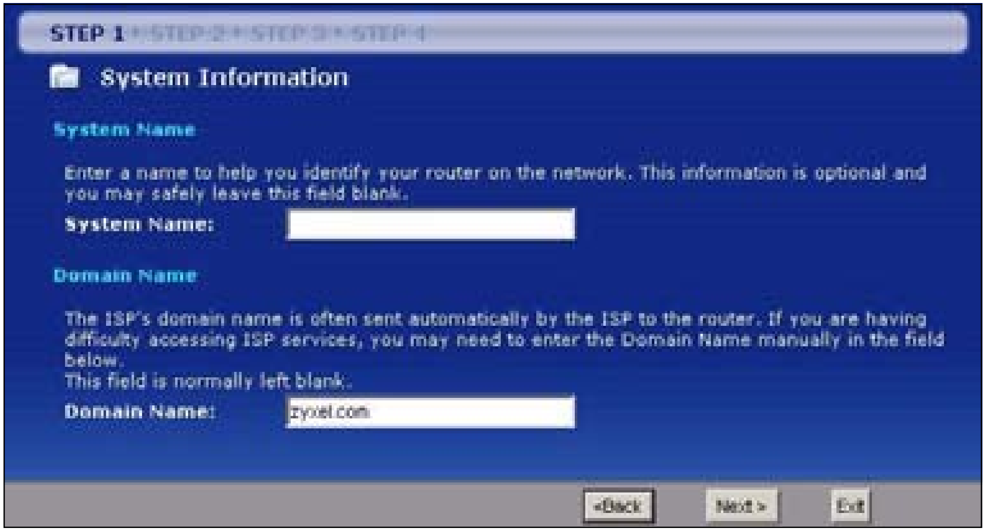
- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the P-320W v3 **System Name**.

3.2.2 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the P-320W v3 via DHCP.

Click **Next** to configure the P-320W v3 for Internet access.

Figure 16 Wizard Step 1: System Information



System Information

System Name

Enter a name to help you identify your router on the network. This information is optional and you may safely leave this field blank.

System Name:

Domain Name

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.
This field is normally left blank.

Domain Name: zyxel.com

The following table describes the labels in this screen.

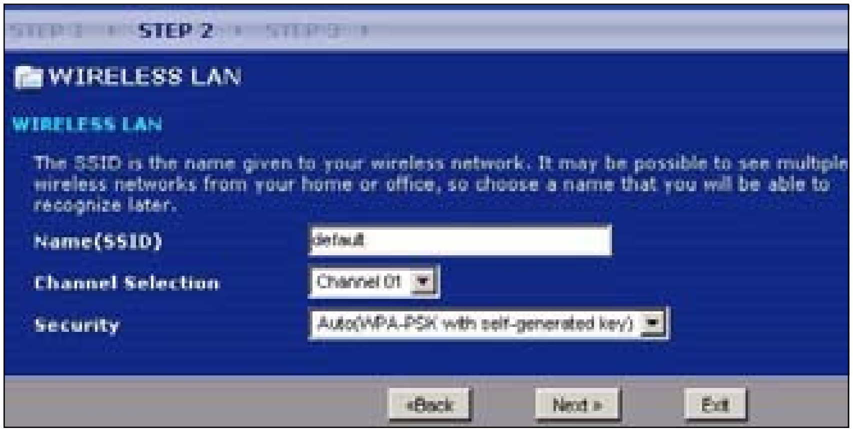
Table 10 Wizard Step 1: System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the P-320W v3 in an Ethernet network. Enter a descriptive name. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Type the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

3.3 Connection Wizard: STEP 2: Wireless LAN

Set up your wireless LAN using the following screen.

Figure 17 Wizard Step 2: Wireless LAN



WIRELESS LAN

The SSID is the name given to your wireless network. It may be possible to see multiple wireless networks from your home or office, so choose a name that you will be able to recognize later.

Name(SSID) default

Channel Selection Channel 01

Security Auto(WPA-PSK with self-generated key)

The following table describes the labels in this screen.

Table 11 Wizard Step 2: Wireless LAN

LABEL	DESCRIPTION
Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the P-320W v3, make sure all wireless stations use the same SSID in order to access the network.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel that is not used by any nearby devices. Note: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

Table 11 Wizard Step 2: Wireless LAN

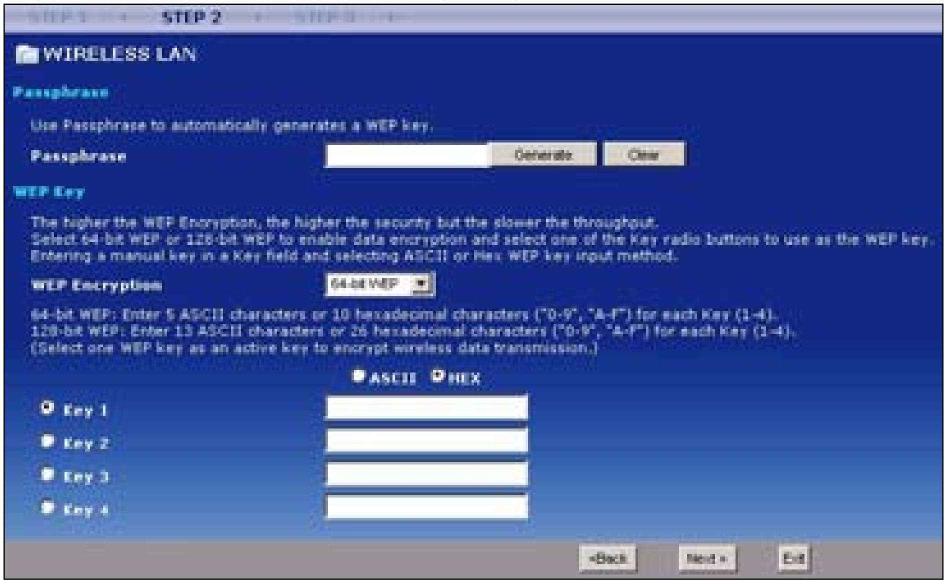
LABEL	DESCRIPTION
Security	Select a **Security** level from the drop-down list box. Choose **Auto (WPA-PSK with self-generated key)** to have the P-320W v3 generate a pre-shared key automatically. A screen pops up displaying the generated pre-shared key after you click **Next**. Write down the key for use later when connecting other wireless devices to your network. Click **OK** to continue. Choose **None** to have no wireless LAN security configured. If you do not enable any wireless security on your P-320W v3, your network is accessible to any wireless networking device that is within range. If you choose this option, skip directly to Section 3.4 on page 43. Choose **Basic (WEP)** security if you want to configure WEP Encryption parameters. If you choose this option, go directly to Section 3.3.1 on page 42. **Basic (WEP)** is only available when WPS (WiFi Protected Setup) is disabled. See Section 4.3.5 on page 60 for more information about WPS. Choose **Extend** (**WPA-PSK with customized key**) security to configure a Pre-Shared Key. Choose this option only if your wireless clients support WPA-PSK. If you choose this option, skip directly to Section 3.3.2 on page 43.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

Note: The wireless stations and P-320W v3 must use the same SSID, channel ID and WEP encryption key (if WEP is enabled), WPA-PSK (if WPA-PSK is enabled) or WPA2-PSK (if WPA2-PSK is enabled) for wireless communication.

3.3.1 Basic(WEP) Security

Choose **Basic(WEP)** to setup WEP Encryption parameters.

Figure 18 Wizard Step 2: Basic (WEP) Security



STEP 1 → STEP 2 → STEP 3

WIRELESS LAN

Passphrase

Use Passphrase to automatically generates a WEP key.

Passphrase

WEP Key

The higher the WEP Encryption, the higher the security but the slower the throughput.
Select 64-bit WEP or 128-bit WEP to enable data encryption and select one of the Key radio buttons to use as the WEP key.
Entering a manual key in a Key field and selecting ASCII or Hex WEP key input method.

WEP Encryption: 64-bit WEP

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

○ ASCII ● HEX

● Key 1
○ Key 2
○ Key 3
○ Key 4

The following table describes the labels in this screen.

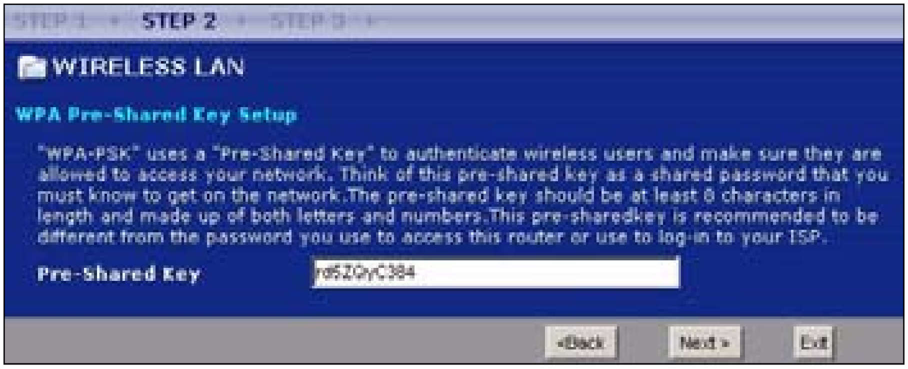
Table 12 Wizard Step 2: Basic (WEP) Security

LABEL	DESCRIPTION
Passphrase	Type a Passphrase (up to 32 printable characters) and click **Generate**. The P-320W v3 automatically generates a WEP key. Click **Clear** to make this field blank.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding “0x” is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the P-320W v3 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

3.3.2 Extend (WPA-PSK) Security

Choose **Extend (WPA-PSK)** security in the Wireless LAN setup screen to set up a **Pre-Shared Key**.

Figure 19 Wizard Step 2: Extend (WPA-PSK) Security



WPA Pre-Shared Key Setup

"WPA-PSK" uses a "Pre-Shared Key" to authenticate wireless users and make sure they are allowed to access your network. Think of this pre-shared key as a shared password that you must know to get on the network.The pre-shared key should be at least 8 characters in length and made up of both letters and numbers.This pre-sharedkey is recommended to be different from the password you use to access this router or use to log-in to your ISP.

Pre-Shared Key: rd5ZQyC384

The following table describes the labels in this screen.

Table 13 Wizard Step 2: Extend (WPA-PSK) Security

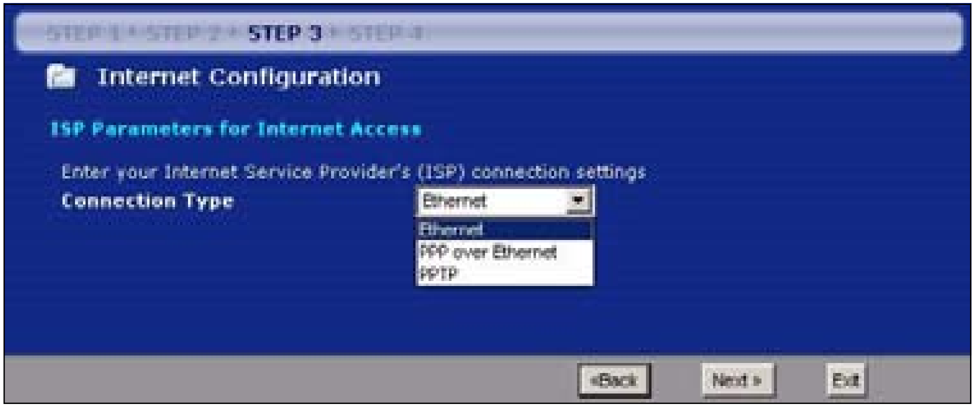
LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens. You need to configure an authentication server to do this.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

3.4 Connection Wizard: STEP 3: Internet Configuration

The P-320W v3 offers three Internet connection types. They are **Ethernet**, **PPP over Ethernet** or **PPTP**. The wizard attempts to detect which WAN connection type you are using. If the wizard does not detect a connection type, you must select one from the drop-down list box. Check with your ISP to make sure you use the correct type.

This wizard screen varies according to the connection type that you select.

Figure 20 Wizard Step 3: ISP Parameters.


STEP 1 • STEP 2 • STEP 3 • STEP 4
Internet Configuration
ISP Parameters for Internet Access
Ethernet
PPP over Ethernet
PPTP
<Back
Next >
Exit

Enter your Internet Service Provider's (ISP) connection settings

Connection Type: Ethernet

The following table describes the labels in this screen,

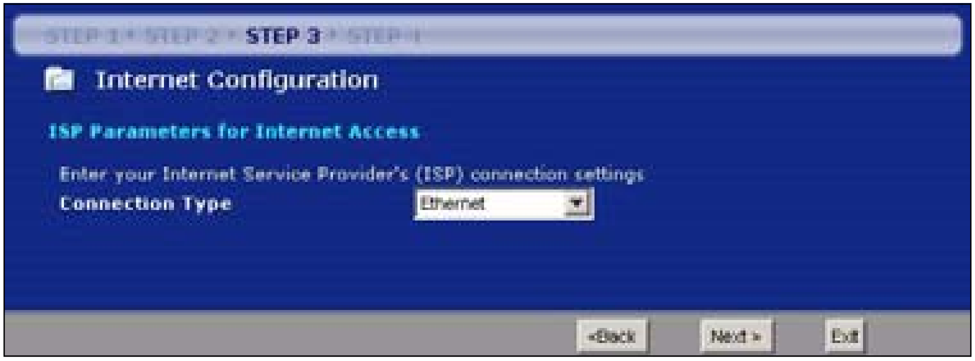
Table 14 Wizard Step 3: ISP Parameters

CONNECTION TYPE	DESCRIPTION
Ethernet	Select the **Ethernet** option when the WAN port is used as a regular Ethernet.
PPPoE	Select the **PPP over Ethernet** option for a dial-up connection. If your ISP gave you an IP address and/or subnet mask, then select **PPTP**.
PPTP	Select the **PPTP** option for a dial-up connection.

3.4.1 Ethernet Connection

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Figure 21 Wizard Step 3: Ethernet Connection


STEP 1 • STEP 2 • STEP 3 • STEP 4
Internet Configuration
ISP Parameters for Internet Access
<Back
Next >
Exit

Enter your Internet Service Provider's (ISP) connection settings

Connection Type: Ethernet

3.4.2 PPPoE Connection

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

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

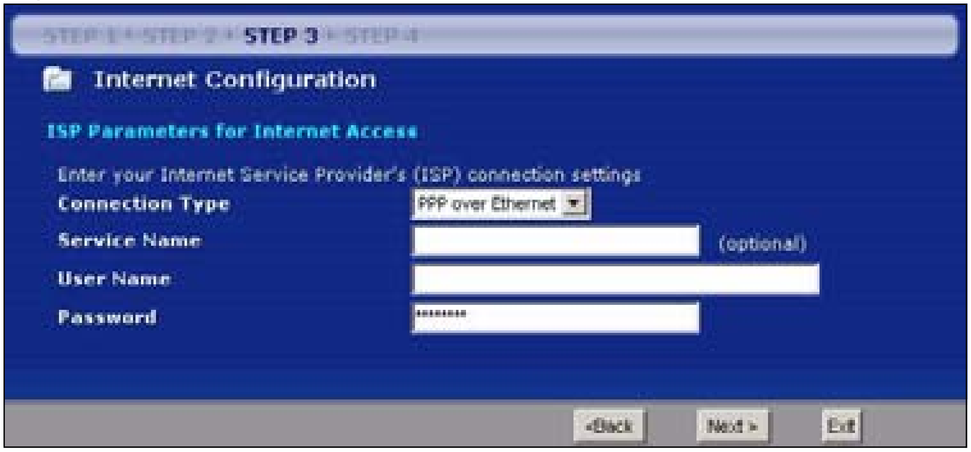
One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/ carrier, as it requires no specific configuration of the broadband modem at the subscriber’s site.

By implementing PPPoE directly on the P-320W v3 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the P-320W v3 does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Refer to the appendix for more information on PPPoE.

Figure 22 Wizard Step 3: PPPoE Connection



Internet Configuration

ISP Parameters for Internet Access

Enter your Internet Service Provider's (ISP) connection settings

Connection Type: PPP over Ethernet

Service Name: (optional)

User Name:

Password: ********

The following table describes the labels in this screen.

Table 15 Wizard Step 3: PPPoE Connection

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Connection Type	Select the **PPP over Ethernet** option for a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Back	Click **Back** to return to the previous screen.

Table 15 Wizard Step 3: PPPoE Connection

LABEL	DESCRIPTION
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

3.4.3 PPTP Connection

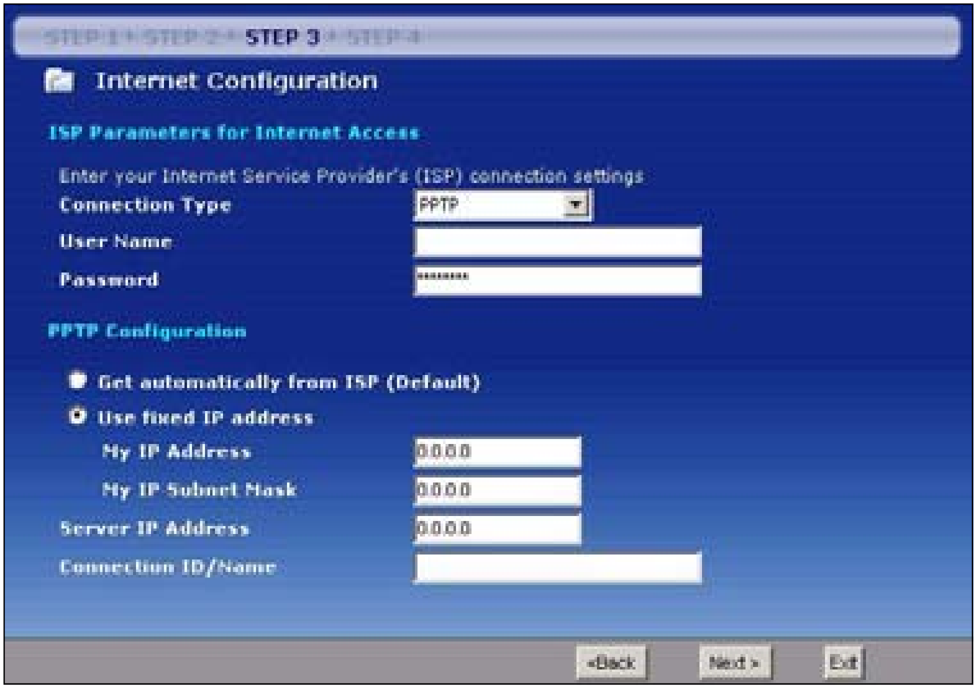
Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

Refer to the appendix for more information on PPTP.

Note: The P-320W v3 supports one PPTP server connection at any given time.

Figure 23 Wizard Step 3: PPTP Connection



Internet Configuration

ISP Parameters for Internet Access

Enter your Internet Service Provider's (ISP) connection settings

Connection Type	PPTP
User Name	
Password	********

PPTP Configuration

○ Get automatically from ISP (Default)

● Use fixed IP address

My IP Address	0.0.0.0
My IP Subnet Mask	0.0.0.0
Server IP Address	0.0.0.0
Connection ID/Name	

The following table describes the fields in this screen

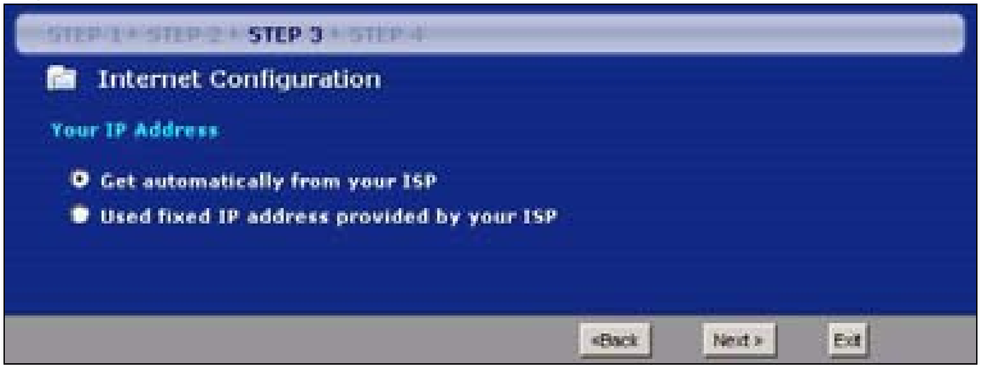
Table 16 Wizard Step 3: PPTP Connection

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select **PPTP** from the drop-down list box. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
PPTP Configuration	
Get automatically from ISP	Select this radio button if your ISP did not assign you a fixed IP address.
Use fixed IP address	Select this radio button, provided by your ISP to give the P-320W v3 a fixed, unique IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

3.4.4 Your IP Address

The following wizard screen allows you to assign a fixed IP address or give the P-320W v3 an automatically assigned IP address depending on your ISP.

Figure 24 Wizard Step 3: Your IP Address


STEP 1 » STEP 2 » STEP 3 » STEP 4
Internet Configuration
Your IP Address
◉ Get automatically from your ISP
○ Used fixed IP address provided by your ISP
<Back
Next >
Exit

The following table describes the labels in this screen

Table 17 Wizard Step 3: Your IP Address

LABEL	DESCRIPTION
Get automatically from your ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection. If you choose this option, skip directly to section Section 3.4.9 on page 51.
Use fixed IP address provided by your ISP	Select this option if you were given IP address and/or DNS server settings by the ISP. The fixed IP address should be in the same subnet as your broadband modem or router.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

3.4.5 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, 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.

Table 18 Private IP Address Ranges

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 have it assigned by 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.

3.4.6 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. 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-320W v3, 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-320W v3 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-320W v3 unless you are instructed to do otherwise.

3.4.7 DNS Server Address Assignment

Use DNS (Domain Name System) 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-320W v3 can get the DNS server addresses in the following ways.

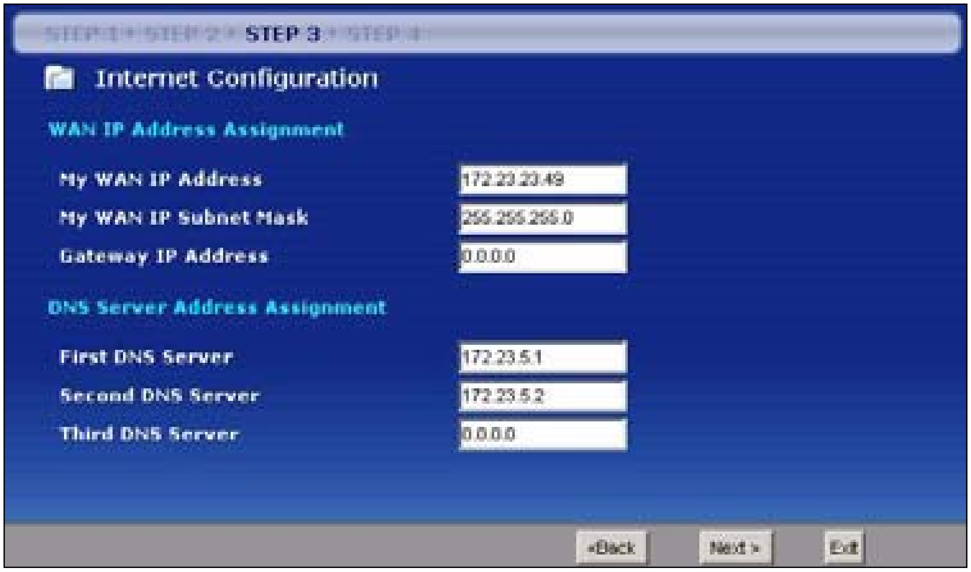
1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **Wizard** and/or **WAN > Internet Connection** screen.

2 If the ISP did not give you DNS server information, leave the **DNS Server** fields set to **0.0.0.0** in the **Wizard** screen and/or set to **From ISP** in the **WAN > Internet Connection** screen for the ISP to dynamically assign the DNS server IP addresses.

3.4.8 WAN IP and DNS Server Address Assignment

The following wizard screen allows you to assign a fixed WAN IP address and DNS server addresses.

Figure 25 Wizard Step 3: WAN IP and DNS Server Addresses



Internet Configuration

WAN IP Address Assignment

My WAN IP Address: 172.23.23.49

My WAN IP Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

DNS Server Address Assignment

First DNS Server: 172.23.5.1

Second DNS Server: 172.23.5.2

Third DNS Server: 0.0.0.0

The following table describes the labels in this screen

Table 19 Wizard Step 3: WAN IP and DNS Server Addresses

LABEL	DESCRIPTION
WAN IP Address Assignment	
My WAN IP Address	Enter your WAN IP address in this field. The WAN IP address should be in the same subnet as your DSL/Cable modem or router.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	Enter the gateway IP address in this field.
System DNS Server Address Assignment (if applicable) DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The P-320W v3 uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server.	
First DNS Server Second DNS Server Third DNS Server	Enter the DNS server's IP address in the fields provided. If you do not configure a system DNS server, you must use IP addresses when configuring DDNS and the time server.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

3.4.9 WAN MAC Address

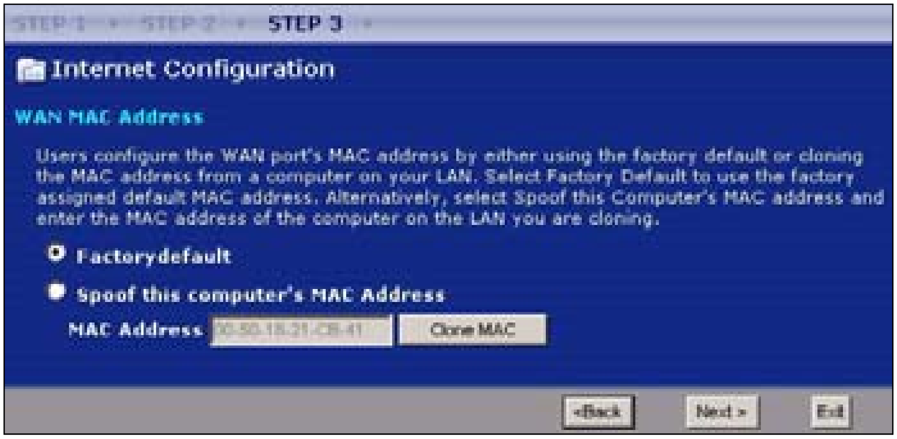
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Table 20 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(P-320W v3 LAN IP)

This screen allows users to configure the WAN port's MAC address by either using the P-320W v3’s MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.

Figure 26 Wizard Step 3: WAN MAC Address



Internet Configuration

WAN MAC Address

Users configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Select Factory Default to use the factory assigned default MAC address. Alternatively, select Spoof this Computer's MAC address and enter the MAC address of the computer on the LAN you are cloning.

● Factorydefault

○ Spoof this computer's MAC Address

MAC Address 00-50-18-21-C8-41

The following table describes the fields in this screen.

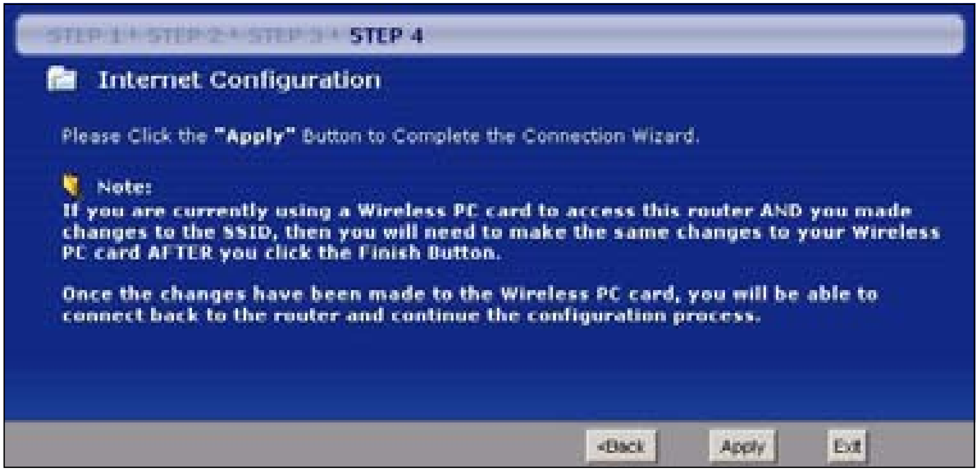
Table 21 Wizard Step 3: WAN MAC Address

LABEL	DESCRIPTION
Factory Default	Select **Factory Default** to use the factory assigned default MAC address.
Spoof the computer’s MAC address	Select this option, enter the IP address of the computer on the LAN whose MAC you are cloning and click **Clone MAC**. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

3.5 Connection Wizard Complete

Click **Apply** to save your configuration.

Figure 27 Connection Wizard Save



Internet Configuration

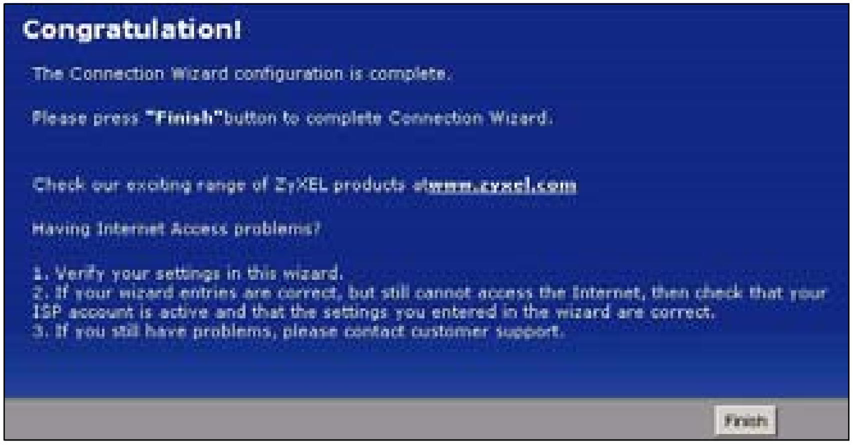
Please Click the **"Apply"** Button to Complete the Connection Wizard.

Note:
If you are currently using a Wireless PC card to access this router AND you made changes to the SSID, then you will need to make the same changes to your Wireless PC card AFTER you click the Finish Button.

Once the changes have been made to the Wireless PC card, you will be able to connect back to the router and continue the configuration process.

Follow the on-screen instructions and click **Finish** to complete the wizard setup.

Figure 28 Connection Wizard Complete



Congratulation!

The Connection Wizard configuration is complete.

Please press **"Finish"**button to complete Connection Wizard.

Check our exciting range of ZyXEL products at**www.zyxel.com**

Having Internet Access problems?

1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.

Well done! You have successfully set up your P-320W v3 to operate on your network and access the Internet.

PART II
Network

4

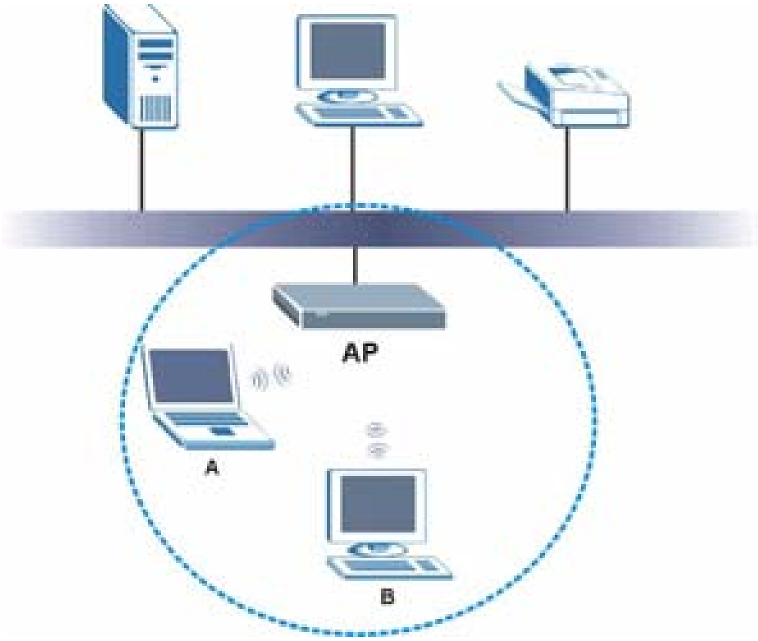
Wireless LAN

4.1 Overview

This chapter discusses how to configure the wireless network settings in your P-320W v3. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 29 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your P-320W v3 is the AP.

Every wireless network must follow these basic guidelines.

- Every wireless client 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 different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every wireless client 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.

4.2 What You Can Do

- Use the **General Wireless** screen (Section 4.4 on page 60) configure your P-320W v3 as a wireless router or access point (AP).
- Use the **MAC Filter** screen (Section 4.5 on page 68) to configure the P-320W v3 to give or deny access to up to 32 devices.
- Use the **WPS** screen (Section 4.6 on page 69) to enable/disable WPS, view or generate a new PIN number and check current WPS status.
- Use the **WPS Station** screen (Section 4.7 on page 70) to add a wireless station using WPS.
- Use the **Wireless LAN Advanced** screen (Section 4.8 on page 70) to configure your P-320W v3's advanced wireless setup.

4.3 What You Need To Know

The following sections provide information that can help you set up your wireless network. It also introduces different types of wireless security you can set up in the wireless network.

4.3.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP 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 devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

4.3.2 MAC Address Filter

Every wireless client 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 wireless client, see the appropriate User's Guide or other documentation.

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

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

4.3.3 User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized 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.

Local user databases also have an additional limitation that is explained in the next section.

[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.

4.3.4 Encryption

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

The types of encryption you can choose depend on the type of user authentication. (See Section 4.3.3 on page 57 for information about this.)

Table 22 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

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

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. 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. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

Note: It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

When you select **WPA2** or **WPA2-PSK** in your P-320W v3, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients 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-320W v3.

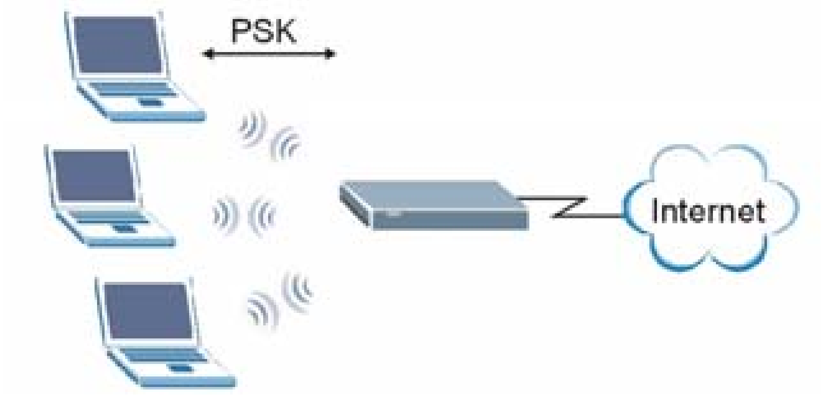
Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

4.3.4.1 WPA-PSK Application Example

A WPA-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and allows it to join the network only if the password matches.
3. The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.
4. The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 30 WPA-PSK Authentication



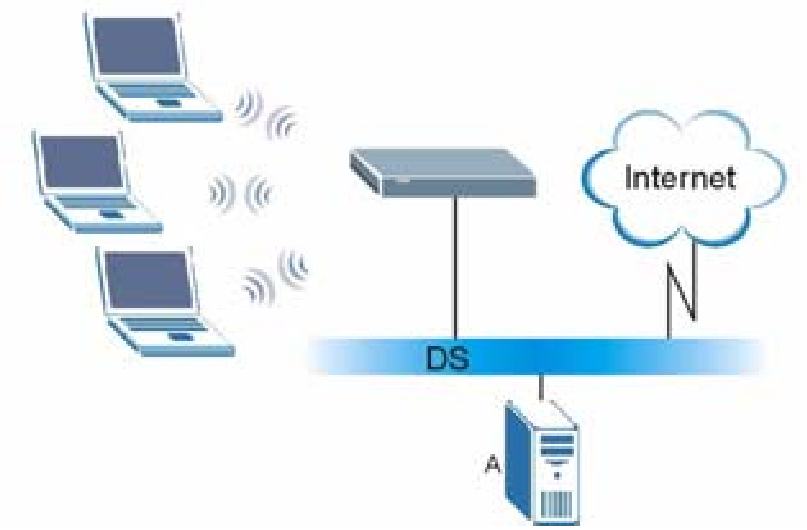
4.3.4.2 WPA with RADIUS Application Example

To set up WPA, you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA 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 31 WPA with RADIUS Application Example



4.3.5 WiFi Protected Setup

WiFi Protected Setup (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. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the Section 6.2 on page 77.

4.4 General Wireless LAN Screen

Use this screen to configure your P-320W v3 as a wireless router or access point (AP).

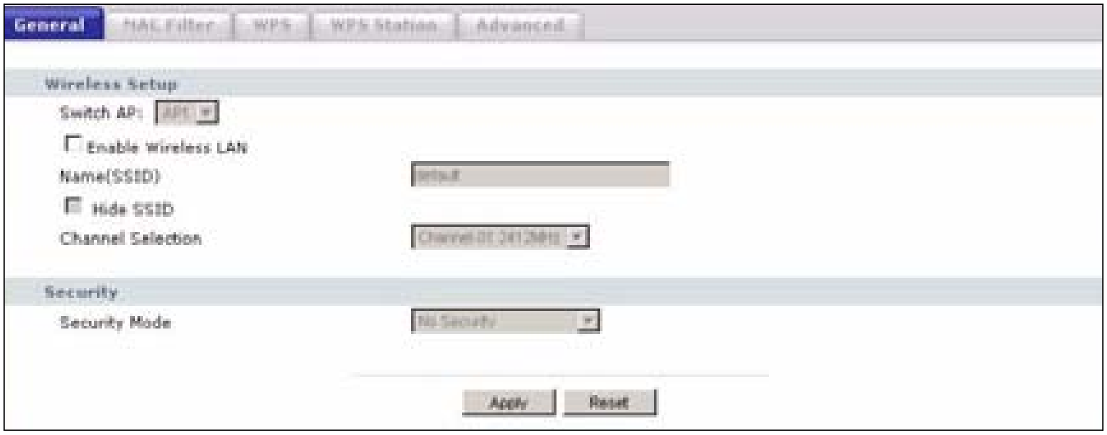
The P-320W v3 can broadcast up to four wireless profiles at the same time. This means that users can connect to the P-320W v3 using different SSIDs.

You can only secure the connection on one SSID profile (**AP1**). Clients connecting to the P-320W v3 using different SSIDs are in the same subnet but cannot communicate with each other.

Note: If you are configuring the P-320W v3 from a computer connected to the wireless LAN and you change the P-320W v3's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the P-320W v3's new settings.

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

Figure 32 Network > Wireless LAN > General



Wireless Setup

Switch AP: AP1

□ Enable Wireless LAN

Name(SSID) default

□ Hide SSID

Channel Selection Channel-01 2412MHz

Security

Security Mode No Security

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

Table 23 Network > Wireless LAN > General

LABEL	DESCRIPTION
Wireless Setup	
Switch AP	Select the AP profile you want to configure. You can enable up to 4 AP profiles with your P-320W v3.
Enable Wireless LAN	Click the check box to activate wireless LAN.
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations 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.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on whether you are using B/G frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels. Note: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.
Security	

Table 23 Network > Wireless LAN > General

LABEL	DESCRIPTION
Security Mode	Select **Static-WEP**, **WPA-PSK**, **WPA**, **802.1x + Dynamic WEP** or **WPA-PSK/WPA2-PSK (Mixed)** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See 4.4.2, 4.4.3, 4.4.4 sections. Or you can select **No Security** to allow any client to associate this network without authentication. Note: If you enable the WPS function, only **No Security** and **WPA-PSK** are available in this option.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

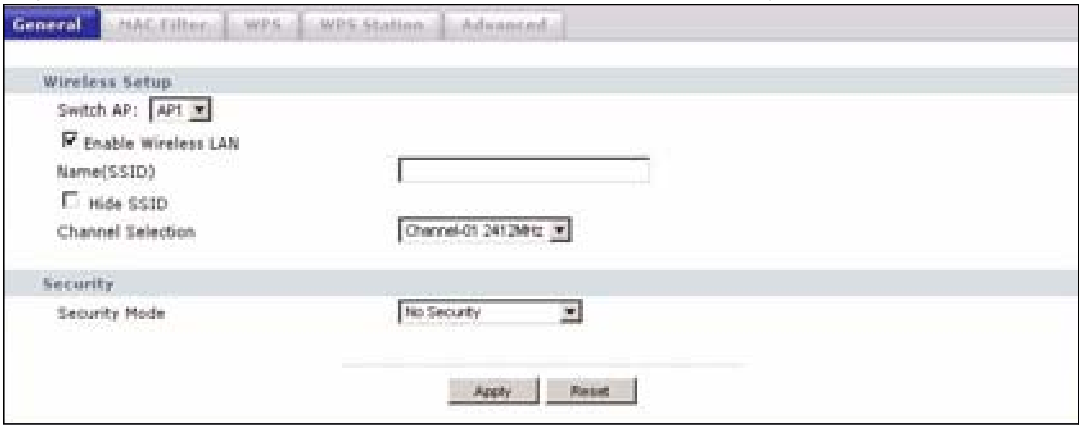
See the rest of this chapter for information on the other labels in this screen.

4.4.1 No Security

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

Note: If you do not enable any wireless security on your P-320W v3, your network is accessible to any wireless networking device that is within range.

Figure 33 Network > Wireless LAN > General: No Security



Wireless Setup

Switch AP: AP1

☑ Enable Wireless LAN

Name(SSID)

☐ Hide SSID

Channel Selection: Channel-01 2412MHz

Security

Security Mode: No Security

The following table describes the labels in this screen.

Table 24 Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

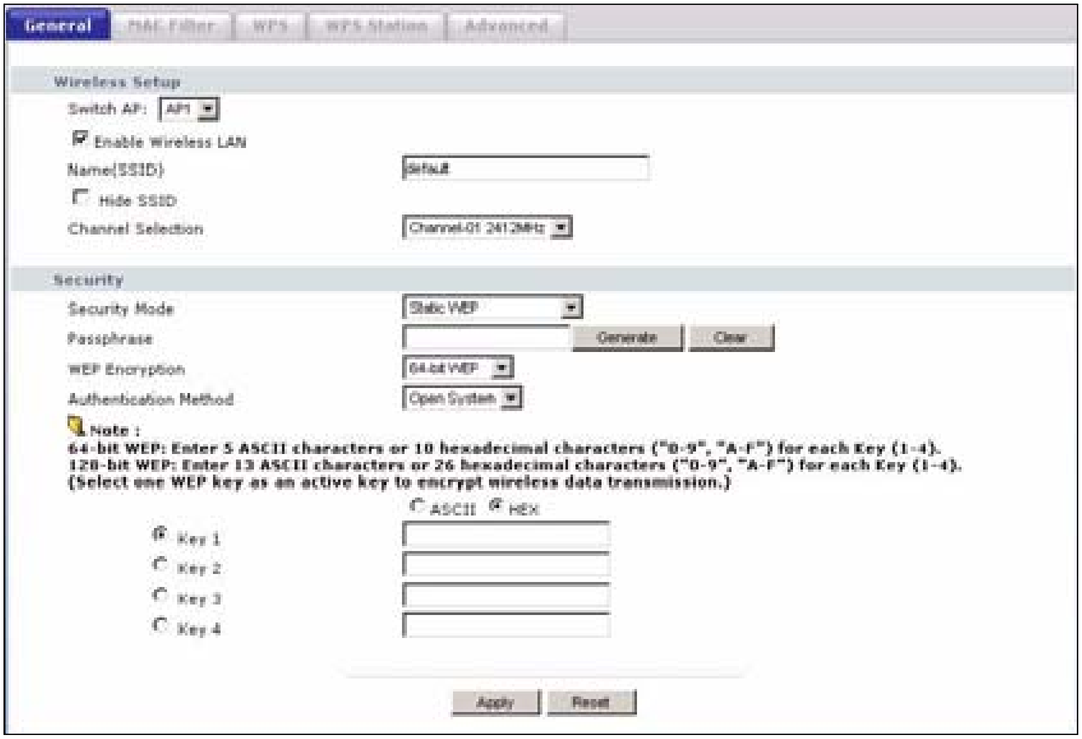
4.4.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your P-320W v3 allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

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

Figure 34 Network > Wireless LAN > General: Static WEP



Wireless Setup

Switch AP: AP1

☑ Enable Wireless LAN

Name(SSID) default

□ Hide SSID

Channel Selection Channel-01 2412MHz

Security

Security Mode Static WEP

Passphrase

WEP Encryption 64-bit WEP

Authentication Method Open System

Note :
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

○ ASCII ● HEX

● Key 1
○ Key 2
○ Key 3
○ Key 4

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

Table 25 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Passphrase	Enter a passphrase (password phrase) of up to 32 printable characters and click **Generate**. The P-320W v3 automatically generates four different WEP keys and displays them in the **Key** fields below.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	This field is activated when you select **64-bit WEP** or **128-bit WEP** in the **WEP Encryption** field. Select **Auto** or **Shared Key** from the drop-down list box.

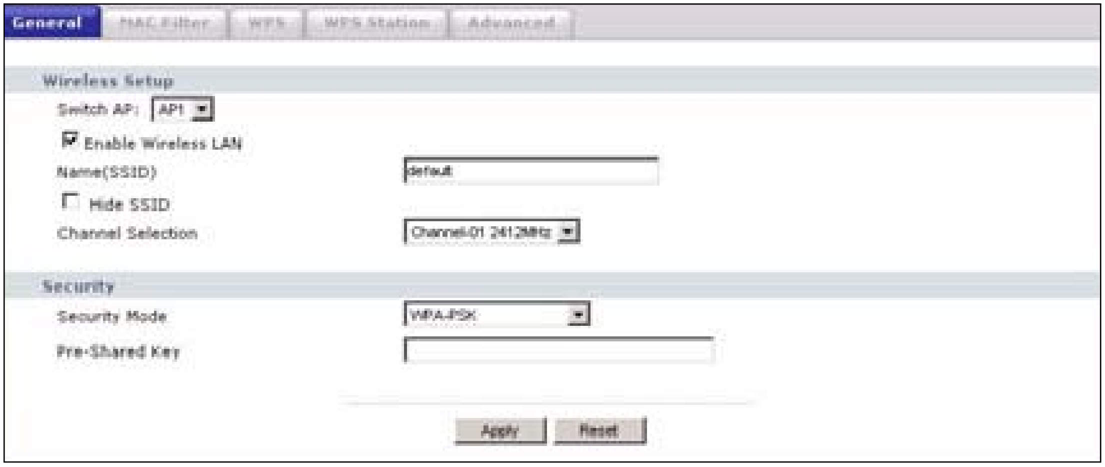
Table 25 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the P-320W v3 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4.3 WPA-PSK

Click **Network** > **Wireless LAN** to display the **General** screen. Select **WPA-PSK** from the **Security Mode** list.

Figure 35 Network > Wireless LAN > General: WPA-PSK



Wireless Setup

Switch AP: AP1

☑ Enable Wireless LAN

Name(SSID) default

☐ Hide SSID

Channel Selection Channel-01 2412MHz

Security

Security Mode WPA-PSK

Pre-Shared Key

The following table describes the labels in this screen.

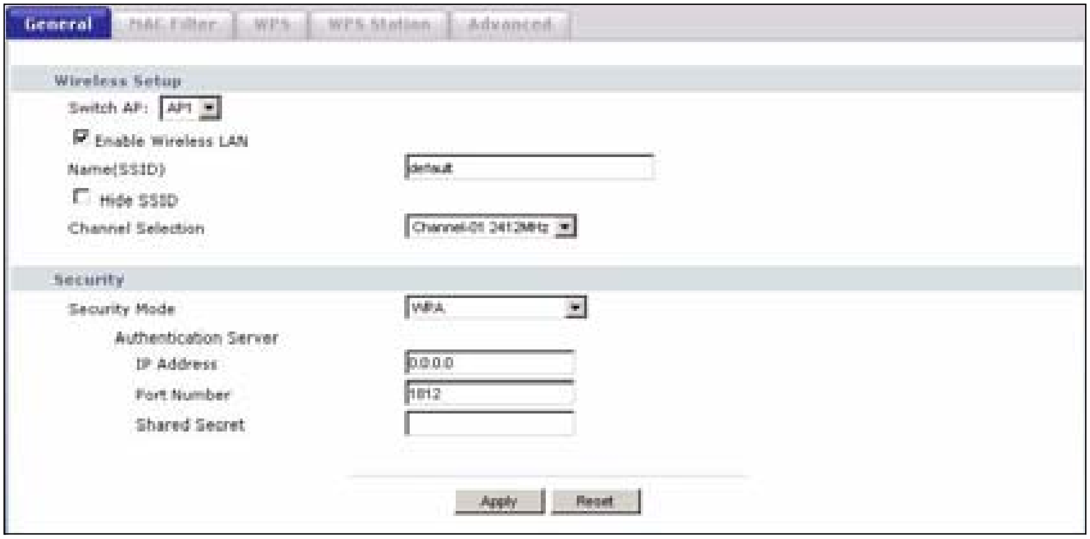
Table 26 Network > Wireless LAN > General: WPA-PSK

LABEL	DESCRIPTION
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-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).
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4.4 WPA

Click **Network** > **Wireless LAN** to display the **General** screen. Select **WPA** from the **Security Mode** list.

Figure 36 Network > Wireless LAN > General: WPA



Wireless Setup

Switch AP: AP1

☑ Enable Wireless LAN

Name(SSID): default

☐ Hide SSID

Channel Selection: Channel-01 2412MHz

Security

Security Mode: WPA

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

The following table describes the labels in this screen.

Table 27 Network > Wireless LAN > General: WPA/WPA2

LABEL	DESCRIPTION
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.

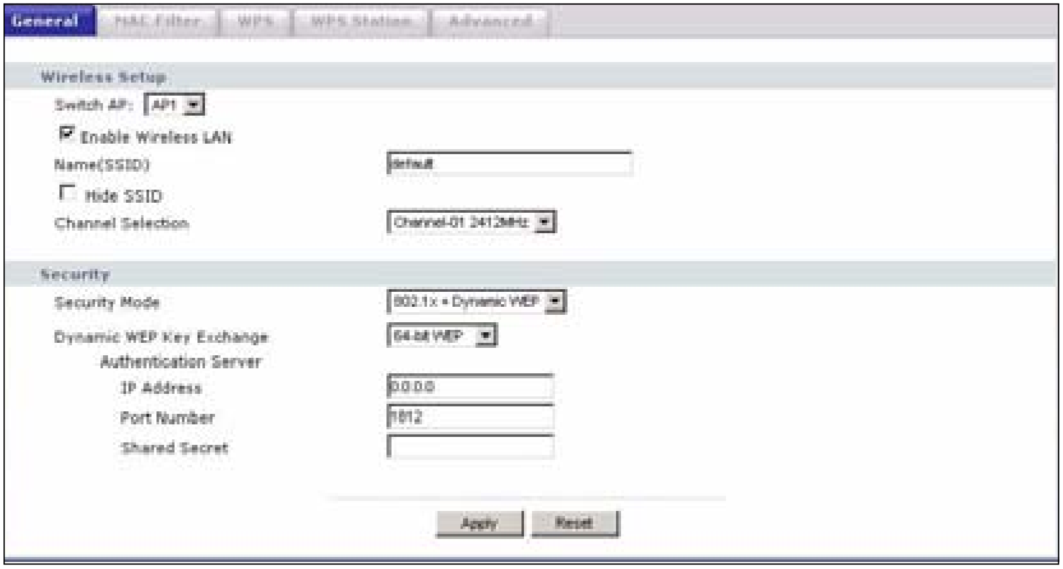
Table 27 Network > Wireless LAN > General: WPA/WPA2

LABEL	DESCRIPTION
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the P-320W v3. The key must be the same on the external authentication server and your P-320W v3. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4.5 802.1x + Dynamic WEP

Click **Network** > **Wireless LAN** to display the **General** screen. Select **802.1x + Dynamic WEP** from the **Security Mode** list.

Figure 37 Network > Wireless LAN > General: 802.1x + Dynamic WEP



Wireless Setup

Switch AP: AP1

☑ Enable Wireless LAN

Name(SSID): default

□ Hide SSID

Channel Selection: Channel-01 2412MHz

Security

Security Mode: 802.1x + Dynamic WEP

Dynamic WEP Key Exchange: 64-bit WEP

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

The following table describes the labels in this screen..

Table 28 Network > Wireless LAN > General: 802.1x + Dynamic WEP

LABEL	DESCRIPTION
Dynamic WEP Key Exchange	The WEP keys are used to encrypt data. Both the P-320W v3 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Security	

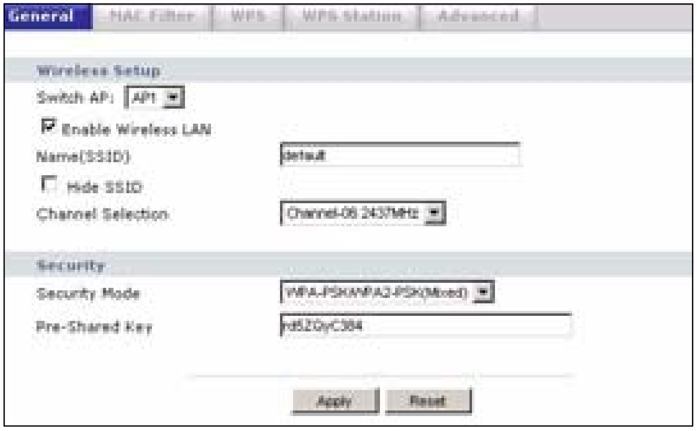
Table 28 Network > Wireless LAN > General: 802.1x + Dynamic WEP

LABEL	DESCRIPTION
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. 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-320W v3. The key must be the same on the external authentication server and your P-320W v3. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4.6 WPA-PSK/WPA2-PSK (Mixed)

Click **Network** > **Wireless LAN** to display the **General** screen. Select **WPA-PSK/WPA2-PSK (Mixed)** from the **Security Mode** list.

Figure 38 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK (Mixed)



Wireless Setup

Switch AP: AP1

☑ Enable Wireless LAN

Name(SSID): default

☐ Hide SSID

Channel Selection: Channel-06 2437MHz

Security

Security Mode: WPA-PSK/WPA2-PSK(Mixed)

Pre-Shared Key: nd5ZQyC384

The following table describes the labels in this screen.

Table 29 Network > Wireless LAN > General: WPA-PSK

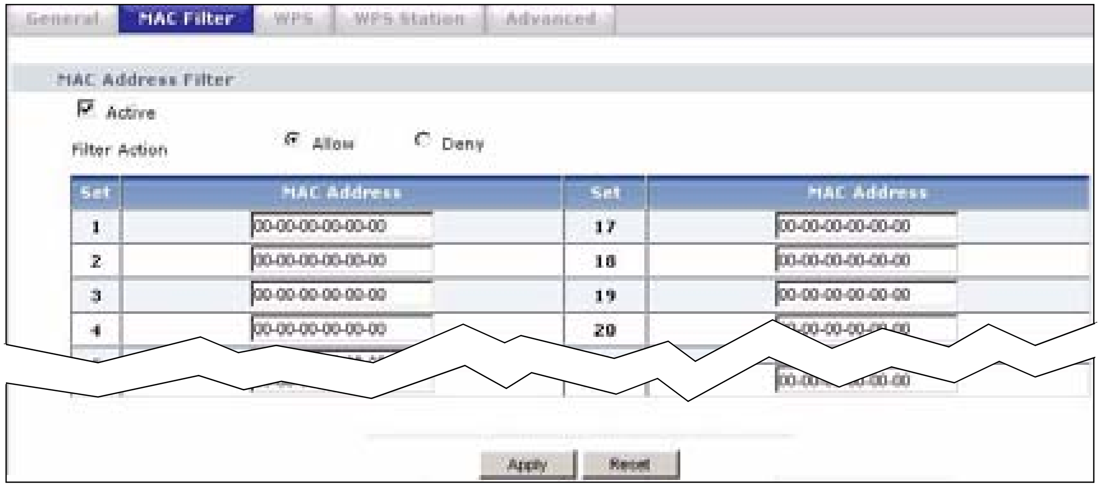
LABEL	DESCRIPTION
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.5 MAC Filter

The MAC filter screen allows you to configure the P-320W v3 to give exclusive access to up to 32 devices (Allow) or exclude up to 32 devices from accessing the P-320W v3 (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 address of the devices to configure this screen.

To change your P-320W v3's MAC filter settings, click **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 39 Network > Wireless LAN > MAC Filter



MAC Address Filter

☑ Active

Filter Action ● Allow ○ Deny

Set	MAC Address	Set	MAC Address
1	00-00-00-00-00-00	17	00-00-00-00-00-00
2	00-00-00-00-00-00	18	00-00-00-00-00-00
3	00-00-00-00-00-00	19	00-00-00-00-00-00
4	00-00-00-00-00-00	20	00-00-00-00-00-00

The following table describes the labels in this menu.

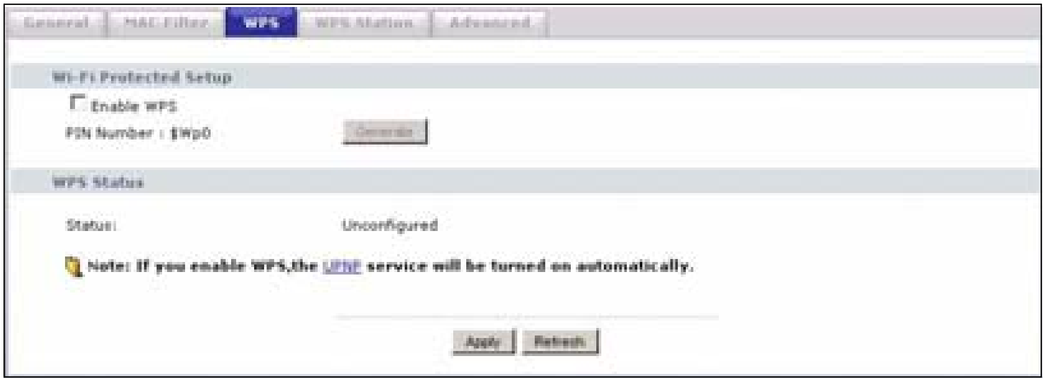
Table 30 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny** to block access to the P-320W v3, MAC addresses not listed will be allowed to access the P-320W v3 Select **Allow** to permit access to the P-320W v3, MAC addresses not listed will be denied access to the P-320W v3.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the P-320W v3 in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.6 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Network** > **Wireless LAN** > **WPS** tab.

Figure 40 WPS



□ Enable WPS

PIN Number : $Wp0

Status: Unconfigured

Note: If you enable WPS,the UPNP service will be turned on automatically.

The following table describes the labels in this screen.

Table 31 WPS

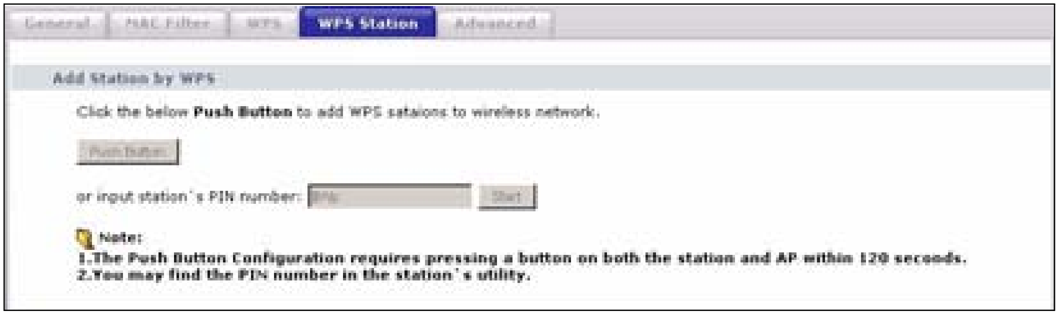
LABEL	DESCRIPTION
Wi-Fi Protected Setup	
Enable	Select this to enable the WPS feature.
PIN Number	This displays a PIN number last time system generated. Click **Generate** to generate a new PIN number.
WPS Status	
Status	This displays **Configured** when the P-320W v3 has connected to a wireless network 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-320W v3 or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release_Configuration	This button is available when the WPS status is Configured. Click this button to remove all configured wireless and wireless security settings for WPS connections on the P-320W v3.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Refresh	Click **Refresh** to get this screen information afresh.

4.7 WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Network** > **Wireless LAN** > **WPS Station** tab.

Note: Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

Figure 41 WPS Station



Add Station by WPS

Click the below **Push Button** to add WPS sataions to wireless network.

or input station's PIN number:

Note:
1.The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2.You may find the PIN number in the station's utility.

The following table describes the labels in this screen.

Table 32 WPS Station

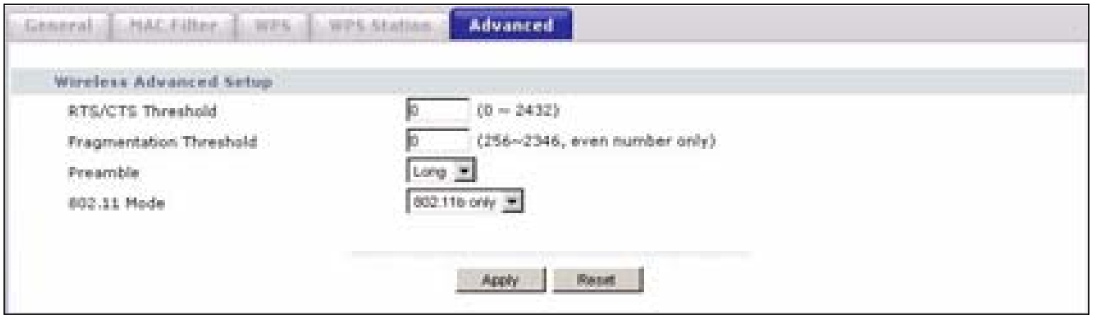
LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. See Section 6.2.1 on page 78. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. See Section 6.2.2 on page 79. Type the same PIN number generated in the wireless station's utility. Then click **Start** to associate to each other and perform the wireless security information synchronization.

4.8 Wireless LAN Advanced Screen

Use this screen to configure your P-320W v3's advanced wireless setup.

Click **Network** > **Wireless LAN** > **Advanced**. The screen appears as shown.

Figure 42 Network > Wireless LAN > Advanced



Wireless Advanced Setup

RTS/CTS Threshold 0 (0 ~ 2432)

Fragmentation Threshold 0 (256~2346, even number only)

Preamble Long

802.11 Mode 802.11b only

The following table describes the labels in this screen.

Table 33 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. If the RTS/CTS value is greater than the **Fragmentation Threshold** value, then the RTS/CTS handshake will never occur as data frames will be fragmented before they reach RTS/CTS size. Enter a value between 0 and 2432.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
Preamble	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. Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks. Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications.
802.11 Mode	Select **802.11b** to allow only IEEE 802.11b compliant WLAN devices to associate with the P-320W v3. Select **802.11g** to allow only IEEE 802.11g compliant WLAN devices to associate with the P-320W v3. Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the P-320W v3. The transmission rate of your P-320W v3 might be reduced.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

5

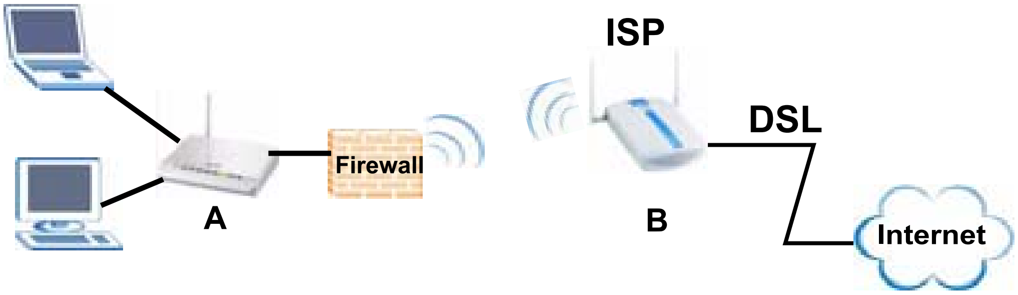
Wireless Client Mode

5.1 Overview

Your P-320W v3 can act as a wireless client. In wireless client mode, it can connect to an existing network via an access point.

In the example below, one P-320W v3 (**A**) is configured as a wireless client and another is used as an access point (**B**). The wireless client has two clients that need to connect to the Internet. The P-320W v3 wirelessly connects to the available access point (**B**).

Figure 43 Wireless Client Mode



After the P-320W v3 and the access point connect, the P-320W v3 acquires its WAN IP address from the access point. The clients of the P-320W v3 can now surf the Internet.

5.2 What You Can Do

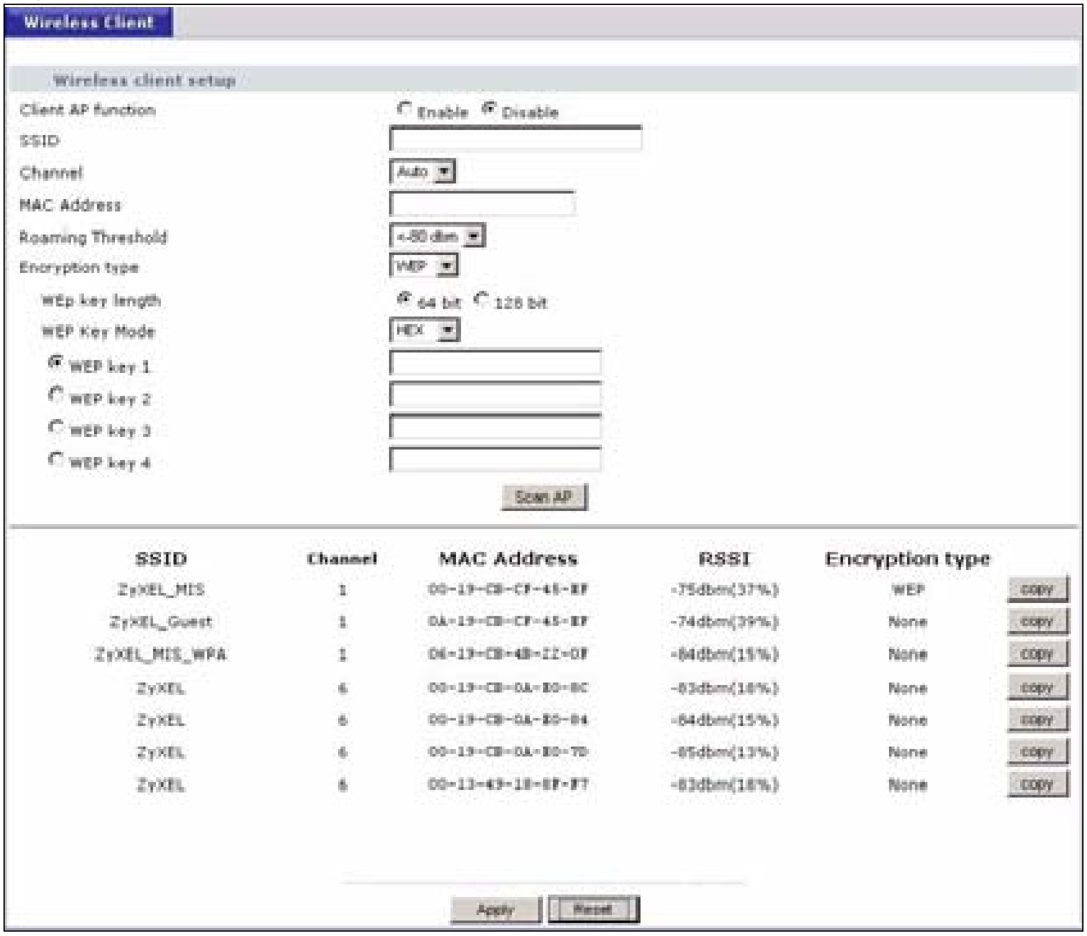
Use the **Wireless Client Mode** screen (Section 5.3 on page 74) to use your P-320W v3 as a wireless client and connect to an existing AP.

5.3 Wireless Client Mode Screen

Use this screen to use your P-320W v3 as a wireless client and connect to an existing AP.

Click **Wireless Client Mode** to open the following screen.

Figure 44 Wireless Client Mode



Wireless Client

Wireless client setup

Client AP function ○ Enable ● Disable

SSID

Channel Auto

MAC Address

Roaming Threshold <-80 dbm

Encryption type WEP

WEp key length ● 64 bit ○ 128 bit

WEP Key Mode HEX

● WEP key 1

○ WEP key 2

○ WEP key 3

○ WEP key 4

Scan AP

SSID	Channel	MAC Address	RSSI	Encryption type	
ZyXEL_MIS	1	00-19-CB-CF-45-BF	-75dbm(37%)	WEP	copy
ZyXEL_Guest	1	0A-19-CB-CF-45-BF	-74dbm(39%)	None	copy
ZyXEL_MIS_WPA	1	06-19-CB-4B-22-0F	-84dbm(15%)	None	copy
ZyXEL	6	00-19-CB-0A-B0-8C	-83dbm(18%)	None	copy
ZyXEL	6	00-19-CB-0A-B0-84	-84dbm(15%)	None	copy
ZyXEL	6	00-19-CB-0A-B0-7D	-85dbm(13%)	None	copy
ZyXEL	6	00-13-49-18-8F-F7	-83dbm(18%)	None	copy

The following table describes the labels in this screen.

Table 34 Summary: DHCP Table

LABEL	DESCRIPTION
Client AP Function	Select **Enable** to use your P-320W v3 as a wireless client and connect to an existing AP. Select **Disable** to use your P-320W v3 as a router or an access point if the network to which you are connecting already has a router. Your P-320W v3 is configured as a router/access point by default.
SSID	Enter the name of the access point to which you are connecting. You can also copy the SSID of the access point to which you want to connect by clicking **copy** in the list of access points that appears when you click **Scan AP**.
Channel	Select the channel of the access point to which you are connecting. Note: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.
MAC Address	Enter the MAC address of the access point to which you are connecting.
Roaming Threshold	Select the signal strength threshold between the wireless client and the access point. When the signal strength between the two devices goes below the value you set in this field, the wireless client searches for and connects to another access point within the roaming threshold.
Encryption type	Select **WEP** if you want to secure the wireless connection.Otherwise, select **No Security**.
WEP key length	This field appears when you select **WEP** as the security type. Select either **64 bit** or **128 bit** as the key length for your WEP key.
WEP Key Mode	This field appears when you select **WEP** as the security type. Select either **HEX** or **ASCII** as the key length for your WEP key.
WEP Key 1 to 4	This field appears when you select **WEP** as the security type. Select which WEP key you want to use for your wireless connection. By default, the P-320W v3 uses **WEP key 1**.
Scan AP	Click this to view a list of available access points to which you can connect.
SSID	This is the SSID of the access point.
Channel	This is the channel of the access point.
MAC Address	This is the MAC Address of the access point.
RSSI	This is the RSSI or signal strength of the access point.
Encryption type	This is the encryption type of the access point.
copy	Click this to copy the SSID of the access point to the **SSID** field.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to reload the previous configuration for this screen.

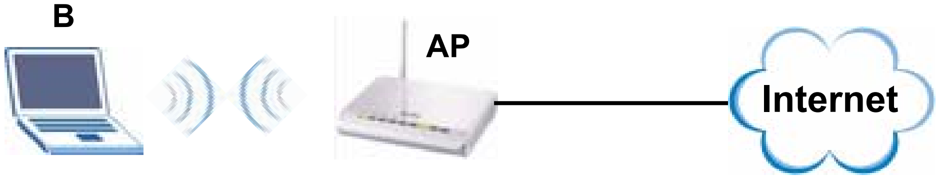
6

Wireless Tutorial

6.1 How to Connect to the Internet from an AP

This section gives you an example of how to set up an access point (**AP**) and wireless client (a notebook (**B**), in this example) for wireless communication. **B** can access the Internet through the AP wirelessly.

Figure 45 Wireless AP Connection to the Internet



6.2 Configure Wireless Security Using WPS on both your P-320W v3 and Wireless Client

This section gives you an example of how to set up wireless network using WPS. This example uses the P-320W v3 as the AP and NWD210N as the wireless client which connects to a notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 6.2.1 on page 78.This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the P-320W v3's interface. See Section 6.2.2 on page 79. This is the more secure method, since one device can authenticate the other.

6.2.1 Push Button Configuration (PBC)

1 Make sure that your P-320W v3 is turned on and that it is within range of your computer.

2 Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.

3 In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)

4 Log into P-320W v3's web configurator and press the **Push Button** button in the **Network** > **Wireless Client** > **WPS Station** screen.

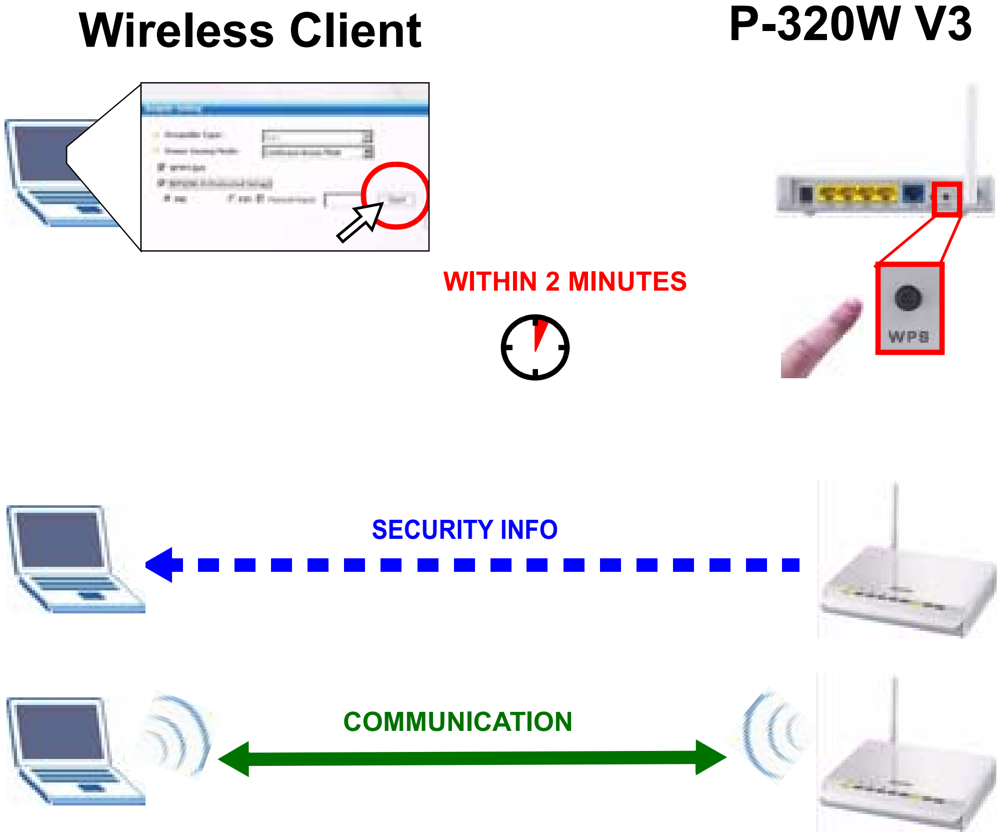
Note: Your P-320W v3 has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The P-320W v3 sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the P-320W v3 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both P-320W v3 and wireless client (the NWD210N in this example).

Figure 46 Example WPS Process: PBC Method



6.2.2 PIN Configuration

When you use the PIN configuration method, you need to use both P-320W v3's configuration interface and the client's utilities.

1 Launch your wireless client's configuration utility. go to the WPS settings and select the PIN method to get a PIN number.

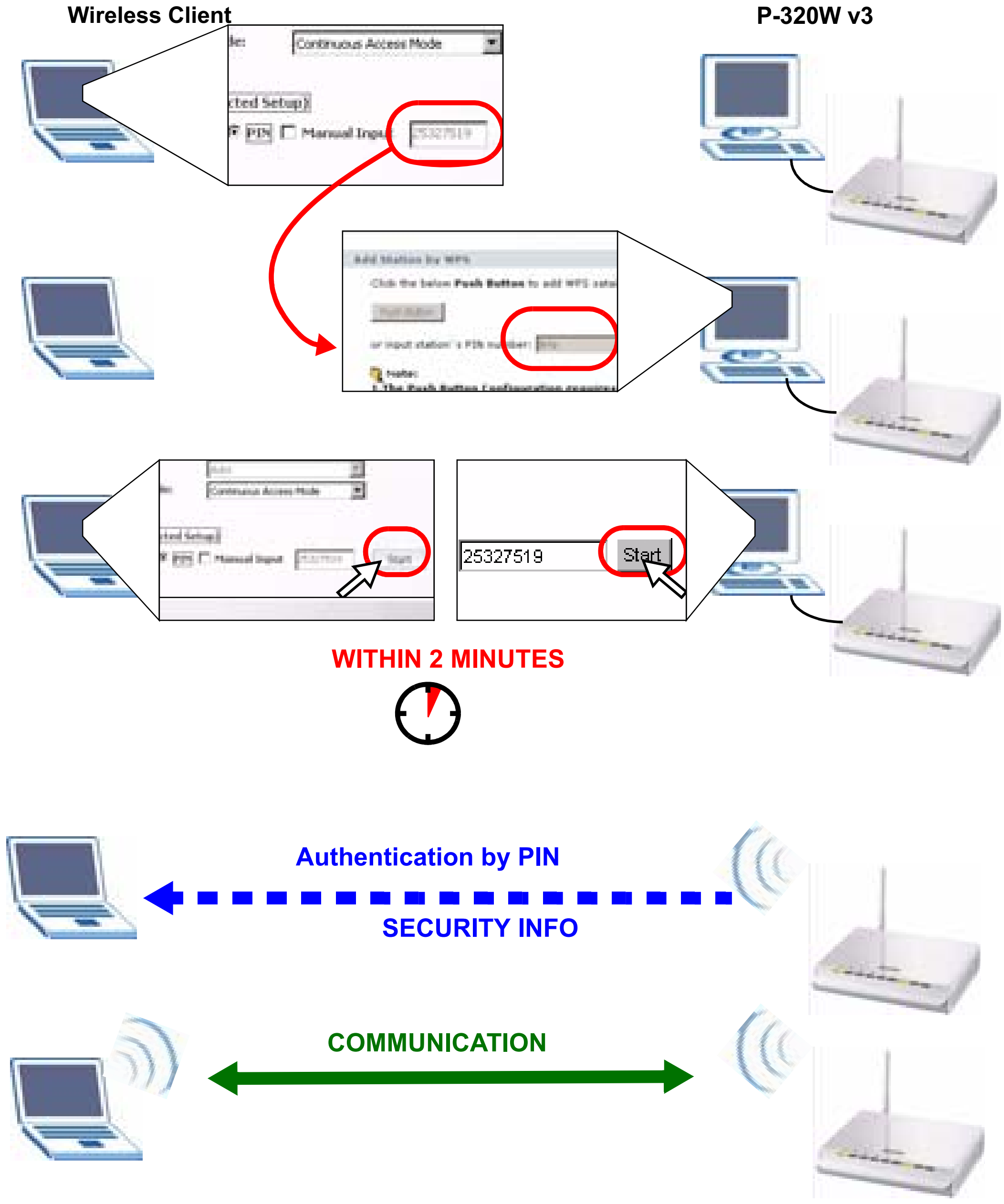
2 Enter the PIN number to the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen on the P-320W v3.

3 Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the P-320W v3's **WPS Station** screen within two minutes.

The P-320W v3 authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the P-320W v3 securely.

The following figure shows you the example to set up wireless network and security on P-320W v3 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 47 Example WPS Process: PIN Method



6.3 Enable and Configure Wireless Security without WPS on your P-320W v3

This example shows you how to configure wireless security settings with the following parameters on your P-320W v3.

SSID	SSID_Example3
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your P-320W v3.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the web configurator through your LAN connection (see Section 2.2 on page 25).

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

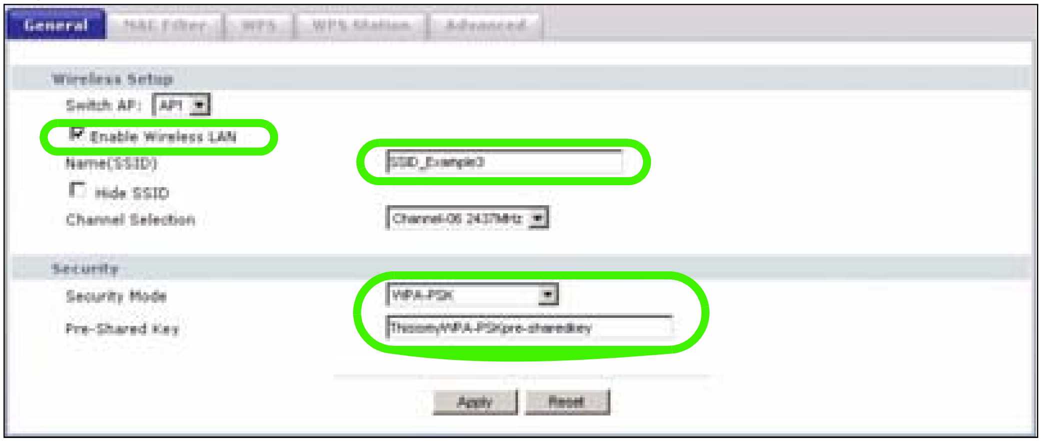
2 Make sure the **Enable Wireless LAN** check box is selected.

3 Enter **SSID_Example3** as the SSID and select a channel.

Note: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

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

Figure 48 Network > Wireless LAN > General



Wireless Setup

Switch AP: AP1

☑ Enable Wireless LAN

Name(SSID) SSID_Example3

□ Hide SSID

Channel Selection Channel-06 2437MHz

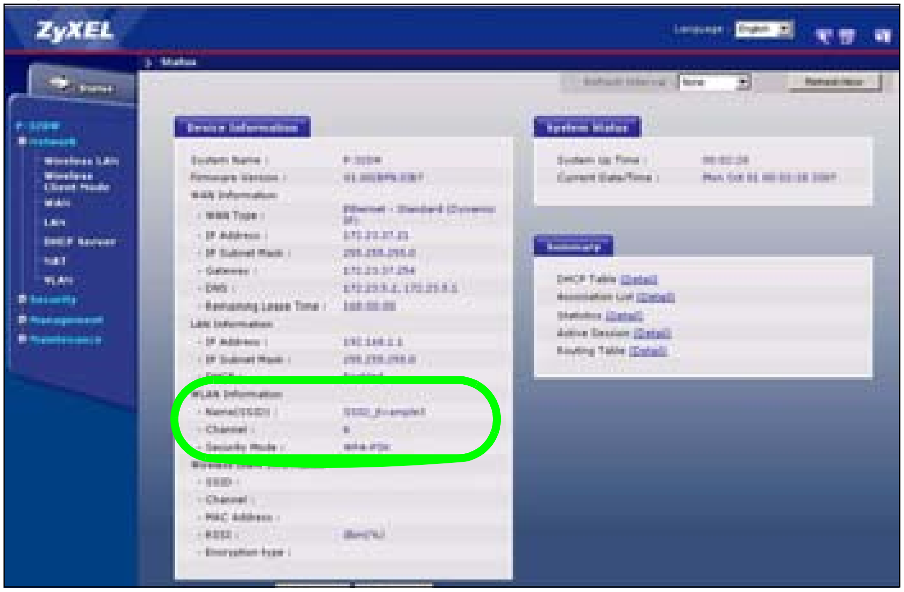
Security

Security Mode WPA-PSK

Pre-Shared Key ThisismyWPA-PSKpre-sharedkey

5 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information**.

Figure 49 Status: AP Mode



Device Information

System Name :	P-320W
Firmware Version :	[illegible]
WAN Information	
- WAN Type :	Ethernet - Standard (Dynamic IP)
- IP Address :	172.23.37.21
- IP Subnet Mask :	255.255.255.0
- Gateway :	172.23.37.254
- DNS :	172.23.5.2, 172.23.5.1
- Remaining Lease Time :	168:00:00
LAN Information	
- IP Address :	192.168.1.1
- IP Subnet Mask :	255.255.255.0
- DHCP :	Enabled
WLAN Information	
- Name(SSID) :	SSID_Example3
- Channel :	6
- Security Mode :	WPA-PSK
Wireless Client Information	
- SSID :	
- Channel :	
- MAC Address :	
- RSSI :	dBm(%)
- Encryption type :	

System Status

System Up Time :	00:02:16
Current Date/Time :	Mon Oct 01 00:02:16 2007

Summary

DHCP Table (Detail)
Association List (Detail)
Statistics (Detail)
Active Session (Detail)
Routing Table (Detail)

6.4 Configure Your Notebook

Note: We use the ZyXEL M-302 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

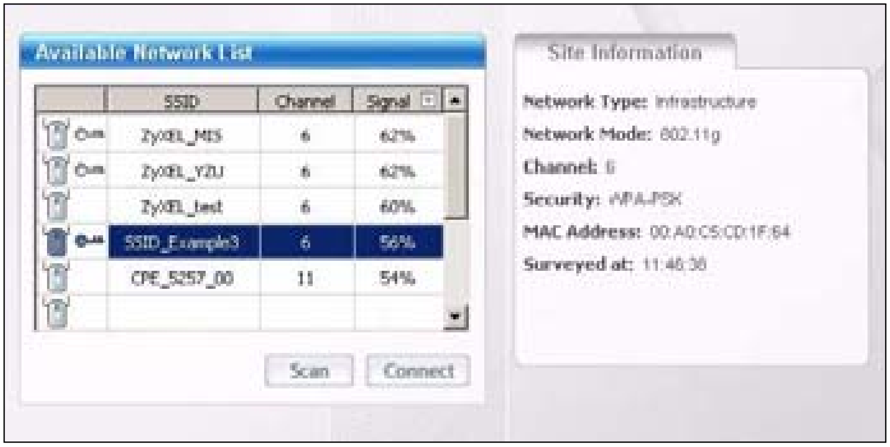
1 The P-320W v3 supports IEEE 802.11b and IEEE 802.11g wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.

3 After you've installed the utility, open it. If you cannot see your utility's icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.

4 Select SSID_Example3 and click **Connect**.

Figure 50 Connecting a Wireless Client to a Wireless Network t



Available Network List

SSID	Channel	Signal
ZyXEL_MIS	6	62%
ZyXEL_YZU	6	62%
ZyXEL_test	6	60%
SSID_Example3	6	56%
CPE_5257_00	11	54%

Site Information

Network Type: Infrastructure

Network Mode: 802.11g

Channel: 6

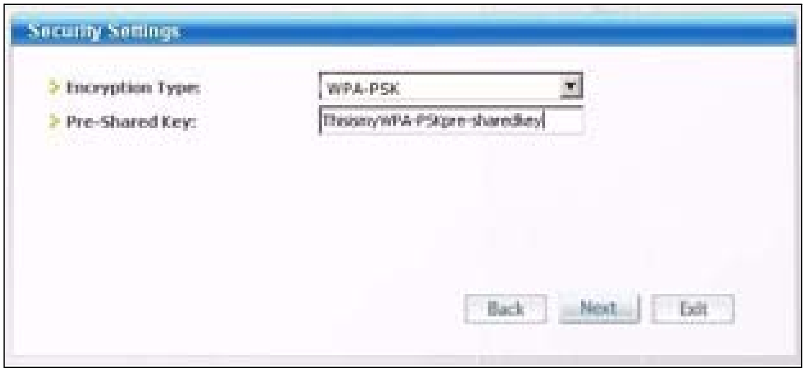
Security: WPA-PSK

MAC Address: 00:A0:C5:CD:1F:64

Surveyed at: 11:46:38

5 Select WPA-PSK and type the security key in the following screen. Click **Next**.

Figure 51 Security Settings



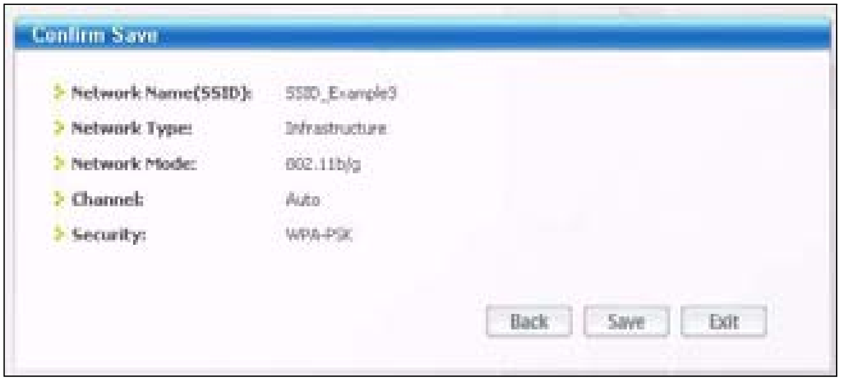
Security Settings

Encryption Type: WPA-PSK

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 52 Confirm Save



Confirm Save

Network Name(SSID): SSID_Example3

Network Type: Infrastructure

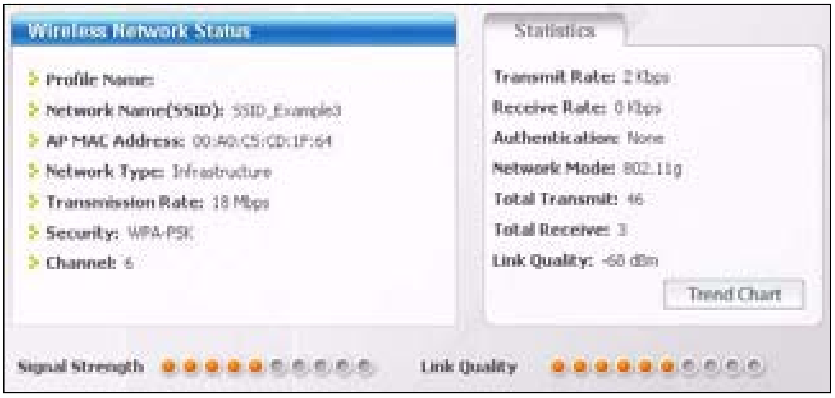
Network Mode: 802.11b/g

Channel: Auto

Security: WPA-PSK

7 Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see the Troubleshooting section of this User's Guide.

Figure 53 Link Status



Wireless Network Status

- Profile Name:
- Network Name(SSID): SSID_Example3
- AP MAC Address: 00:A0:C5:CD:1F:64
- Network Type: Infrastructure
- Transmission Rate: 18 Mbps
- Security: WPA-PSK
- Channel: 6

Statistics

Transmit Rate: 2 Kbps

Receive Rate: 0 Kbps

Authentication: None

Network Mode: 802.11g

Total Transmit: 46

Total Receive: 3

Link Quality: -60 dBm

8 If your connection is successful, 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.

7

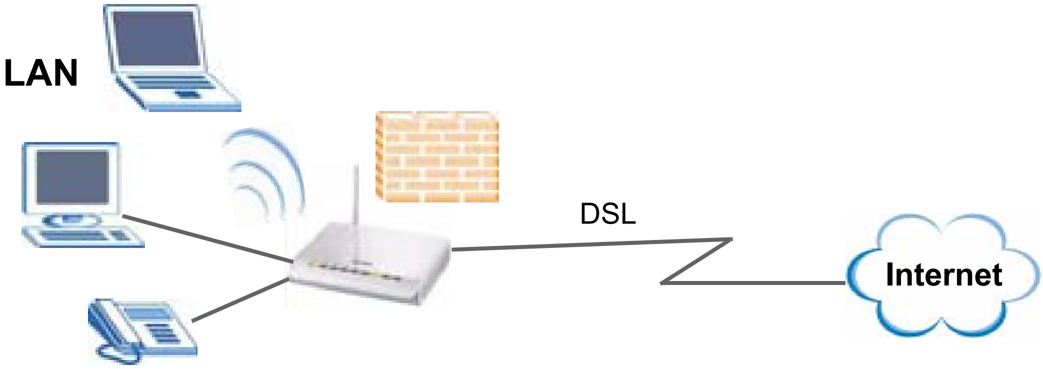
LAN

7.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screen can help you identify your local network.

Figure 54 Local Area Network



7.2 What You Can Do

Use the **LAN IP** screen (Section 7.4 on page 87) to change your basic LAN settings.

7.3 What You Need to Know

The following sections provide information that you may need when configuring the **LAN IP** screen.

7.3.1 IP Pool Setup

The P-320W v3 is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the P-320W v3 itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

7.3.2 System DNS Servers

Refer to Section 3.4.6 on page 48 in the **Connection Wizard** chapter.

7.3.3 LAN TCP/IP

The P-320W v3 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

7.3.4 Factory LAN Defaults

The LAN parameters of the P-320W v3 are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

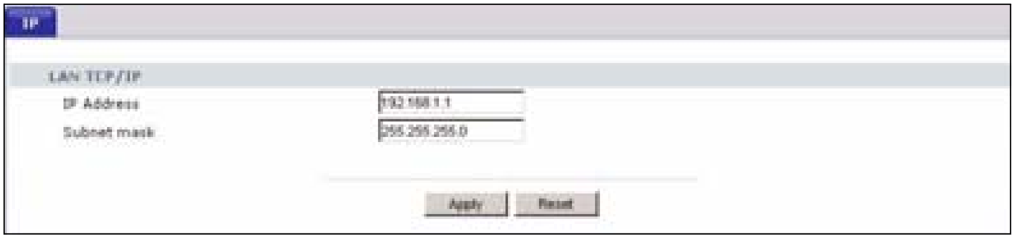
7.3.5 IP Address and Subnet Mask

Refer to the IP address and subnet mask section in the **Connection Wizard** chapter for this information.

7.4 LAN IP Screen

Use this screen to change your basic LAN settings. Click **Network** > **LAN**.

Figure 55 Network > LAN > IP



IP Address 192.168.1.1

Subnet mask 255.255.255.0

The following table describes the labels in this screen.

Table 35 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your P-320W v3 in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your P-320W v3 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the P-320W v3.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

8

DHCP Server

8.1 Overview

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-320W v3's DHCP server(s) or disable it.

When configured as a server, the P-320W v3 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN or Guest WLAN, or else the computer must be manually configured.

8.2 What You Can Do

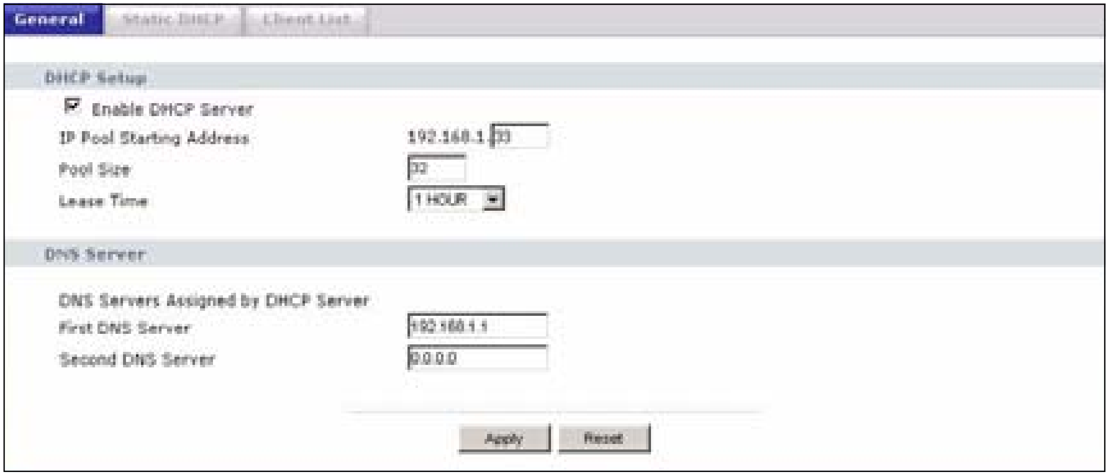
- Use the **DHCP Server General** screen (Section 8.3 on page 89) to enable and configure your DHCP server.
- Use the **Static DHCP** screen (Section 8.4 on page 91) to change your P-320W v3's Static DHCP settings.
- Use the **Client List** screen (Section 8.5 on page 91) to view a list of current DHCP client information.

8.3 DHCP Server General Screen

Use this screen to enable and configure your DHCP server.

Click **Network** > **DHCP Server**. The following screen displays.

Figure 56 Network > DHCP Server > General



DHCP Setup

☑ Enable DHCP Server

IP Pool Starting Address 192.168.1.33

Pool Size 32

Lease Time 1 HOUR

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server 192.168.1.1

Second DNS Server 0.0.0.0

The following table describes the labels in this screen.

Table 36 Network > DHCP Server > General

LABEL	DESCRIPTION
Enable DHCP Server	Leave the check box selected unless your ISP instructs you to do otherwise. Clear it to disable the P-320W v3 acting as a DHCP server. When configured as a server, the P-320W v3 provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured.
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.
Lease Time	Select how long a computer can lease its IP address in the network. You can select from **1 HOUR** (default) to as long as **Forever** (unlimited time).
DNS Servers The P-320W v3 passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The P-320W v3 only passes this information to the LAN DHCP clients when you select the Enable DHCP Server check box. When you clear the Enable DHCP Server check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.	
First DNS Server Second DNS Server	Enter the IP address(es) of the DNS server(s). If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

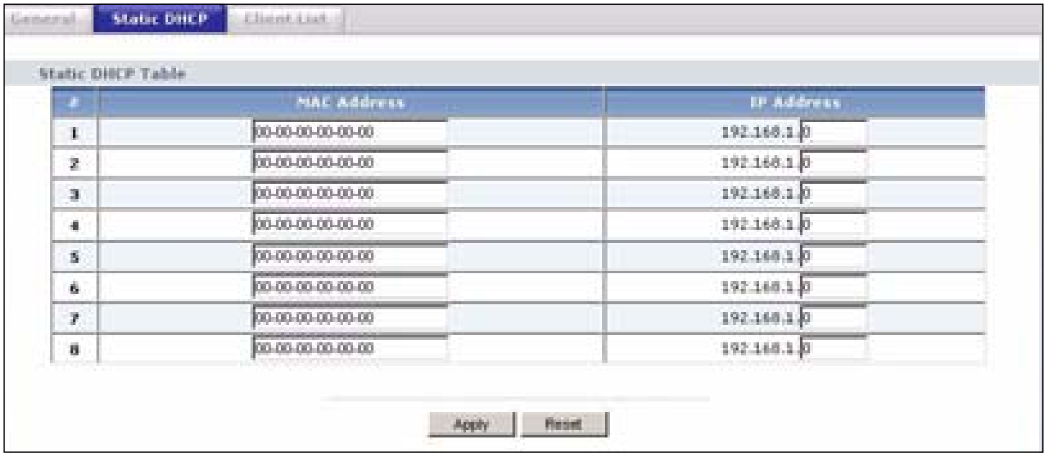
8.4 Static DHCP Screen

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

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

To change your P-320W v3's Static DHCP settings, click the DHCP Server link under Network and the Static DHCP tab. The following screen displays.

Figure 57 Network > DHCP Server > Advanced



Static DHCP Table

#	MAC Address	IP Address
1	00-00-00-00-00-00	192.168.1. 0
2	00-00-00-00-00-00	192.168.1. 0
3	00-00-00-00-00-00	192.168.1. 0
4	00-00-00-00-00-00	192.168.1. 0
5	00-00-00-00-00-00	192.168.1. 0
6	00-00-00-00-00-00	192.168.1. 0
7	00-00-00-00-00-00	192.168.1. 0
8	00-00-00-00-00-00	192.168.1. 0

The following table describes the labels in this screen.

Table 37 Network > DHCP Server > Advanced

LABEL	DESCRIPTION
#	This is the index number of the static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address of a computer on your LAN.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

8.5 Client List Screen

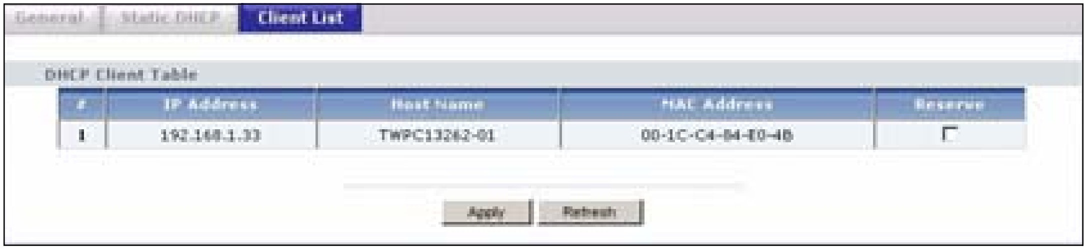
The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of LAN or Guest WLAN network clients using the P-320W v3's DHCP servers.

Configure this screen to always assign an IP address to a MAC address (and host name). Click **Network** > **DHCP Server** > **Client List**.

Note: You can also view a read-only client list by clicking the **DHCP Table (Details...)** hyperlink in the **Status** screen.

The following screen displays.

Figure 58 Network > DHCP Server > Client List



DHCP Client Table

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	TWPC13262-01	00-1C-C4-84-E0-4B	□

The following table describes the labels in this screen.

Table 38 Network > DHCP Server > Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select this check box in the **LAN DHCP Setup** or **Guest WLAN DHCP Setup** section to have the P-320W v3 always assign the IP address(es) to the MAC address(es) (and host name(s)). After you click **Apply**, the MAC address and IP address also display in the **Advanced** screen (where you can edit them).
Apply	Click **Apply** to save your settings.
Refresh	Click **Refresh** to reload the DHCP table.

9

Network Address Translation (NAT)

9.1 Overview

This chapter discusses how to configure NAT on the P-320W v3.

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

9.2 What You Can Do

- Use the **General NAT** screen (Section 9.4 on page 96) to enable NAT on your P-320W v3.
- Use the **Port Forwarding** screen (Section 9.5 on page 97) to define the local servers to which the incoming services will be forwarded.
- Use the **Trigger Port** screen (Section 9.3.2 on page 95) change your P-320W v3's trigger port settings.

9.3 What You Need to Know

The following section provides information on how you can properly configure NAT.

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the P-320W v3.

9.3.1 Port Forwarding: Services and Port Numbers

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

Use the **Application** screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

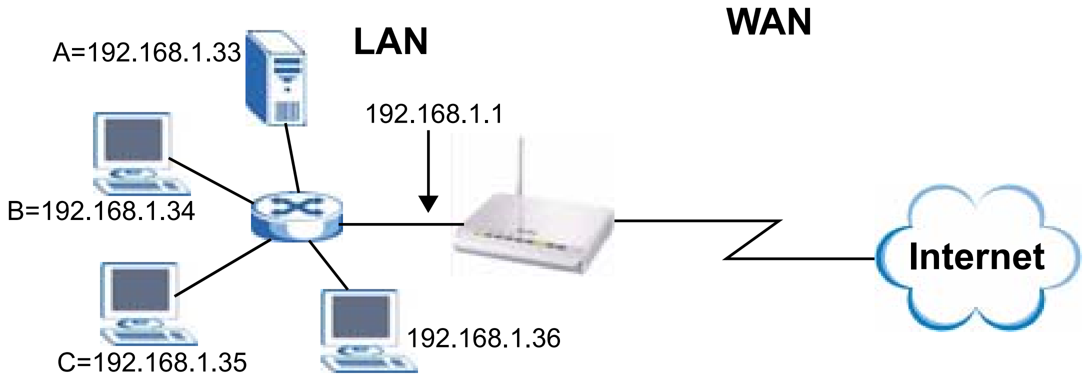
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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.

9.3.1.1 Configuring Servers Behind Port Forwarding Example

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

Figure 59 Multiple Servers Behind NAT Example



9.3.2 Trigger Port Forwarding

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

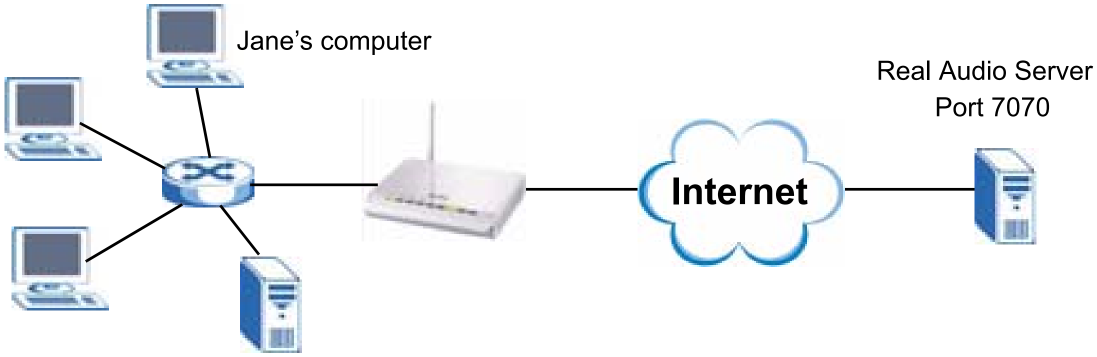
WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another 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-320W v3 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-320W v3's WAN port receives a response with a specific port number and protocol ("incoming" port), the P-320W v3 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.

9.3.2.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 60 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-320W v3 to record Jane's computer IP address. The P-320W v3 associates Jane's computer IP address with the "incoming" port range of 6970-7170.

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

4 The P-320W v3 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-320W v3 times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

9.3.3 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is going coming from inside the P-320W v3 and going to the outside.

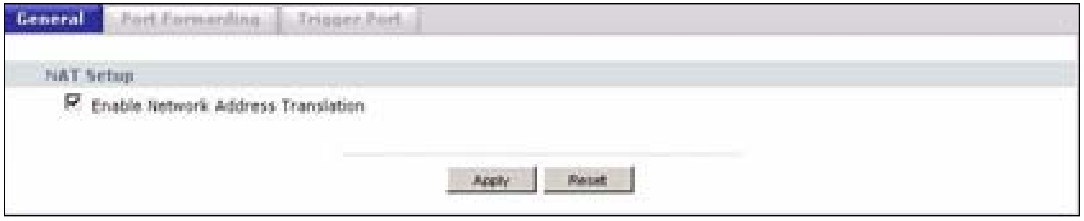
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

9.4 General NAT Screen

Use this screen to enable NAT on your P-320W v3.

Click **Network > NAT** to open the **General** screen.

Figure 61 Network > NAT > General



☑ Enable Network Address Translation

The following table describes the labels in this screen.

Table 39 Network > NAT > General

LABEL	DESCRIPTION
Enable Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select the check box to enable NAT.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

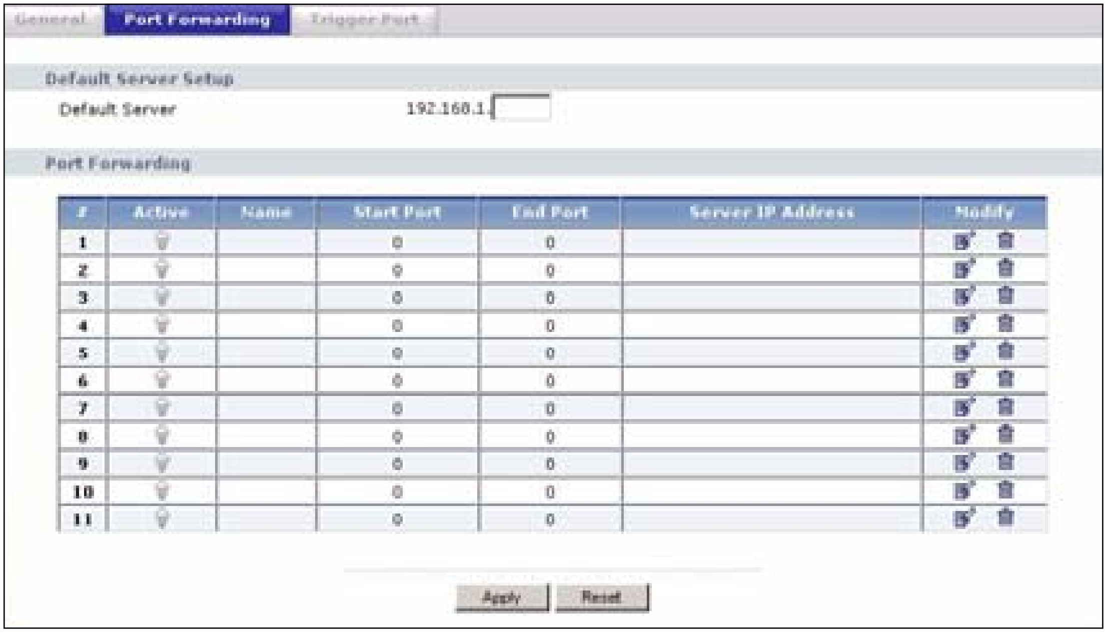
9.5 Port Forwarding Screen

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your P-320W v3's port forwarding settings, click **Network > NAT** > **Application**. The screen appears as shown.

Note: If you do not assign a **Default Server** IP address in the **NAT > General** screen, the P-320W v3 discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix E on page 247 for port numbers commonly used for particular services.

Figure 62 Network > NAT > Application



Default Server Setup

Default Server 192.168.1.

Port Forwarding

#	Active	Name	Start Port	End Port	Server IP Address	Modify
1			0	0		
2			0	0		
3			0	0		
4			0	0		
5			0	0		
6			0	0		
7			0	0		
8			0	0		
9			0	0		
10			0	0		
11			0	0		

The following table describes the labels in this screen.

Table 40 NAT Application

LABEL	DESCRIPTION
Default Server Setup	
Default Server	Type the inside IP address of the server that receives packets from the port(s) that are not specified in the **Port** field.
Port Forwarding	
#	This is the number of an individual port forwarding server entry.
Active	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.
Start Port	This field displays a start port number.
End Port	This field displays an end port number. If the same port number as the **Start Port** is displayed then a single port is forwarded. If a different number to the **Start Port** number is displayed then a range of ports are forwarded.
Server IP Address	This field displays the inside IP address of the server.

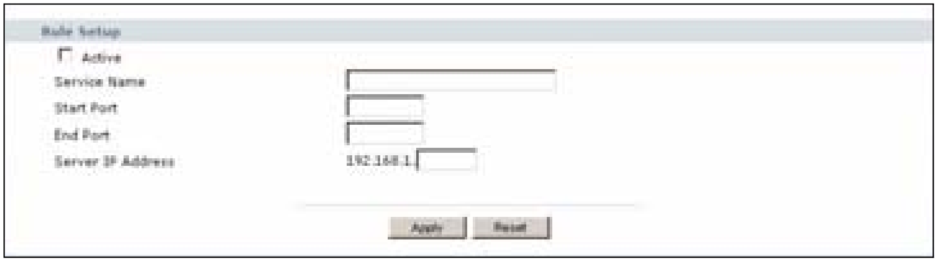
Table 40 NAT Application (continued)

LABEL	DESCRIPTION
Modify	Click the **Edit** icon to display and modify an existing rule setting in the fields under **Add Application Rule**. Click the **Remove** icon to delete a rule.
Apply	Click **Apply** to save your changes to the **Application Rules Summary** table.
Reset	Click **Reset** to not save and return your new changes in the **Service Name** and **Port** fields to the previous one.

9.5.1 Rule Setup Screen

To edit a port forwarding rule, click the edit icon under Modify. The following screen displays.

Figure 63 NAT: Port Forwarding: Rule Setup



Rule Setup

□ Active

Service Name

Start Port

End Port

Server IP Address 192.168.1.

The following table describes the labels in this screen.

Table 41 Network > NAT > General

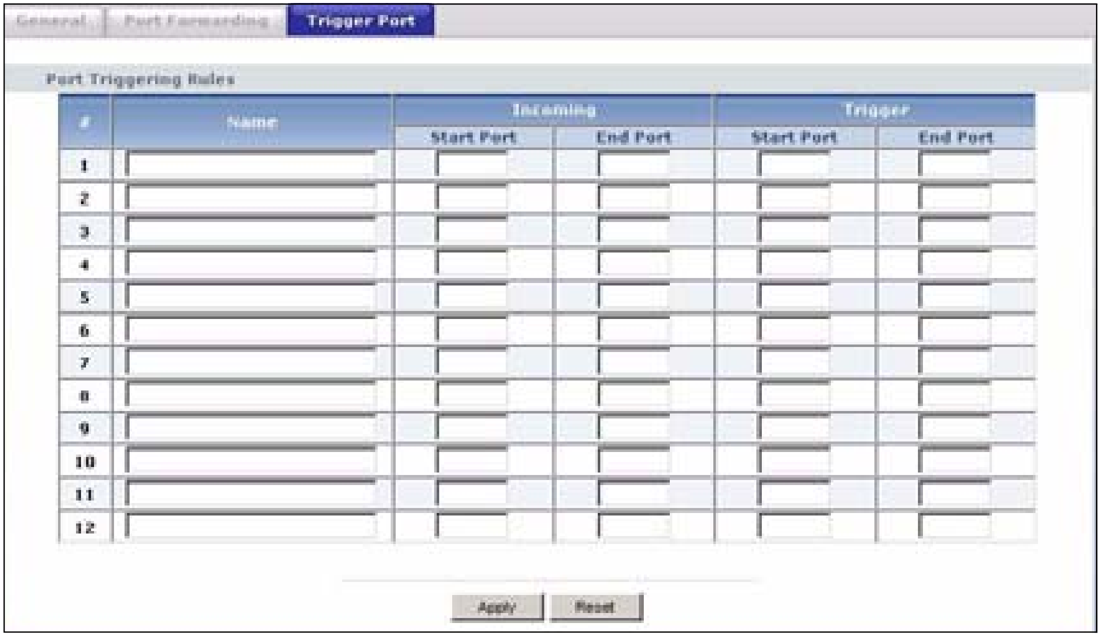
LABEL	DESCRIPTION
Active	Select the check box to enable this port forwarding entry. Clear the checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Type a Service Name to identify this port-forwarding rule.
Start Port	Type a start port number. To forward only one port, enter it again in the End Port field. To specify a range of ports, enter the last port to be forwarded in the End Port field.
End Port	Type an end port number.
Server IP Address	Type the inside IP address of the server.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

9.6 Trigger Port Screen

To change your P-320W v3's trigger port settings, click **Network > NAT** > **Advanced**. The screen appears as shown.

Note: Only one LAN computer can use a trigger port (range) at a time.

Figure 64 Network > NAT > Advanced



Port Triggering Rules

#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					

The following table describes the labels in this screen.

Table 42 Network > NAT > Advanced

LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The P-320W v3 forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the P-320W v3 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.

Table 42 Network > NAT > Advanced

LABEL	DESCRIPTION
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

9.7 Technical Reference

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

9.7.1 Game List Example

Here is an example game list text file. The index number, service name and associated port(s) are specified by semi-colons (no spaces). Use the name=xxx (where xxx is the service name) to create a new service. Port range can be separated with a hyphen (-) (no spaces). Multiple (non-consecutive) ports can be separated by commas.

Figure 65 Game List Example

```
version=1
1;name=Battlefield 1942;port=14567,22000,23000-23009,27900,28900
2;name=Call of Duty;port=28960
3;name=Civilization IV;port=2056
4;name=Diablo I and II;port=6112-6119,4000
5;name=Doom 3;port=27666
6;name=F.E.A.R;port=27888
7;name=Final Fantasy XI;port=25,80,110,443,50000-65535
8;name=Guild Wars;port=6112,80
9;name=Half Life;port=6003,7002,27005,27010,27011,27015
10;name=Jedi Knight III: Jedi Academy;port=28060-28062,28070-28081
11;name=Need for Speed: Hot Pursuit 2;port=1230,8511-
8512,27900,28900,61200-61230
12;name=Neverwinter Nights;port=5120-5300,6500,27900,28900
13;name=Quake 2;port=27910
14;name=Quake 3;port=27660,27960
15;name=Rainbow Six 3: Raven Shield;port=7777-7787,8777-8787
16;name=Serious Sam II;port=25600-25605
17;name=Silent Hunter III;port=17997-18003
18;name=Soldier of Fortune II;port=20100-20112
19;name=Starcraft;port=6112-6119,4000
20;name=Star Trek: Elite Force II;port=29250,29256
21;name=SWAT 4;port=10480-10483
22;name=Warcraft II and III;port=6112-6119,4000
23;name=World of Warcraft;port=3724
```

10

VLAN

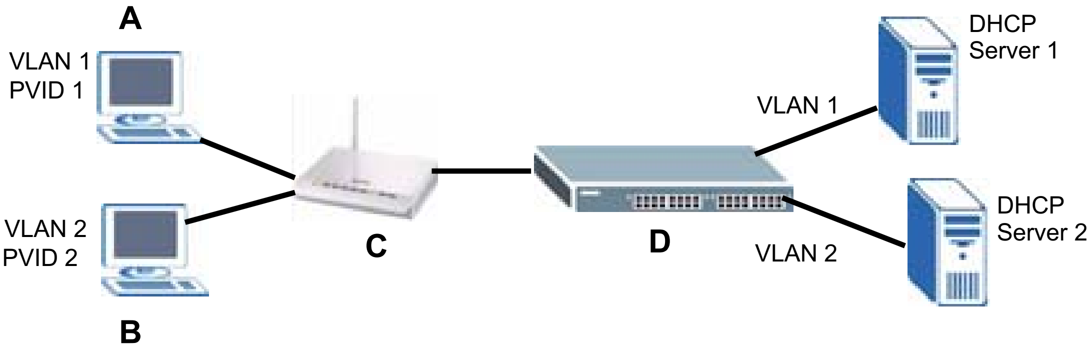
10.1 Overview

This chapter shows you how to configure VLANs on your P-320W v3.

A Virtual LAN (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other. Stations on a logical network can belong to one or more groups.

In the figure below, your P-320W v3 (**C**) has VLAN configured on two of its ports. Frames coming from computer **A** are tagged with Port VLAN ID (PVID) 1 and those from computer **B** are tagged with PVID 2. When computers **A** and **B** request IP addresses, the P-320W v3 forwards this to the VLAN-aware switch (**D**). The switch sends each request to the corresponding DHCP server. Computer **A** gets its IP address from DHCP Server 1, and computer **B** gets its IP address from DHCP server 2.

Figure 66 VLAN Example



10.2 What You Can Do

Use the **VLAN** screen (Section 10.4 on page 102) to configure the Port VLAN ID (PVID) on the physical ports of the P-320W v3.

10.3 What You Need to Know

The following sections provide information that can help you configure the VLAN screen of your P-320W v3.

10.3.1 How VLAN Works

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 (which is an 802.1 protocol). 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 for the TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes for the TCI (Tag Control Information, starting after the source address field of the Ethernet frame).

10.3.2 VLAN Tag

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 the value 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4,094.

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

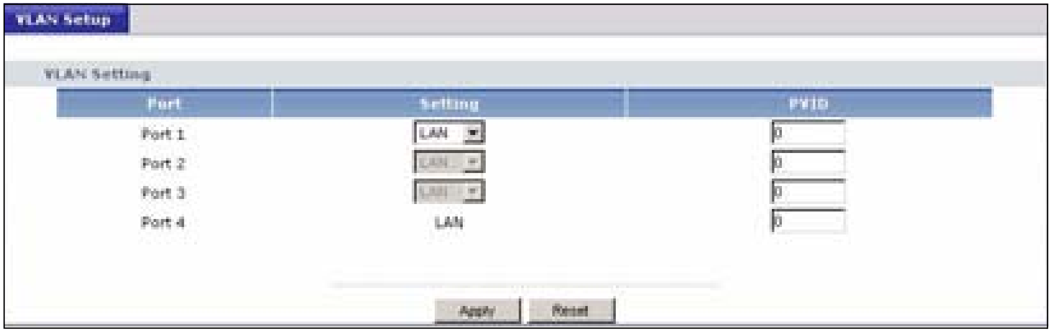
10.4 VLAN Screen

Use this screen to configure the Port VLAN ID (PVID) on the physical ports of the P-320W v3. The P-320W v3 forwards tagged frames to a VLAN-aware switch that can send the frames to its corresponding destination.

Note: Tagged traffic remains in the same VLAN and cannot be seen by other VLANs.

Click **Network > VLAN** to open the following screen.

Figure 67 Network > VLAN



VLAN Setting

Port	Setting	PVID
Port 1	LAN	0
Port 2	LAN	0
Port 3	LAN	0
Port 4	LAN	0

The following table describes the labels in this screen.

Table 43 Network > VLAN

LABEL	DESCRIPTION
Port	This column displays the port name (LAN1 ~ LAN4).
Setting	Specify whether a port is **LAN** (default for all ports) or is part of a **VLAN**. Note: **Port 4**’s setting is always set to **LAN**. This ensures that you can manage the P-320W v3 through a LAN port if necessary.
PVID	Enter the Port VLAN ID (1 ~ 4094) to add to untagged frames received on each port.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

PART III
Security

11

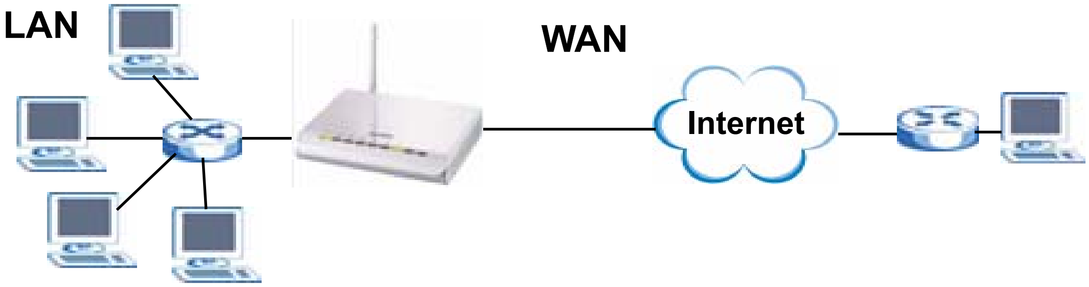
WAN

11.1 Overview

This chapter discusses the P-320W v3's **WAN** screens. Use these screens to configure your P-320W v3 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 68 LAN and WAN



See the chapter about the connection wizard for more information on the fields in the WAN screens.

11.2 What You Can Do

- Use the **Internet Connection** screen (Section 11.3 on page 108) to configure your P-320W v3's Internet access settings.
- Use the **Advanced** screen (Section 11.4 on page 114) to change your P-320W v3's advanced WAN settings.
- Use the **Traffic Redirect** screen (Section 11.5 on page 114) to enable the P-320W v3 to redirect traffic.

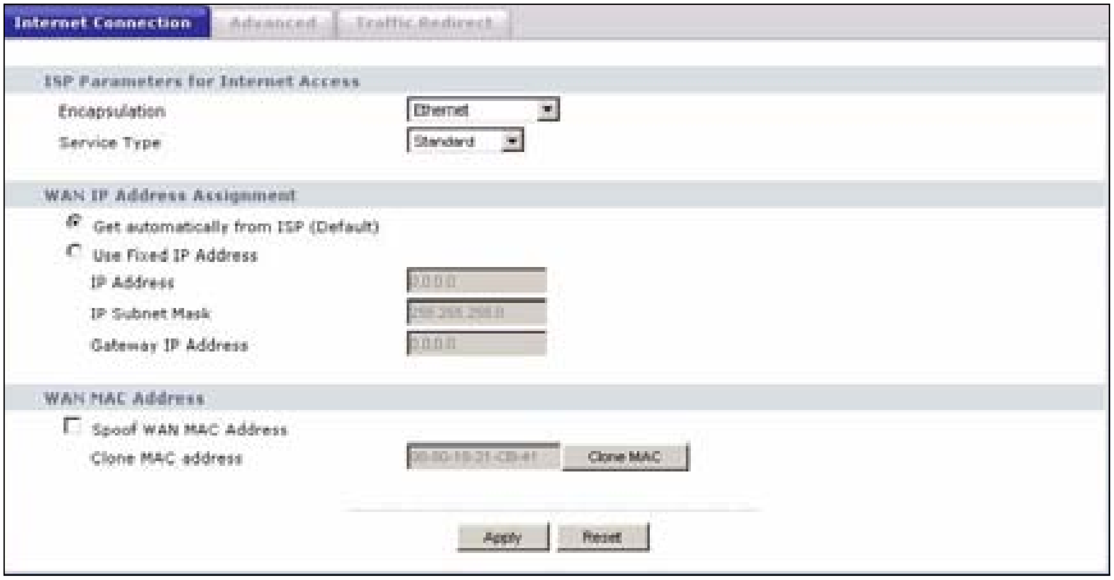
11.3 Internet Connection Screen

Use this screen to configure your P-320W v3's Internet access settings. Click **Network** > **WAN**. The screen differs according to the encapsulation you choose.

11.3.1 Ethernet Encapsulation

This screen displays when you select **Ethernet** encapsulation.

Figure 69 Network > WAN > Internet Connection: Ethernet Encapsulation



ISP Parameters for Internet Access

Encapsulation: Ethernet

Service Type: Standard

WAN IP Address Assignment

● Get automatically from ISP (Default)

○ Use Fixed IP Address

IP Address: 0.0.0.0

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

WAN MAC Address

□ Spoof WAN MAC Address

Clone MAC address: 00-50-18-21-C8-41

The following table describes the labels in this screen.

Table 44 Network > WAN > Internet Connection: Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Choose the **Ethernet** option when the WAN port is used as a regular Ethernet.
Service Type	Choose from **Standard**, **RR-Toshiba** (Roadrunner Toshiba authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Telstra** (RoadRunner Telstra authentication method) or **Telia Login**. The following fields do not appear with the **Standard** service type. • **User Name** - Enter the user name for the account. • **Password** - Enter the password associated with the user name above. • **Retype to Confirm** - Type your password again to make sure that you have entered is correctly. • **Login Server** - Enter the IP address of the server you want to use.
WAN IP Address Assignment	

Table 44 Network > WAN > Internet Connection: Ethernet Encapsulation

LABEL	DESCRIPTION
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
IP Subnet Mask	Enter the **IP Subnet Mask** in this field.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the P-320W v3's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Spoof WAN MAC address	Select this if you want to hide your computer's MAC address. Enter the MAC address you want to use and click **Clone MAC**. Clear the check box to use the factory assigned default MAC Address.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

11.3.2 PPPoE Encapsulation

The P-320W v3 supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

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

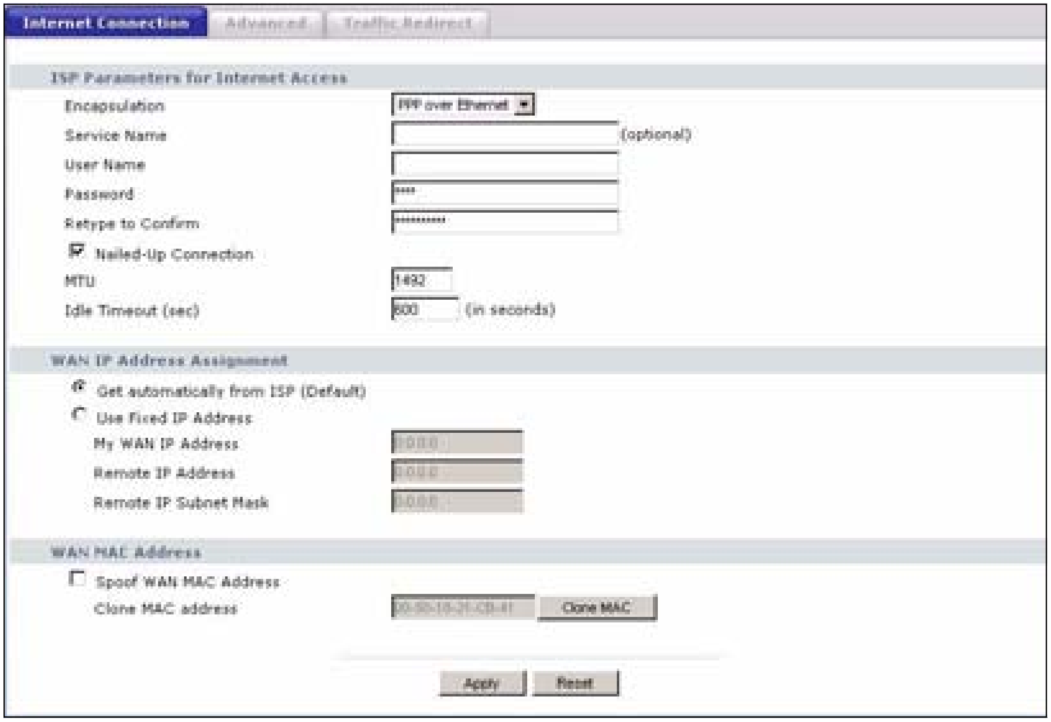
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

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

By implementing PPPoE directly on the P-320W v3 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the P-320W v3 does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

This screen displays when you select **PPPoE** encapsulation.

Figure 70 Network > WAN > Internet Connection: PPPoE Encapsulation



ISP Parameters for Internet Access

Encapsulation	PPP over Ethernet
Service Name	(optional)
User Name	
Password	****
Retype to Confirm	**********
☑ Nailed-Up Connection	
MTU	1492
Idle Timeout (sec)	600 (in seconds)

WAN IP Address Assignment

● Get automatically from ISP (Default)	
○ Use Fixed IP Address	
My WAN IP Address	0.0.0.0
Remote IP Address	0.0.0.0
Remote IP Subnet Mask	0.0.0.0

WAN MAC Address

□ Spoof WAN MAC Address	
Clone MAC address	00-50-18-21-CB-41

The following table describes the labels in this screen.

Table 45 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Choose the **PPP over Ethernet** if you connect to the Internet using dial-up.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
MTU	The Maximum Transmission Unit (MTU) refers to the largest packet size that a device can forward. Enter the value (in bytes) that you want the P-320W v3 to be able to handle. The default value is 1492 bytes.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default value is 600 seconds.
WAN IP Address Assignment	

Table 45 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
Remote IP Address	Enter the remote IP address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	Enter the remote IP subnet mask in this field.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the P-320W v3's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Spoof the computer's MAC address	Select this if you want to hide your computer's MAC address. Enter the MAC address you want to use and click **Clone MAC**. Clear the check box to use the factory assigned default MAC Address.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

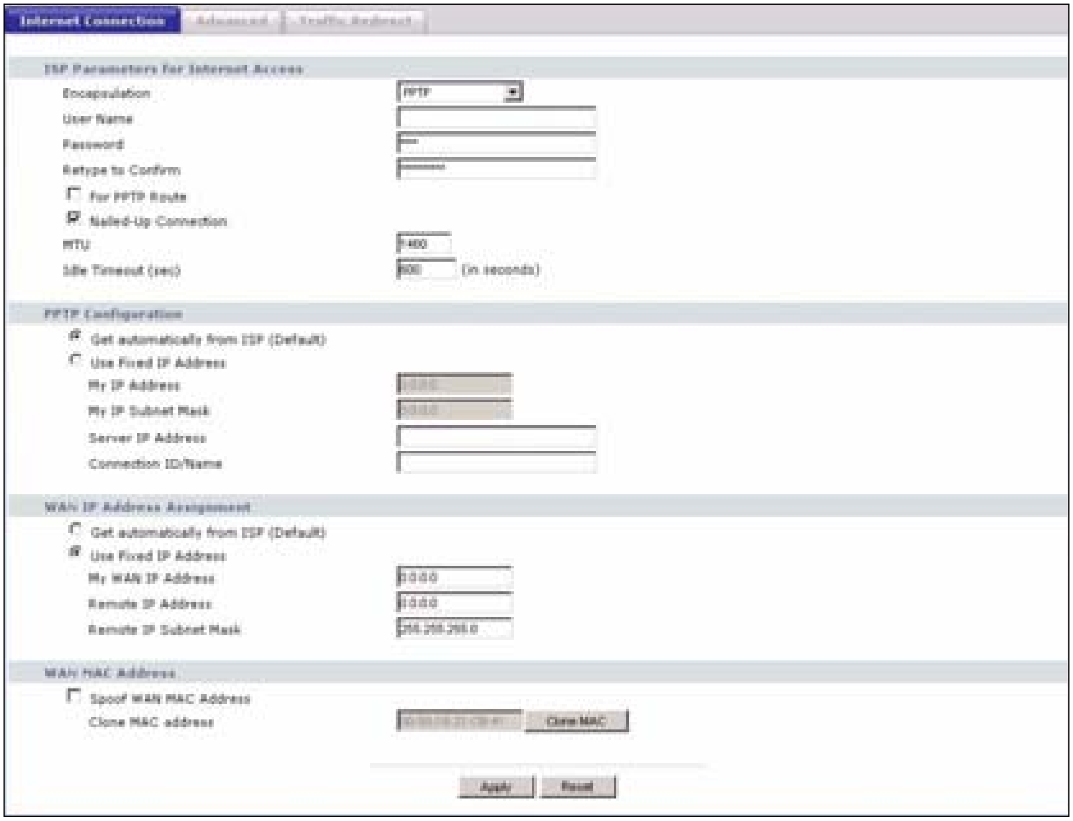
11.3.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

This screen displays when you select **PPTP** encapsulation.

Figure 71 Network > WAN > Internet Connection: PPTP Encapsulation



ISP Parameters for Internet Access

Encapsulation	PPTP
User Name	
Password	****
Retype to Confirm	********
☐ For PPTP Route	
☑ Nailed-Up Connection	
MTU	1460
Idle Timeout (sec)	600 (in seconds)

PPTP Configuration

● Get automatically from ISP (Default)	
○ Use Fixed IP Address	
My IP Address	0.0.0.0
My IP Subnet Mask	0.0.0.0
Server IP Address	
Connection ID/Name	

WAN IP Address Assignment

○ Get automatically from ISP (Default)	
● Use Fixed IP Address	
My WAN IP Address	0.0.0.0
Remote IP Address	0.0.0.0
Remote IP Subnet Mask	255.255.255.0

WAN MAC Address

☐ Spoof WAN MAC Address	
Clone MAC address	[illegible]

The following table describes the labels in this screen.

Table 46 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Choose **PPTP** to enable secure transfer of data from a remote client to a private server. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
For PPTP Route	
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
MTU	The Maximum Transmission Unit (MTU) refers to the largest packet size that a device can forward. Enter the value (in bytes) that you want the P-320W v3 to be able to handle. The default value is 1460 bytes.

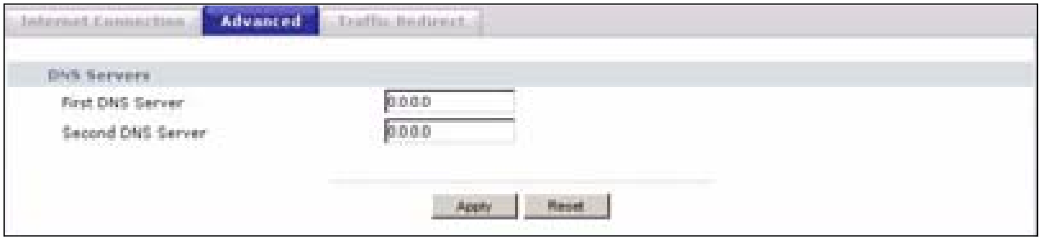
Table 46 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
Idle Timeout	This value specifies the time in seconds that elapses before the P-320W v3 automatically disconnects from the PPTP server. The default value is 600 seconds.
PPTP Configuration	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your P-320W v3 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the P-320W v3.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Type your identification name for the PPTP server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
Remote IP Address	Enter the remote IP address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	Enter the remote IP subnet mask in this field.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the P-320W v3's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Spoof the computer's MAC address	Select this if you want to hide your computer's MAC address. Enter the MAC address you want to use and click **Clone MAC**. Clear the check box to use the factory assigned default MAC Address.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

11.4 Advanced Screen

To change your P-320W v3’s advanced WAN settings, click **Network** > **WAN** > **Advanced**. The screen appears as shown.

Figure 72 Network > WAN > Advanced



DNS Servers

First DNS Server 0.0.0.0

Second DNS Server 0.0.0.0

The following table describes the labels in this screen.

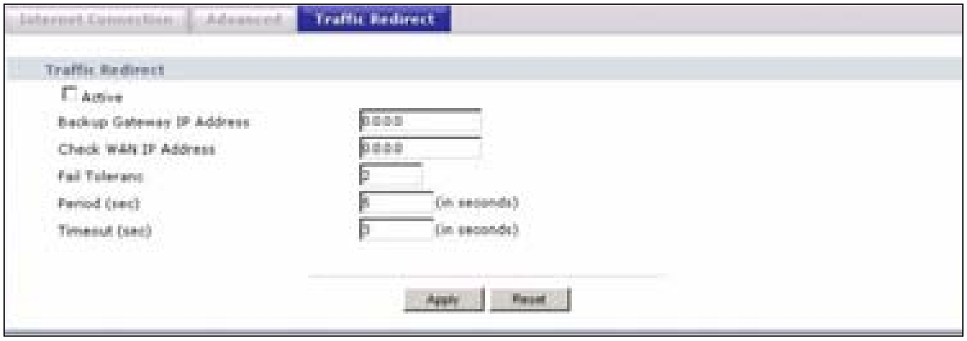
Table 47 WAN > Advanced

LABEL	DESCRIPTION
First DNS Server Second DNS Server	Enter the DNS server's IP address in the field to the right. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

11.5 Traffic Redirect Screen

To enable the P-320W v3 to redirect traffic, click **Network** > **WAN** > **Advanced**. The screen appears as shown.

Figure 73 Network > WAN > Advanced



Traffic Redirect

□ Active

Backup Gateway IP Address 0.0.0.0

Check WAN IP Address 0.0.0.0

Fail Toleranc 2

Period (sec) 5 (in seconds)

Timeout (sec) 3 (in seconds)

The following table describes the labels in this screen.

Table 48 WAN > Advanced

LABEL	DESCRIPTION
Active	Select this check box to have the P-320W v3 use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The P-320W v3 automatically forwards traffic to this IP address if the P-320W v3's Internet connection terminates.
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the P-320W v3 will use the default gateway IP address. Configure this field to test your P-320W v3's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you are using PPTP or PPPoE Encapsulation, type "0.0.0.0" to configure the P-320W v3 to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Type the number of times your P-320W v3 may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
Period	Type the number of seconds for the P-320W v3 to wait between checks to see if it can connect to the WAN IP address (Check WAN IP Address field) or default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds for your P-320W v3 to wait for a ping response from the IP Address in the Check WAN IP Address field before it times out. The WAN connection is considered "down" after the P-320W v3 times out the number of times specified in the Fail Tolerance field. Use a higher value in this field if your network is busy or congested.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

12

Firewall

12.1 Overview

This chapter gives some background information on firewalls and explains how to get started with the P-320W v3's firewall.

Originally, the term "firewall" referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from a network that is not trusted. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

12.2 What You Can Do

- Use the **General** screen (Section 12.4 on page 119) to enable or disable the P-320W v3's firewall.
- Use the **Services** screen (Section 12.5 on page 119) to to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

12.3 What You Need to Know

The following sections provide more information about the P-320W v3's firewalls.

12.3.1 About the P-320W v3 Firewall

The P-320W v3 firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The P-320W v3's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The P-320W v3 can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The P-320W v3 is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The P-320W v3 has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

12.3.1.1 Stateful Inspection Firewall

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

12.3.2 Security Parameter Index (SPI)

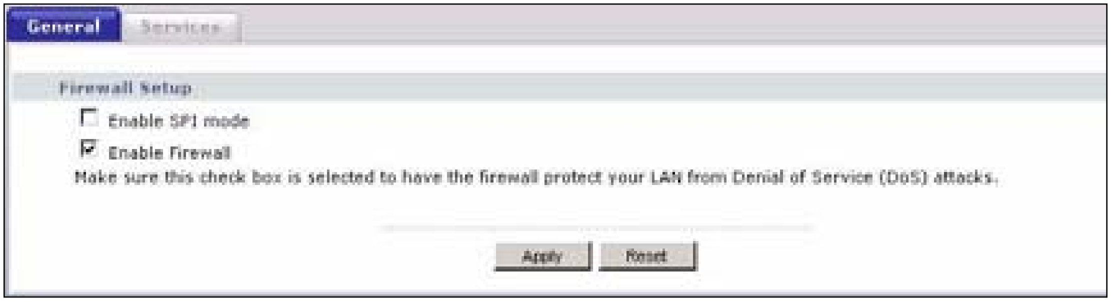
An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The SPI (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The SPI is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel. Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

12.4 General Firewall Screen

Use this screen to enable or disable the P-320W v3's firewall.

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

Figure 74 Security > Firewall > General I



Firewall Setup

☐ Enable SPI mode

☑ Enable Firewall

Make sure this check box is selected to have the firewall protect your LAN from Denial of Service (DoS) attacks.

The following table describes the labels in this screen.

Table 49 Security > Firewall > General

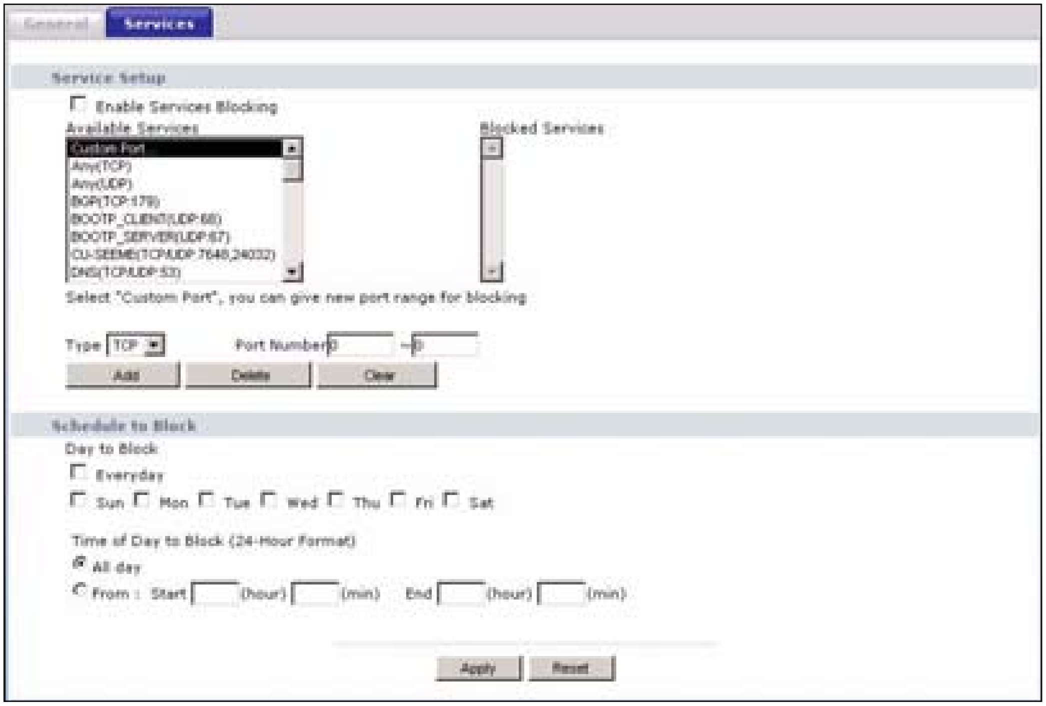
LABEL	DESCRIPTION
Enable SPI mode	Check this to enable SPI. The inspects incoming packets and determines whether the destination and source port is in the session table or not.
Enable Firewall	Select this check box to activate the firewall. The P-320W v3 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

12.5 Services Screen

Use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Click **Security** > **Firewall** > **Services**. The screen appears as shown next.

Figure 75 Security > Firewall > Services



□ Enable Services Blocking

Select "Custom Port", you can give new port range for blocking

Type TCP

Port Number 0 ~ 0

□ Everyday

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Time of Day to Block (24-Hour Format)

● All day

○ From : Start (hour) (min) End (hour) (min)

The following table describes the labels in this screen.

Table 50 Security > Firewall > Services

LABEL	DESCRIPTION
Service Setup	
Enable Services Blocking	Select this check box to enable this feature.
Available Services	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Please see Section 9.3.1 on page 111 for more information on services available. Select the port you want to block using the drop-down list and click Add to add the port to the Blocked Services field.
Blocked Services	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking. Choose the IP port (TCP, UDP or TCP/UDP) that defines your customized port from the drop down list box.
Custom Port	A custom port is a service that is not available in the pre-defined Available Services list and you must define using the next two fields.
Type	Services are either TCP and/or UDP. Select from either TCP or UDP.
Port Number	Enter the port number range that defines the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range from 6345-6349.
Add	Select a service from the Available Services drop-down list and then click Add to add a service to the Blocked Services.

Table 50 Security > Firewall > Services

LABEL	DESCRIPTION
Delete	Select a service from the Blocked Services list and then click Delete to remove this service from the list.
Clear	Click Clear to empty the Blocked Services.
Schedule to Block	
Day to Block	Select a check box to configure which days of the week (or everyday) you want the content filtering to be active.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting the All Day check box. You can also configure specific times that by entering the start time in the Start (hr) and Start (min) fields and the end time in the End (hr) and End (min) fields. Enter times in 24-hour format, for example, "3:00pm" should be entered as "15:00".
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

12.6 Technical Reference

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

12.6.1 Guidelines For Enhancing Security With Your Firewall

1 Change the default password via web configurator.

2 Think about access control before you connect to the network in any way, including attaching a modem to the port.

3 Limit who can access your router.

4 Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.

5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

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

Keep the firewall in a secured (locked) room.

12.6.2 Services

The commonly used services and port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the DNS service. (UDP/TCP:53) means UDP port 53 and TCP port 53..

Table 51 Services

SERVICE	DESCRIPTION
AIM/NEW_ICQ(TCP:5190)	AOL's Internet Messenger service, 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(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
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: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)	Net Meeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IPSEC_TRANSPORT/ TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
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.

Table 51 Services (continued)

SERVICE	DESCRIPTION
PING(ICMP:0)	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).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	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.
SSDP(UDP:1900)	Simole Service Discovery Protocol (SSDP) is a discovery service searching for Universal Plug and Play devices on your home network or upstream Internet gateways using DUDP port 1900.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRMWORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

13

Content Filtering

13.1 Overview

This chapter provides a brief overview of content filtering using the embedded web GUI.

Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering is the ability to block certain web features or specific URL keywords.

The P-320W v3 can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

13.2 What You Can Do

Use the Filter screen (Section 13.3 on page 125) to configure filter rules on your P-320W v3.

13.3 Filter Screen

Use this screen to block web features such as ActiveX controls, Java applets, cookies and disable web proxies. You can create a list of keywords to block so that web pages containing these words cannot be viewed by users.

Click **Security** > **Content Filter** to open the **Filter** screen.

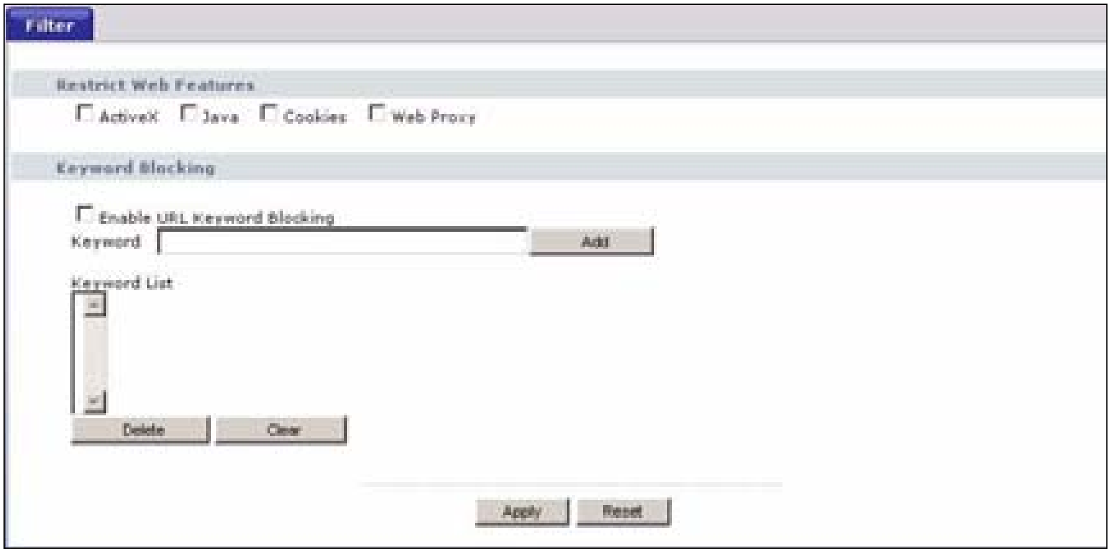


Figure 76 Security > Content Filter > Filter

The following table describes the labels in this screen.

Table 52 Security > Content Filter > Filter

LABEL	DESCRIPTION
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Keyword Blocking	
Enable URL Keyword Blocking	The P-320W v3 can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.

Table 52 Security > Content Filter > Filter

LABEL	DESCRIPTION
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Clear	Click this button to remove all of the listed keywords.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh

13.4 Technical Reference

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

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

13.4.1 Domain Name or IP Address URL Checking

By default, the P-320W v3 checks the URL's domain name or IP address when performing keyword blocking.

This means that the P-320W v3 checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

13.4.2 Full Path URL Checking

Full path URL checking has the P-320W v3 check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

13.4.3 File Name URL Checking

Filename URL checking has the P-320W v3 check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

PART IV
Management

14

Static Route

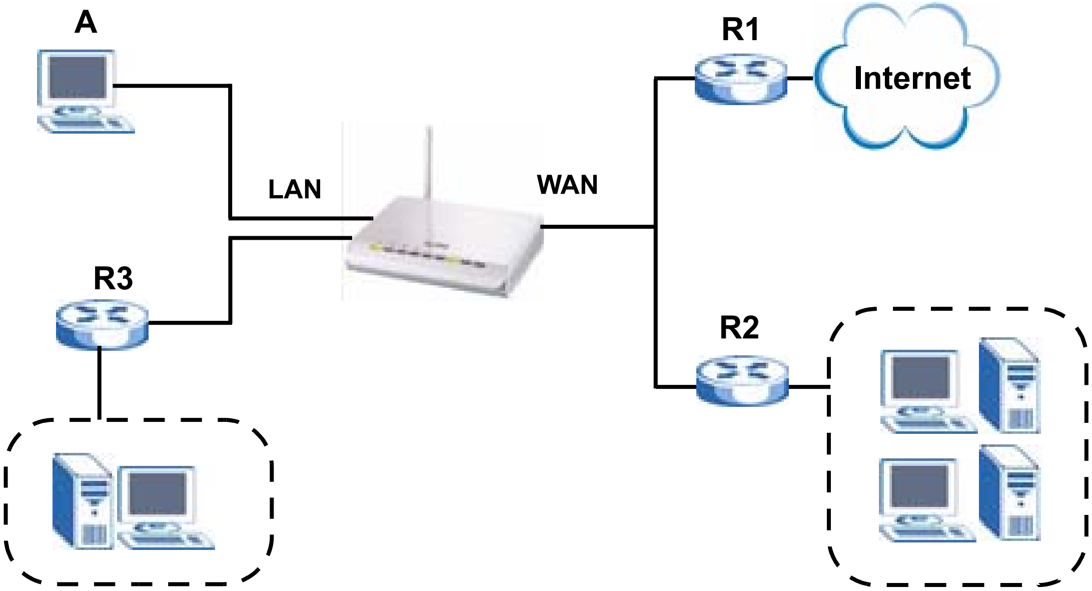
14.1 Overview

This chapter shows you how to configure static routes for your P-320W v3.

The P-320W v3 usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the P-320W v3 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-320W v3's LAN interface. The P-320W v3 routes most traffic from **A** to the Internet through the P-320W v3'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 77 Example of Static Routing Topology



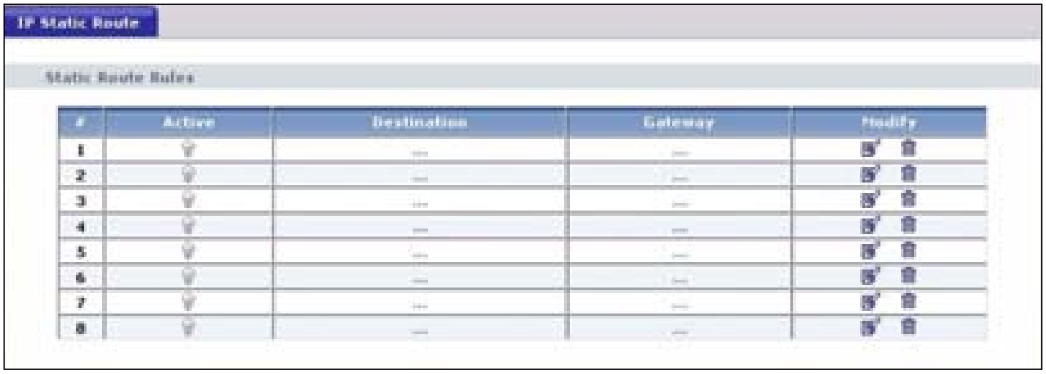
14.2 What You Can Do

Use the **IP Static Route** screen (Section 14.3 on page 132) to create and edit static routes on your P-320W v3.

14.3 IP Static Route Screen

Click **Management** > **Static Route** to open the **IP Static Route** screen. The following screen displays.

Figure 78 Management > Static Route > IP Static Route



IP Static Route

Static Route Rules

#	Active	Destination	Gateway	Modify
1		---	---	
2		---	---	
3		---	---	
4		---	---	
5		---	---	
6		---	---	
7		---	---	
8		---	---	

The following table describes the labels in this screen.

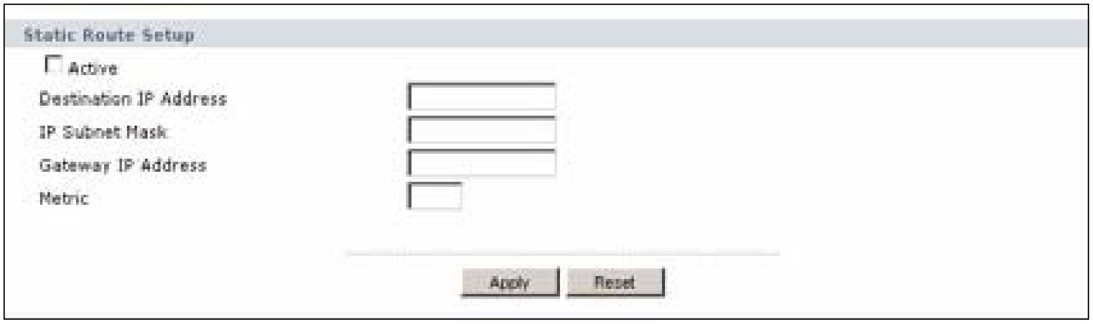
Table 53 Management > Static Route > IP Static Route

LABEL	DESCRIPTION
#	This is the index number of an individual static route. The first entry is for the default route and not editable.
Active	This icon is turned on when this static route is active. Click the **Edit** icon under **Modify** and select the **Active** checkbox in the **Static Route Setup** screen to enable the static route. Clear the checkbox to disable this static route without having to delete the entry.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of your P-320W v3 that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your P-320W v3; over the WAN, the gateway must be the IP address of one of the remote nodes.
Modify	Click the **Edit** icon to open the static route setup screen. Modify a static route or create a new static route in the **Static Route Setup** screen. Click the **Remove** icon to delete a static route.

14.3.1 Static Route Setup Screen

To edit a static route, click the edit icon under **Modify**. The following screen displays. Fill in the required information for each static route.

Figure 79 Management > Static Route > IP Static Route: Static Route Setup



Static Route Setup

□ Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

The following table describes the labels in this screen.

Table 54 Management > Static Route > IP Static Route: Static Route Setup

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Private	This parameter determines if the P-320W v3 will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your P-320W v3 that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your P-320W v3; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

15

Remote Management

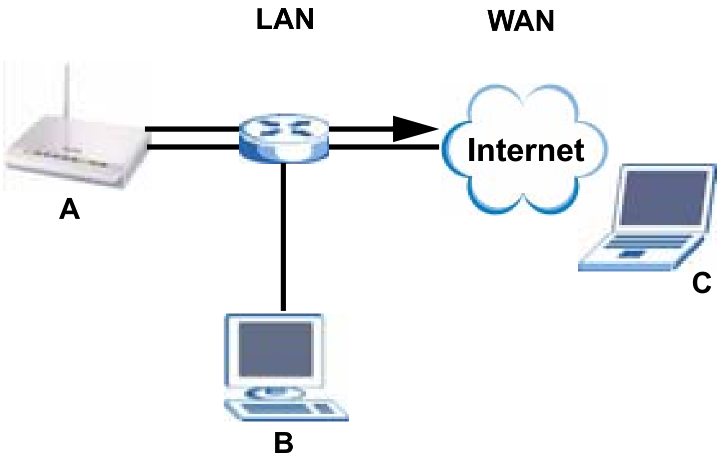
15.1 Overview

This chapter provides information on the Remote Management screens.

Remote management allows you to determine which services/protocols can access which P-320W v3 interface (if any) from which computers. You may manage your P-320W v3 from a remote location via:

- LAN only
- Both WAN and LAN

Figure 80 Remote Management Example



In the figure above, the P-320W v3 (**A**) is being managed by a desktop computer (**B**) connected via LAN (Land Area Network). It is also being accessed by a notebook (**C**) connected via WAN (Wide Area Network).

You may only have one remote management session running at a time.

15.2 What You Can Do

- Use the **WWW** screen (Section 15.4 on page 137) to change your P-320W v3's World Wide Web settings.
- Use the **SNMP** screen (Section 15.5 on page 138) to have a manager station administrate your P-320W v3 over the network.
- Use the **Security** screen (Section 15.6 on page 139) to configure how your P-320W v3 responds to ping from WAN.

15.3 What You Need to Know

The following sections provide helpful information needed to configure the screens in this chapter.

15.3.1 Remote Management Limitations

Remote management over LAN or LAN and WAN will not work when:

1 You have disabled that service in one of the remote management screens.

2 The IP address in the **Secured Client IP Address** field (Section 15.4 on page 137) does not match the client IP address. If it does not match, the P-320W v3 will disconnect the session immediately.

3 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

4 There is a firewall rule that blocks it.

15.3.2 Remote Management and NAT

When NAT is enabled:

- Use the P-320W v3's WAN IP address when configuring from the WAN.
- Use the P-320W v3's LAN IP address when configuring from the LAN.

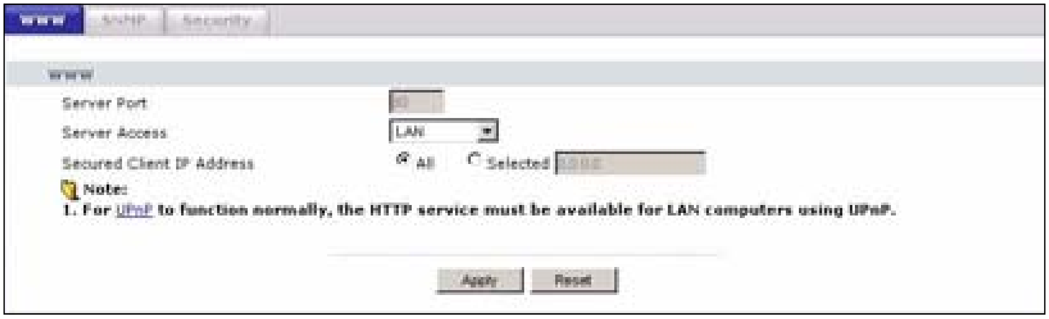
15.3.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The P-320W v3 automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen.

15.4 WWW Screen

To change your P-320W v3's World Wide Web settings, click **Management** > **Remote MGMT** to display the **WWW** screen.

Figure 81 Management > Remote MGMT > WWW



Server Port: 80

Server Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Note:
1. For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

The following table describes the labels in this screen

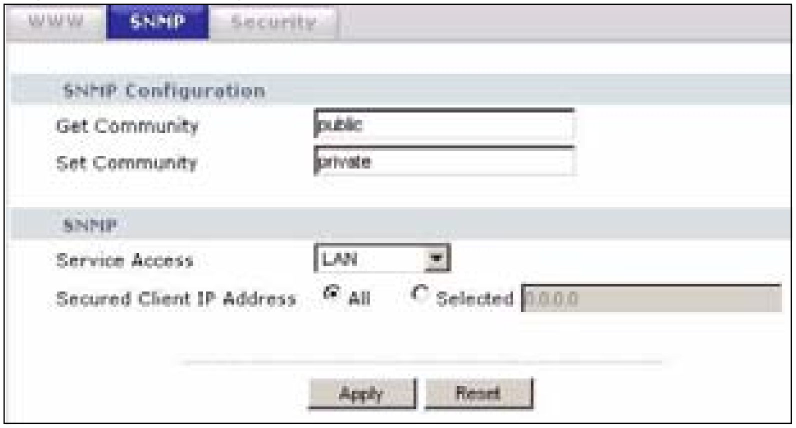
Table 55 Management > Remote MGMT > WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the P-320W v3 using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the P-320W v3 using this service. Select **All** to allow any computer to access the P-320W v3 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the P-320W v3 using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

15.5 The SNMP Screen

Use this screen to have a manager station administrate your P-320W v3 over the network. To change your P-320W v3's SNMP settings, click **Management** > **Remote MGMT > SNMP**. The following screen displays.

Figure 82 Management > Remote MGMT > SNMP



SNMP Configuration

Get Community: public

Set Community: private

SNMP

Service Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 56 Remote MGNT > Remote MGMT > SNMP

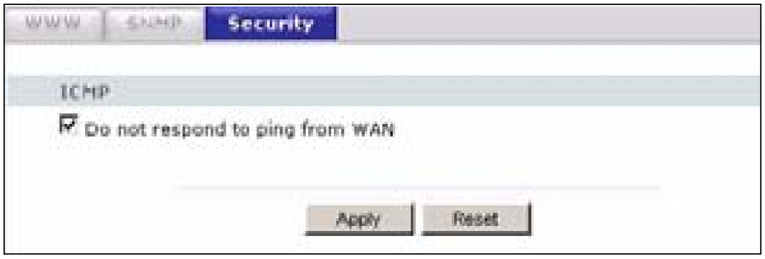
LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
SNMP	
Service Access	Select the interface(s) through which a computer may access the P-320W v3 using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the P-320W v3 using this service. Select **All** to allow any computer to access the P-320W v3 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the P-320W v3 using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

15.6 Security Screen

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

To configure how your P-320W v3 responds to ping from WAN, click **Management** > **Remote MGMT** to display the **Security** screen.

Figure 83 Management > Remote MGMT > Security



☑ Do not respond to ping from WAN

The following table describes the labels in this screen.

Table 57 Management > Remote MGMT > Security

LABEL	DESCRIPTION
Do not respond to ping from WAN	Check this if you do not want the P-320W v3 respond to any incoming WAN Ping requests.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

16

Universal Plug-and-Play (UPnP)

16.1 Overview

This chapter introduces the UPnP feature in the web configurator.

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

See Section 16.4 on page 143 for configuration instructions.

16.2 What You Can Do

Use the **General** screen (Section 16.4 on page 143) to activate UPnP.

16.3 What You Need to Know

The following sections provide information that can help you configure the UPnP screen.

16.3.1 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.

16.3.2 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.

16.3.3 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-320W v3 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.

16.3.4 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.

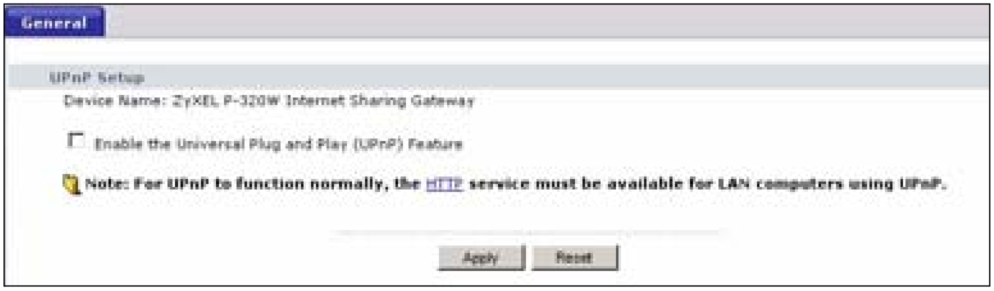
See the following sections for examples of installing and using UPnP.

16.4 UPnP Screen

Use this screen to activate UPnP.

Click the **Management > UPnP** to display the UPnP screen.

Figure 84 Management > UPnP > General



UPnP Setup

Device Name: ZyXEL P-320W Internet Sharing Gateway

□ Enable the Universal Plug and Play (UPnP) Feature

Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

The following table describes the labels in this screen.

Table 58 Management > UPnP > General

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the P-320W v3's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save the setting to the P-320W v3.
Reset	Click **Reset** to return to the previously saved settings.

16.5 Technical Reference

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

16.5.1 Installing UPnP in Windows Example

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

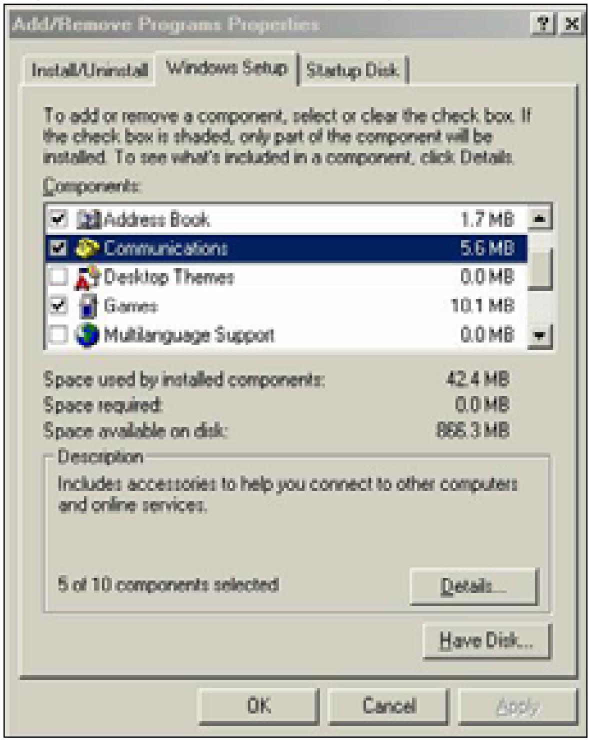
16.5.1.1 Installing UPnP in Windows Me

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 85 Add/Remove Programs: Windows Setup: Communication



To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Address Book	1.7 MB
☑	Communications	5.6 MB
□	Desktop Themes	0.0 MB
☑	Games	10.1 MB
□	Multilanguage Support	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

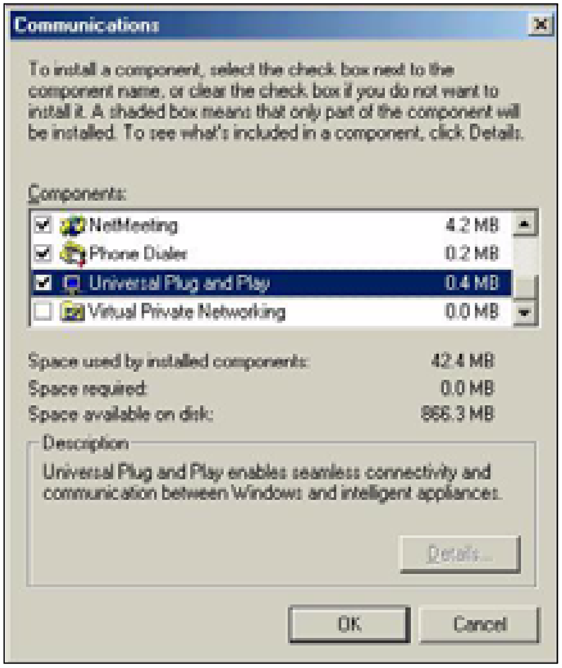
Description

Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

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

Figure 86 Add/Remove Programs: Windows Setup: Communication: Components



To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	NetMeeting	4.2 MB
☑	Phone Dialer	0.2 MB
☑	Universal Plug and Play	0.4 MB
□	Virtual Private Networking	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

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

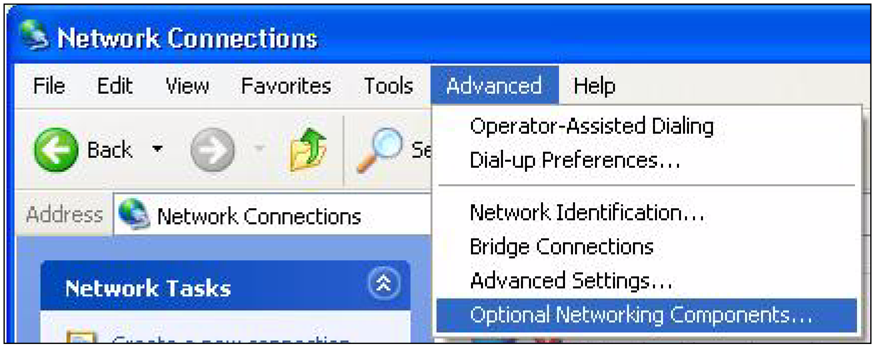
Follow the steps below to install the UPnP in Windows XP.

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

2 Double-click **Network Connections**.

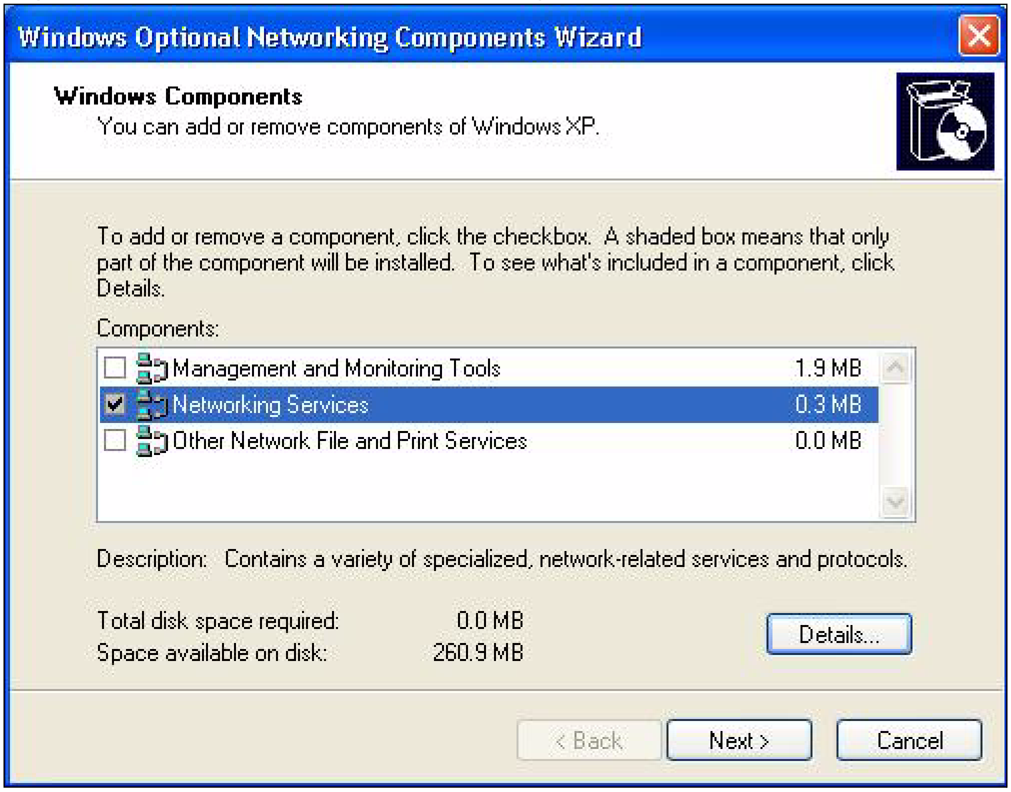
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 87 Network Connections



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

Figure 88 Windows Optional Networking Components Wizard



Windows Optional Networking Components Wizard

Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

□	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB

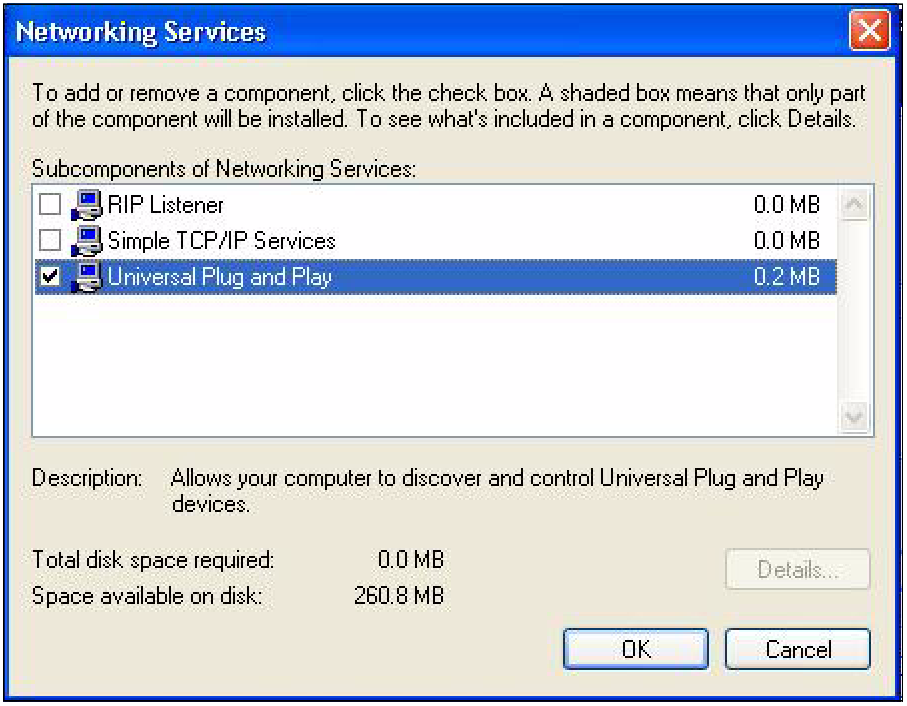
Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 260.9 MB

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

Figure 89 Networking Services



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□	RIP Listener	0.0 MB
□	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB

Space available on disk: 260.8 MB

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

16.5.1.2 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-320W v3.

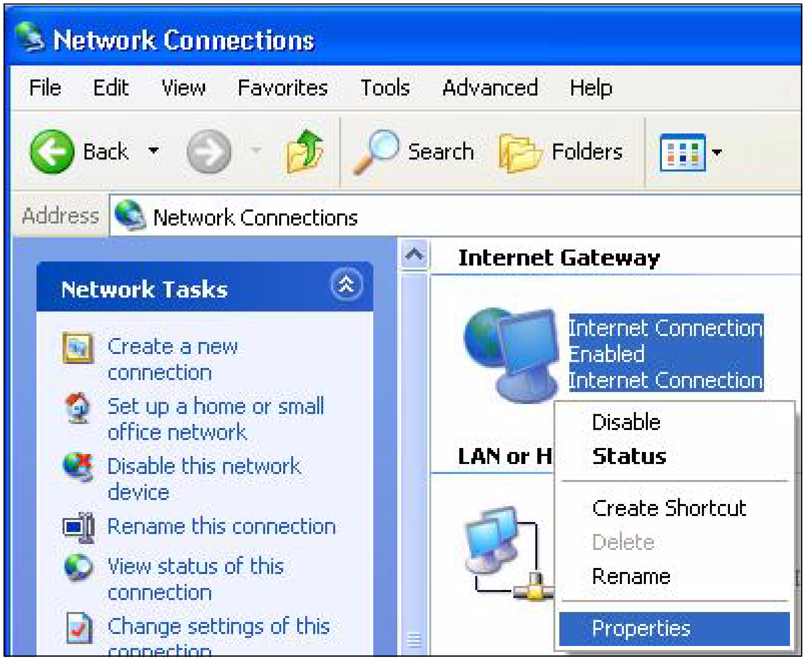
Make sure the computer is connected to a LAN port of the P-320W v3. Turn on your computer and the P-320W v3.

Auto-discover Your UPnP-enabled Network Device

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

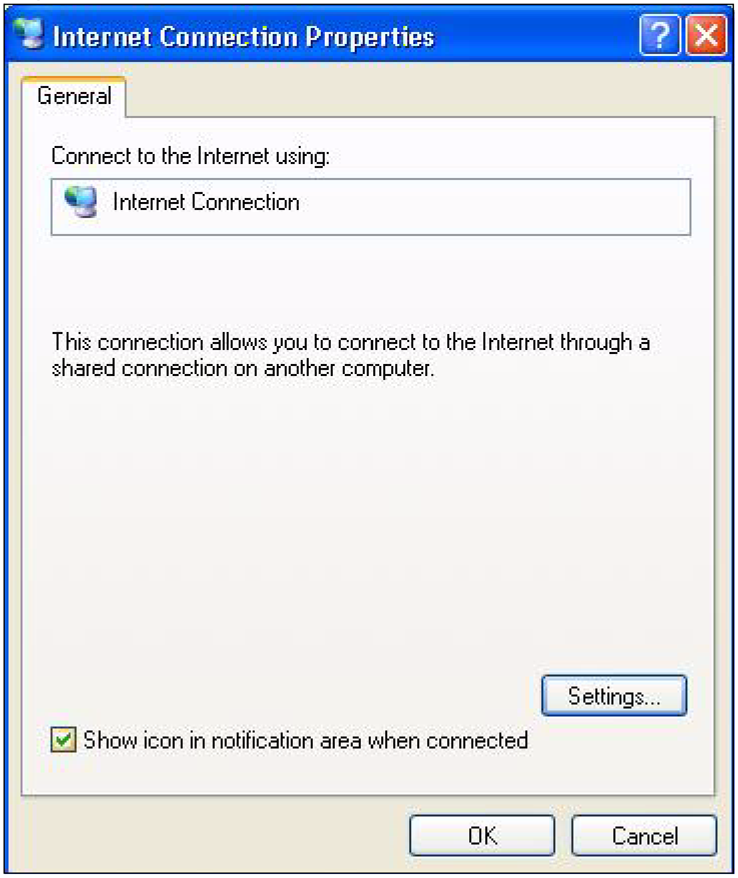
2 Right-click the icon and select **Properties**.

Figure 90 Network Connections



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

Figure 91 Internet Connection Properties



Connect to the Internet using:

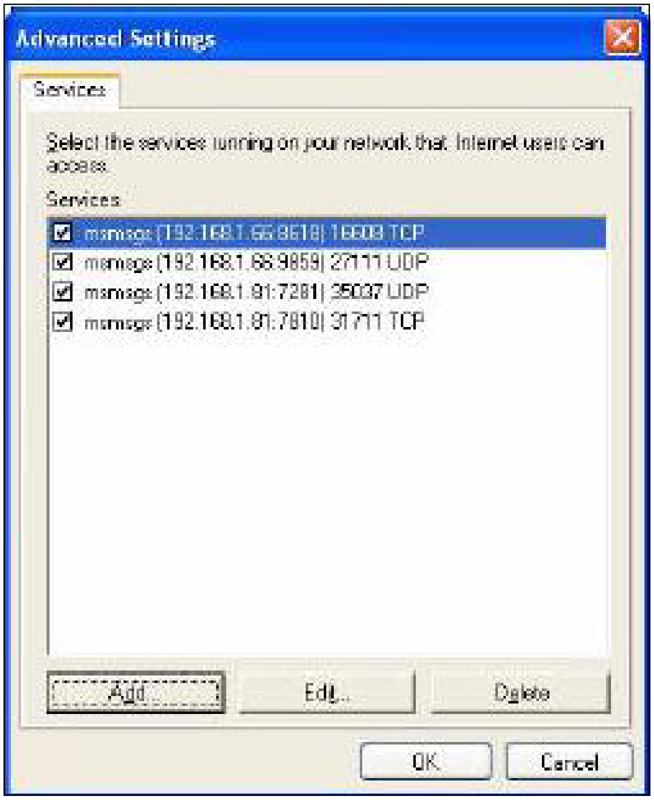
Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

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

Figure 92 Internet Connection Properties: Advanced Settings

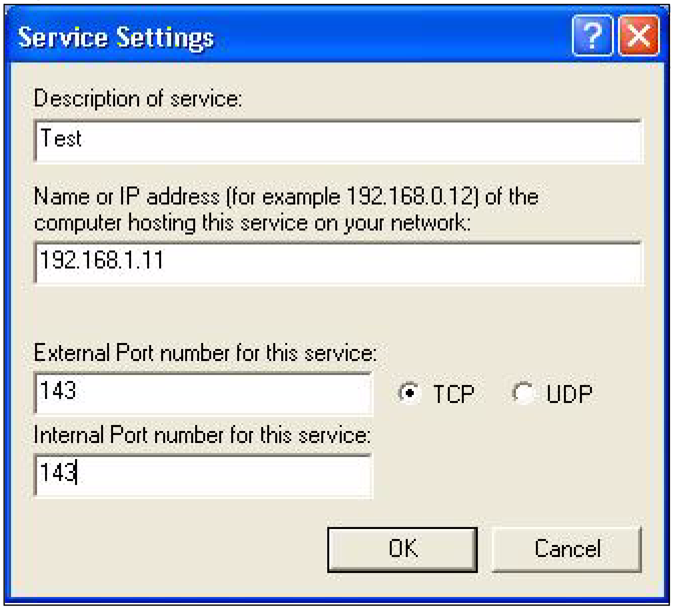


Select the services running on your network that Internet users can access.

Services

- ☑ msmsgs (192.168.1.66:8618) 16608 TCP
- ☑ msmsgs (192.168.1.66:9859) 27111 UDP
- ☑ msmsgs (192.168.1.81:7281) 35037 UDP
- ☑ msmsgs (192.168.1.81:7810) 31711 TCP

Figure 93 Internet Connection Properties: Advanced Settings: Add



Description of service:

Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:

192.168.1.11

External Port number for this service:

143 ● TCP ○ UDP

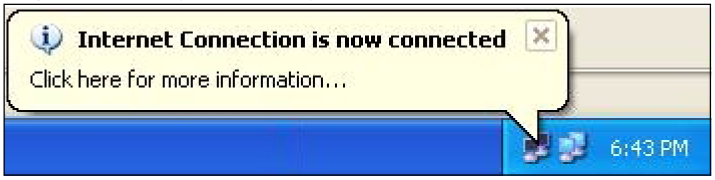
Internal Port number for this service:

143

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 94 System Tray Icon

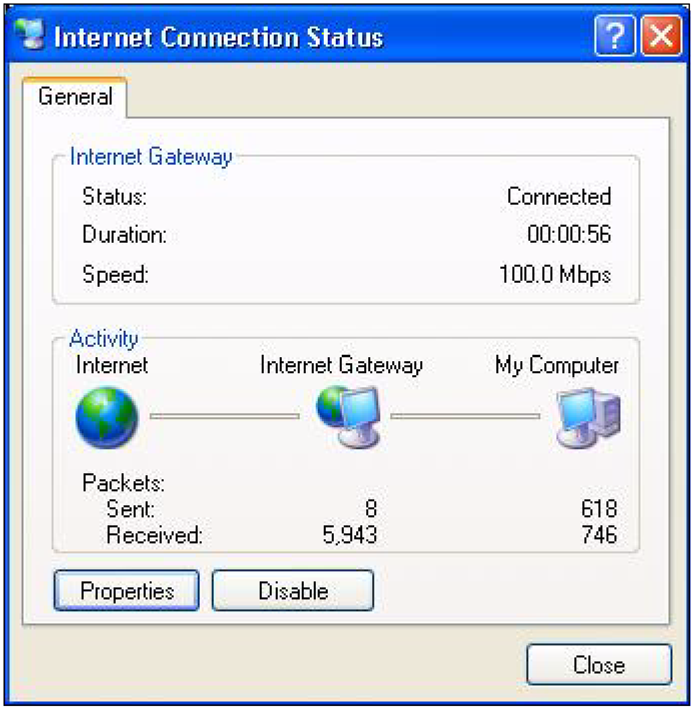


Internet Connection is now connected

Click here for more information...

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

Figure 95 Internet Connection Status



Internet Connection Status

Internet Gateway

Status:	Connected
Duration:	00:00:56
Speed:	100.0 Mbps

Activity

	Internet	Internet Gateway	My Computer
Packets:			
Sent:		8	618
Received:		5,943	746

Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the P-320W v3 without finding out the IP address of the P-320W v3 first. This comes helpful if you do not know the IP address of the P-320W v3.

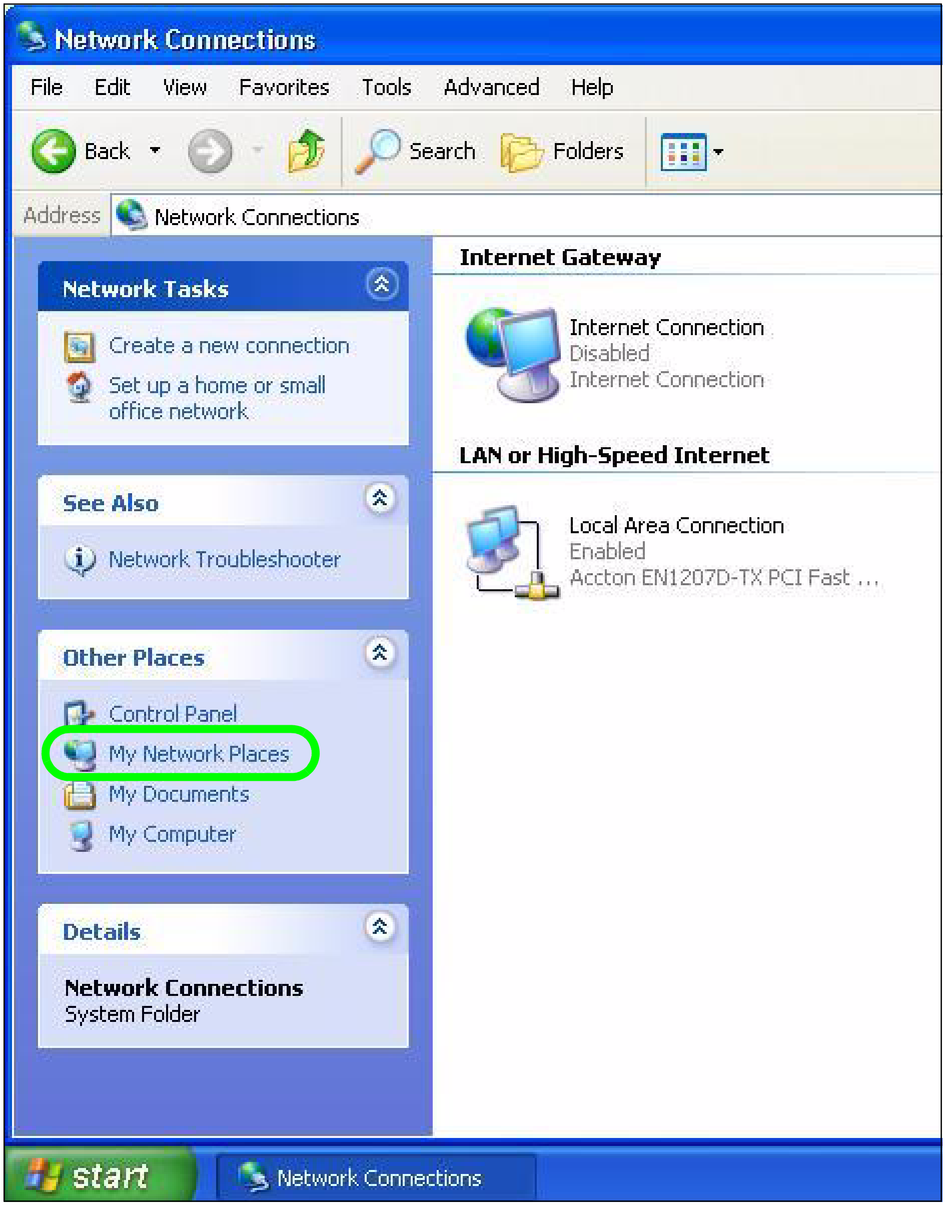
Follow the steps below to access the web configurator.

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

2 Double-click **Network Connections**.

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

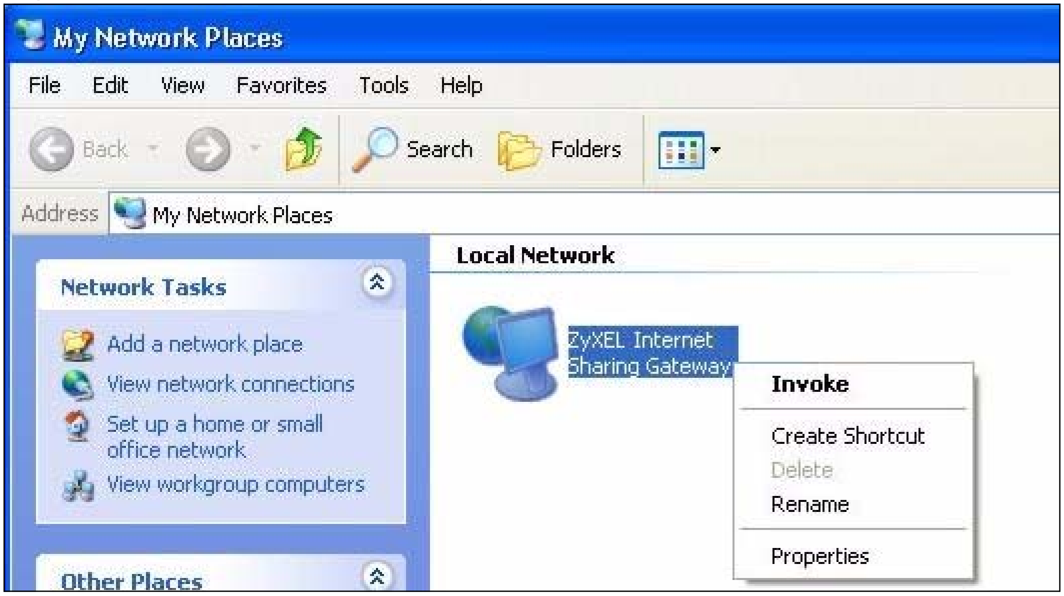
Figure 96 Network Connections



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

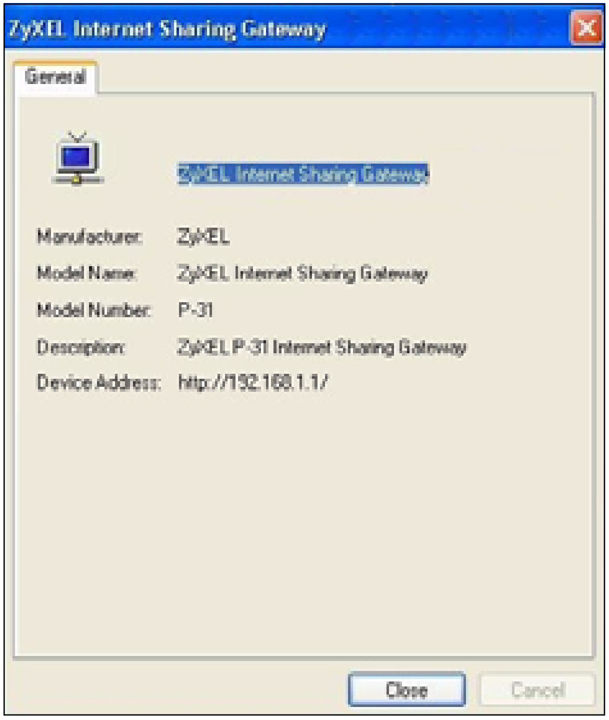
5 Right-click on the icon for your P-320W v3 and select **Invoke**. The web configurator login screen displays.

Figure 97 Network Connections: My Network Places



6 Right-click on the icon for your P-320W v3 and select **Properties**. A properties window displays with basic information about the P-320W v3.

Figure 98 Network Connections: My Network Places: Properties: Example



ZyXEL Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number: P-31

Description: ZyXEL P-31 Internet Sharing Gateway

Device Address: http://192.168.1.1/

PART V
Maintenance and Troubleshooting

17

System

17.1 Overview

This chapter provides information on the **System** screens.

See the chapter about wizard setup for more information on the next few screens.

17.2 What You Can Do

- Use the **General** screen (Section 17.4 on page 158) to identify the P-320W v3 in an Ethernet network.
- Use the **Dynamic DNS** screen (Section 17.5 on page 160) to change your P-320W v3's DDNS settings
- Use the **Time Setting** screen (Section 17.6 on page 161) to change your P-320W v3's time and date.

17.3 What You Need to Know

The following sections provide information that can be helpful in configuring the screens in this chapter.

17.3.1 Dynamic DNS Introduction

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.

17.3.2 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.

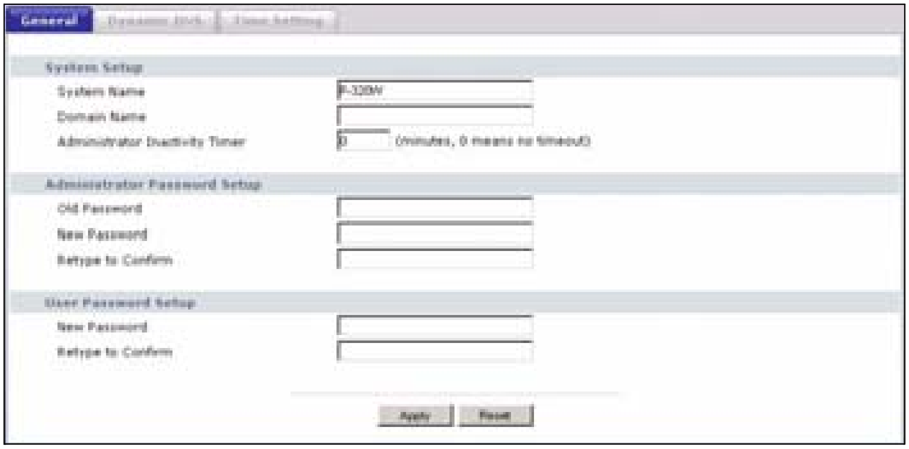
If you have a private WAN IP address, then you cannot use Dynamic DNS.

17.4 System General Screen

Use this screen to identify the P-320W v3 in an Ethernet network.

Click **Maintenance** > **System**. The following screen displays.

Figure 99 Maintenance > System > General



System Setup

System Name	P-320W
Domain Name	
Administrator Inactivity Timer	0 (minutes, 0 means no timeout)

Administrator Password Setup

Old Password	
New Password	
Retype to Confirm	

User Password Setup

New Password	
Retype to Confirm	

The following table describes the labels in this screen.

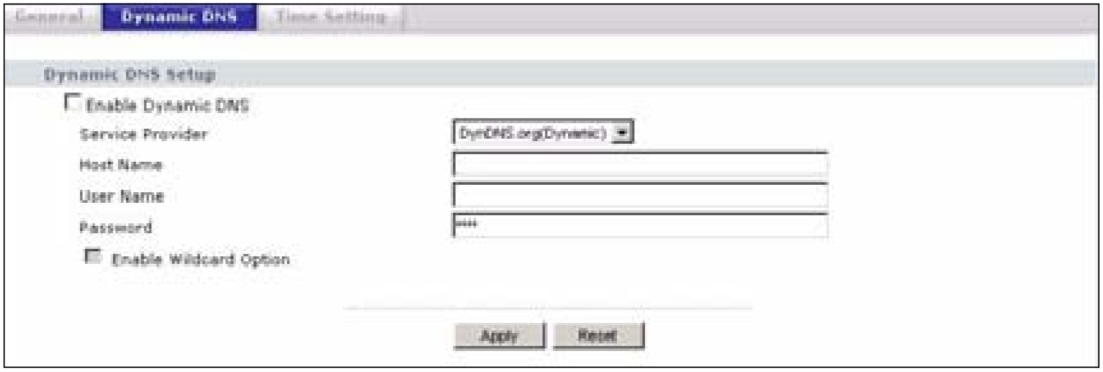
Table 59 Maintenance > System > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the P-320W v3 in an Ethernet network. It is recommended you enter your computer's "Computer name" in this field (see the chapter about wizard setup for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Administrator Password Setup Change the administrator's password using the fields as shown.	
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 an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
User Password Setup Change the user password using the fields as shown.	
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

17.5 Dynamic DNS Screen

To change your P-320W v3’s DDNS settings, click **Network > DDNS**. The screen appears as shown.

Figure 100 Dynamic DNS



Dynamic DNS Setup

□ Enable Dynamic DNS

Service Provider: DynDNS.org(Dynamic)

Host Name

User Name

Password: ****

□ Enable Wildcard Option

The following table describes the labels in this screen.

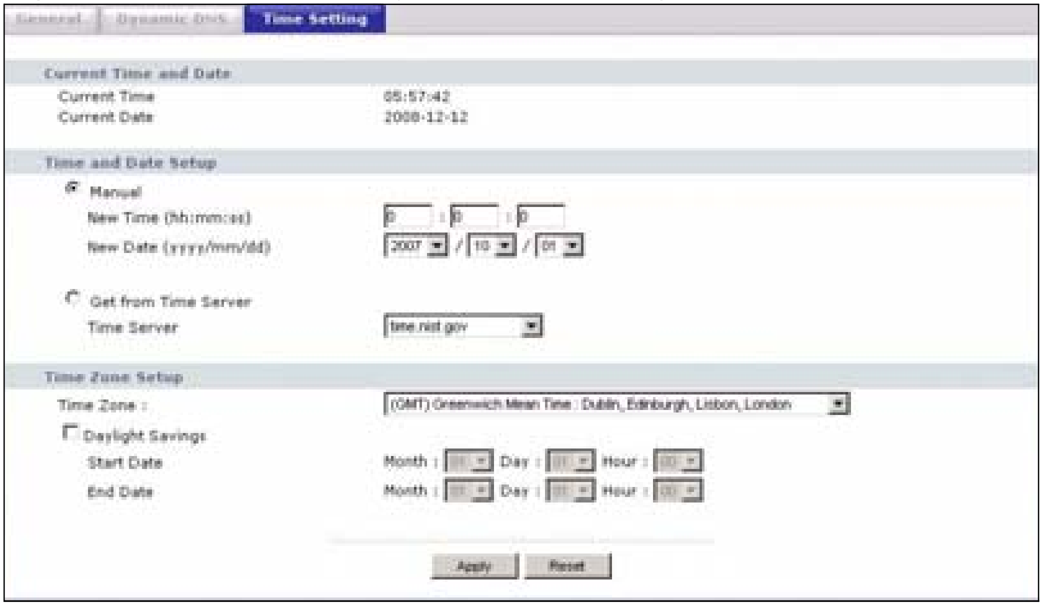
Table 60 Dynamic DNS

LABEL	DESCRIPTION
Enable Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Enter a host names in the field provided. You can specify up to two host names in the field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

17.6 Time Setting Screen

To change your P-320W v3's time and date, click **Maintenance** > **System** > **Time Setting**. The screen appears as shown. Use this screen to configure the P-320W v3's time based on your local time zone.

Figure 101 Maintenance > System > Time Setting



Current Time and Date

Current Time 05:57:42

Current Date 2008-12-12

Time and Date Setup

● Manual

New Time (hh:mm:ss) 0 : 0 : 0

New Date (yyyy/mm/dd) 2007 / 10 / 01

○ Get from Time Server

Time Server time.nist.gov

Time Zone Setup

Time Zone : (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

□ Daylight Savings

Start Date Month : 01 Day : 01 Hour : 00

End Date Month : 01 Day : 01 Hour : 00

The following table describes the labels in this screen.

Table 61 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your P-320W v3. Each time you reload this page, the P-320W v3 synchronizes the time with the time server.
Current Date	This field displays the date of your P-320W v3. Each time you reload this page, the P-320W v3 synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.

Table 61 Maintenance > System > Time Setting

LABEL	DESCRIPTION
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the P-320W v3 get the time and date from the time server you specified below.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **April** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Last**, **Sunday**, **October** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the P-320W v3.
Reset	Click **Reset** to begin configuring this screen afresh.

18

Logs

18.1 Overview

This chapter contains information about configuring general log settings and viewing the P-320W v3's logs.

Refer to the appendices for example log message explanations.

18.2 What You Can Do

- Use the **View Log** screen (Section 18.4 on page 164) to look at all of the P-320W v3's logs in one location.
- Use the **Log Settings** screen (Section 18.5 on page 165) to configure to where the P-320W v3 is to send logs and which logs and/or immediate alerts the P-320W v3 to send.

18.3 What You Need to Know

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen (Section 18.4 on page 164). Alerts display in red and logs display in black.

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

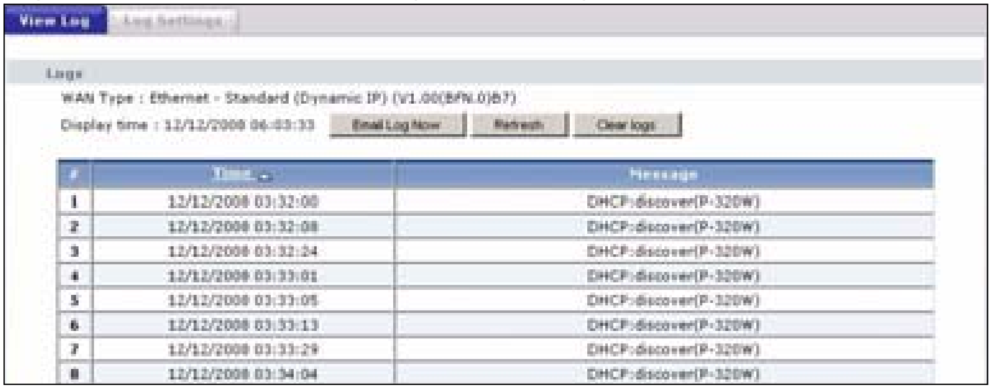
18.4 View Log Screen

Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 18.5 on page 165). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, Java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Click **Maintenance** > **Logs** to open the **View Log** screen.

Figure 102 Maintenance > Logs > View Log



WAN Type : Ethernet - Standard (Dynamic IP) (V1.00(BFN.0)B7)

Display time : 12/12/2008 06:03:33

#	Time	Message
1	12/12/2008 03:32:00	DHCP:discover(P-320W)
2	12/12/2008 03:32:08	DHCP:discover(P-320W)
3	12/12/2008 03:32:24	DHCP:discover(P-320W)
4	12/12/2008 03:33:01	DHCP:discover(P-320W)
5	12/12/2008 03:33:05	DHCP:discover(P-320W)
6	12/12/2008 03:33:13	DHCP:discover(P-320W)
7	12/12/2008 03:33:29	DHCP:discover(P-320W)
8	12/12/2008 03:34:04	DHCP:discover(P-320W)

The following table describes the labels in this screen.

Table 62 Maintenance > Logs > View Log

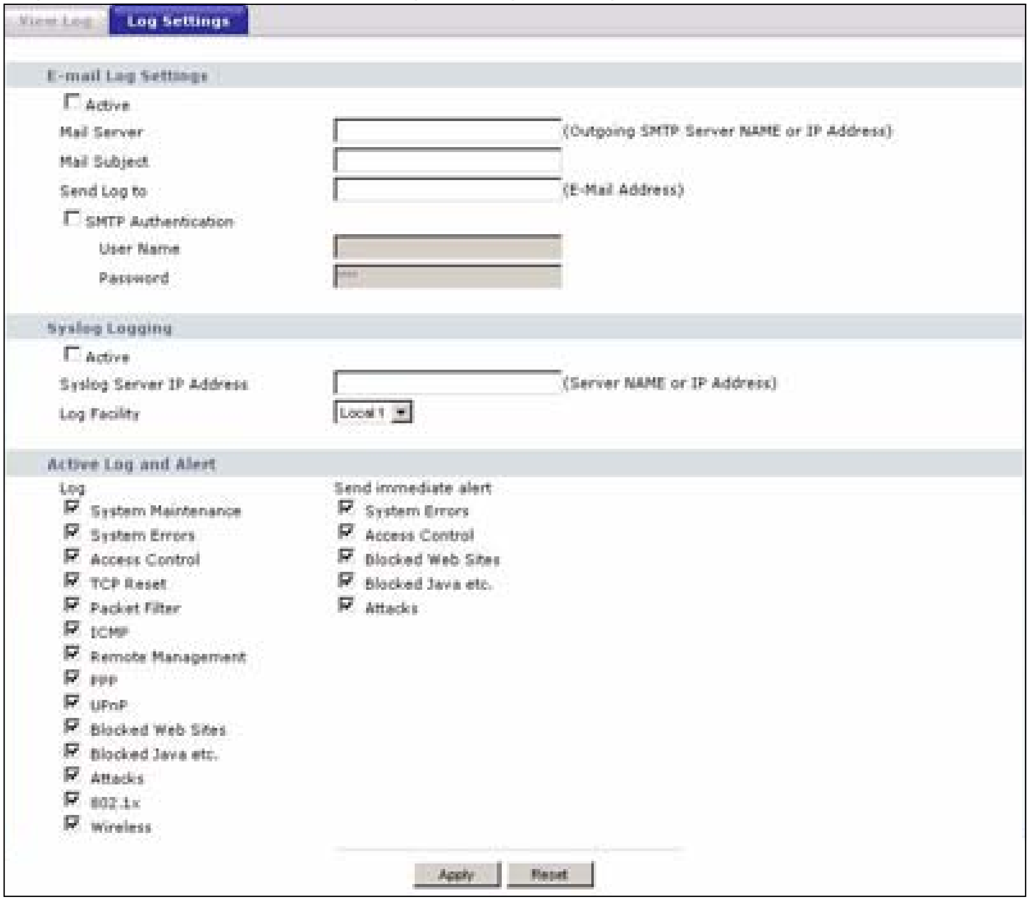
LABEL	DESCRIPTION
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**).
Refresh	Click **Refresh** to renew the log screen.
Clear logs	Click **Clear Log** to delete all the logs.
#	Number of an individual log.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the P-320W v3's time and date.
Message	This field states the reason for the log.

18.5 Log Settings Screen

Use this screen to configure to where the P-320W v3 is to send logs and which logs and/or immediate alerts the P-320W v3 to send.

Click **Maintenance** > **Logs** > **Log Settings** to open the **Log Settings** screen.

Figure 103 Maintenance > Logs > Log Settings



E-mail Log Settings

☐ Active

Mail Server (Outgoing SMTP Server NAME or IP Address)

Mail Subject

Send Log to (E-Mail Address)

☐ SMTP Authentication

User Name

Password

Syslog Logging

☐ Active

Syslog Server IP Address (Server NAME or IP Address)

Log Facility: Local 1

Active Log and Alert

Log	Send immediate alert
☑ System Maintenance	☑ System Errors
☑ System Errors	☑ Access Control
☑ Access Control	☑ Blocked Web Sites
☑ TCP Reset	☑ Blocked Java etc.
☑ Packet Filter	☑ Attacks
☑ ICMP	
☑ Remote Management	
☑ PPP	
☑ UPnP	
☑ Blocked Web Sites	
☑ Blocked Java etc.	
☑ Attacks	
☑ 802.1x	
☑ Wireless	

The following table describes the labels in this screen.

Table 63 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Active	Click **Active** to enable the log feature.
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the P-320W v3 sends. Not all P-320W v3 models have this field.

Table 63 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Send Log To	The P-320W v3 sends logs to the e-mail address specified in this field. If this field is left blank, the P-320W v3 does not send logs via e-mail.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Syslog Logging	The P-320W v3 sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the P-320W v3 to send E-mail alerts immediately.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

18.6 Technical Reference

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

18.6.1 Log Descriptions

This section provides descriptions of example log messages.

Table 64 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.

Table 64 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
`WAN interface gets IP:%s`	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns%s`	The DHCP server assigned an IP address to a client.
`Successful WEB login`	Someone has logged on to the router's web configurator interface.
`WEB login failed`	Someone has failed to log on to the router's web configurator interface.
`Successful TELNET login`	Someone has logged on to the router via telnet.
`TELNET login failed`	Someone has failed to log on to the router via telnet.
`Successful FTP login`	Someone has logged on to the router via ftp.
`FTP login failed`	Someone has failed to log on to the router via ftp.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`Starting Connectivity Monitor`	Starting Connectivity Monitor.
`Time initialized by Daytime Server`	The router got the time and date from the Daytime server.
`Time initialized by Time server`	The router got the time and date from the time server.
`Time initialized by NTP server`	The router got the time and date from the NTP server.
`Connect to Daytime server fail`	The router was not able to connect to the Daytime server.
`Connect to Time server fail`	The router was not able to connect to the Time server.
`Connect to NTP server fail`	The router was not able to connect to the NTP server.
`Too large ICMP packet has been dropped`	The router dropped an ICMP packet that was too large.
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	The router is saving configuration changes.
`Successful SSH login`	Someone has logged on to the router’s SSH server.
`SSH login failed`	Someone has failed to log on to the router’s SSH server.
`Successful HTTPS login`	Someone has logged on to the router's web configurator interface using HTTPS protocol.
`HTTPS login failed`	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

Table 65 System Error Logs

LOG MESSAGE	DESCRIPTION
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
`setNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`readNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`WAN connection is down.`	A WAN connection is down. You cannot access the network through this interface.

Table 66 Access Control Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
`Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
`Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Router sent blocked web site message: TCP`	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

Table 67 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
`Under SYN flood attack, sent TCP RST`	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
`Exceed TCP MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.

Table 67 TCP Reset Logs (continued)

LOG MESSAGE	DESCRIPTION
`Peer TCP state out of order, sent TCP RST`	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
`Firewall session time out, sent TCP RST`	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
`Exceed MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
`Access block, sent TCP RST`	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst").

Table 68 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
`[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set:%d, rule:%d)`	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

Table 69 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	ICMP access matched the default policy and was blocked or forwarded according to the user's setting. For type and code details, see Table 78 on page 175.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. For type and code details, see Table 78 on page 175.
`Triangle route packet forwarded: ICMP`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Unsupported/out-of-order ICMP: ICMP`	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 70 CDR Logs

LOG MESSAGE	DESCRIPTION
`board%d line%d channel%d, call%d,%s C01 Outgoing Call dev=%x ch=%x%s`	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID.For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
`board%d line%d channel%d, call%d,%s C02 OutCall Connected%d%s`	The PPPoE, PPTP or dial-up call is connected.
`board%d line%d channel%d, call%d,%s C02 Call Terminated`	The PPPoE, PPTP or dial-up call was disconnected.

Table 71 PPP Logs

LOG MESSAGE	DESCRIPTION
`ppp:LCP Starting`	The PPP connection's Link Control Protocol stage has started.
`ppp:LCP Opening`	The PPP connection's Link Control Protocol stage is opening.
`ppp:CHAP Opening`	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
`ppp:IPCP Starting`	The PPP connection's Internet Protocol Control Protocol stage is starting.

Table 71 PPP Logs (continued)

LOG MESSAGE	DESCRIPTION
`ppp:IPCP Opening`	The PPP connection’s Internet Protocol Control Protocol stage is opening.
`ppp:LCP Closing`	The PPP connection’s Link Control Protocol stage is closing.
`ppp:IPCP Closing`	The PPP connection’s Internet Protocol Control Protocol stage is closing.

Table 72 UPnP Logs

LOG MESSAGE	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

Table 73 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
`%s: Keyword blocking`	The content of a requested web page matched a user defined keyword.
`%s: Not in trusted web list`	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
`%s: Forbidden Web site`	The web site is in the forbidden web site list.
`%s: Contains ActiveX`	The web site contains ActiveX.
`%s: Contains Java applet`	The web site contains a Java applet.
`%s: Contains cookie`	The web site contains a cookie.
`%s: Proxy mode detected`	The router detected proxy mode in the packet.
`%s`	The content filter server responded that the web site is in the blocked category list, but it did not return the category type.
`%s:%s`	The content filter server responded that the web site is in the blocked category list, and returned the category type.
`%s(cache hit)`	The system detected that the web site is in the blocked list from the local cache, but does not know the category type.
`%s:%s(cache hit)`	The system detected that the web site is in blocked list from the local cache, and knows the category type.
`%s: Trusted Web site`	The web site is in a trusted domain.
`%s`	When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site” check box, the system forwards the web content.
`Waiting content filter server timeout`	The external content filtering server did not respond within the timeout period.
`DNS resolving failed`	The P-320W v3 cannot get the IP address of the external content filtering via DNS query.
`Creating socket failed`	The P-320W v3 cannot issue a query because TCP/IP socket creation failed, port:port number.

Table 73 Content Filtering Logs (continued)

LOG MESSAGE	DESCRIPTION
`Connecting to content filter server fail`	The connection to the external content filtering server failed.
`License key is invalid`	The external content filtering license key is invalid.

Table 74 Attack Logs

LOG MESSAGE	DESCRIPTION
`attack [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
`attack ICMP (type:%d, code:%d)`	The firewall detected an ICMP attack. For type and code details, see Table 78 on page 175.
`land [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
`land ICMP (type:%d, code:%d)`	The firewall detected an ICMP land attack. For type and code details, see Table 78 on page 175.
`ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall detected an IP spoofing attack on the WAN port.
`ip spoofing - WAN ICMP (type:%d, code:%d)`	The firewall detected an ICMP IP spoofing attack on the WAN port. For type and code details, see Table 78 on page 175.
`icmp echo: ICMP (type:%d, code:%d)`	The firewall detected an ICMP echo attack. For type and code details, see Table 78 on page 175.
`syn flood TCP`	The firewall detected a TCP syn flood attack.
`ports scan TCP`	The firewall detected a TCP port scan attack.
`teardrop TCP`	The firewall detected a TCP teardrop attack.
`teardrop UDP`	The firewall detected an UDP teardrop attack.
`teardrop ICMP (type:%d, code:%d)`	The firewall detected an ICMP teardrop attack. For type and code details, see Table 78 on page 175.
`illegal command TCP`	The firewall detected a TCP illegal command attack.
`NetBIOS TCP`	The firewall detected a TCP NetBIOS attack.
`ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall classified a packet with no source routing entry as an IP spoofing attack.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack. For type and code details, see Table 78 on page 175.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack. For type and code details, see Table 78 on page 175.

Table 75 PKI Logs

LOG MESSAGE	DESCRIPTION
`Enrollment successful`	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
`Enrollment failed`	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <SCEP CA server url>`	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
`Enrollment successful`	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.
`Enrollment failed`	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <CMP CA server url>`	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
`Rcvd ca cert: <subject name>`	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd user cert: <subject name>`	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd CRL <size>: <issuer name>`	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd ARL <size>: <issuer name>`	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ca cert`	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received user cert`	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received CRL`	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ARL`	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Rcvd data <size> too large! Max size allowed: <max size>`	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.

Table 75 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Cert trusted: <subject name>`	The router has verified the path of the certificate with the listed subject name.
`Due to <reason codes>, cert not trusted: <subject name>`	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 78 on page 175 for the corresponding descriptions of the codes.

Table 76 802.1X Logs

LOG MESSAGE	DESCRIPTION
`Local User Database accepts user.`	A user was authenticated by the local user database.
`Local User Database reports user credential error.`	A user was not authenticated by the local user database because of an incorrect user password.
`` Local User Database does not find user`s credential. ``	A user was not authenticated by the local user database because the user is not listed in the local user database.
`RADIUS accepts user.`	A user was authenticated by the RADIUS Server.
`RADIUS rejects user. Pls check RADIUS Server.`	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
`Local User Database does not support authentication method.`	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
`User logout because of session timeout expired.`	The router logged out a user whose session expired.
`User logout because of user deassociation.`	The router logged out a user who ended the session.
`User logout because of no authentication response from user.`	The router logged out a user from which there was no authentication response.
`User logout because of idle timeout expired.`	The router logged out a user whose idle timeout period expired.
`User logout because of user request.`	A user logged out.
`Local User Database does not support authentication method.`	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
`No response from RADIUS. Pls check RADIUS Server.`	There is no response message from the RADIUS server, please check the RADIUS server.
`Use Local User Database to authenticate user.`	The local user database is operating as the authentication server.
`Use RADIUS to authenticate user.`	The RADIUS server is operating as the authentication server.

Table 76 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
`No Server to authenticate user.`	There is no authentication server to authenticate a user.
`Local User Database does not find user`s credential.`	A user was not authenticated by the local user database because the user is not listed in the local user database.

Table 77 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(L to L/P)	LAN to LAN/P-320W v3	ACL set for packets traveling from the LAN to the LAN or the P-320W v3.
(W to W/P)	WAN to WAN/P-320W v3	ACL set for packets traveling from the WAN to the WAN or the P-320W v3.

Table 78 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host

Table 78 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 79 Syslog Logs

LOG MESSAGE	DESCRIPTION
`<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>`	"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 80 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate

Table 80 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
`CER_REQ`	Certificate Request
`HASH`	Hash
`SIG`	Signature
`NONCE`	Nonce
`NOTFY`	Notification
`DEL`	Delete
`VID`	Vendor ID

19

Tools

19.1 Overview

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the P-320W v3.

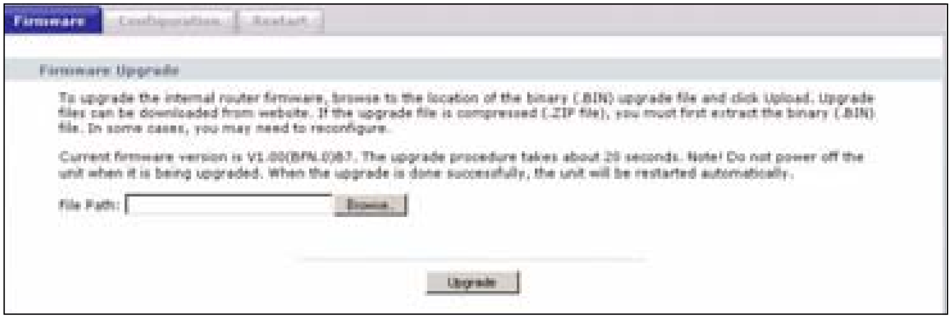
19.2 What You Can Do

- Use the **Firmware** screen (Section 19.3 on page 179) to upload a new firmware to your P-320W v3.
- Use the **Configuration** screen (Section 19.4 on page 181) to backup or restore a configuration file to your P-320W v3. You can also reset the P-320W v3 to its factory default settings.
- Use the **Restart** screen (Section 19.5 on page 183) to reboot your P-320W v3.

19.3 Firmware Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "P-320W v3.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the Firmware and Configuration File Maintenance chapter for upgrading firmware using FTP/TFTP commands.

Click **Maintenance > Tools**. Follow the instructions in this screen to upload firmware to your P-320W v3.



Firmware Upgrade

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.

Current firmware version is V1.00(BFN.0)B7. The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically.

File Path:

Figure 104 Maintenance > Tools > Firmware

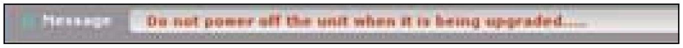
The following table describes the labels in this screen.

Table 81 Maintenance > Tools > Firmware

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

Note: Do not turn off the P-320W v3 while firmware upload is in progress!

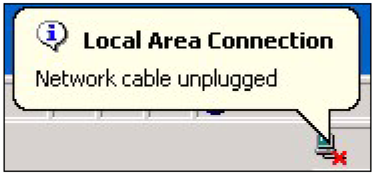
Wait two minutes before logging into the P-320W v3 again.



Do not power off the unit when it is being upgraded....

Figure 105 Upload Warning

The P-320W v3 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.



Local Area Connection

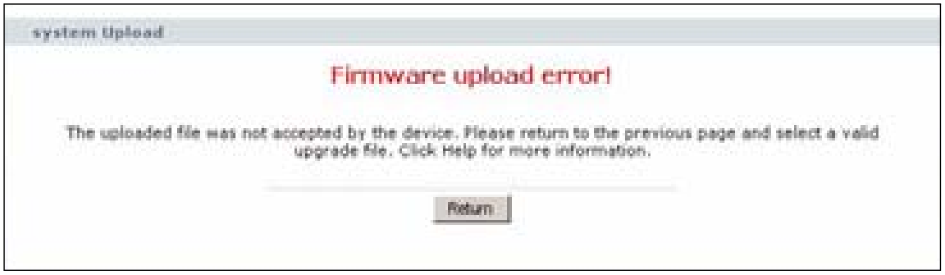
Network cable unplugged

Figure 106 Network Temporarily Disconnected

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

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

Figure 107 Upload Error Message



system Upload

Firmware upload error!

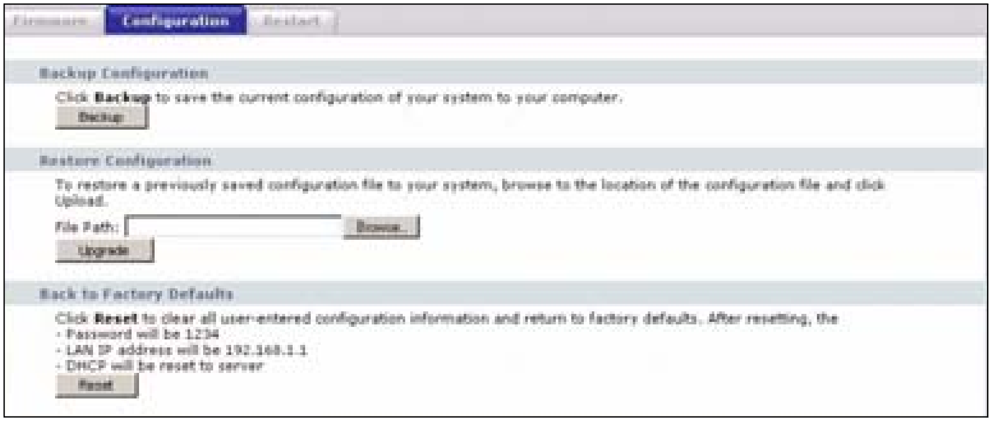
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.

19.4 Configuration Screen

Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Click **Maintenance > Tools** > **Configuration**.

Figure 108 Maintenance > Tools > Configuration



Backup Configuration

Click **Backup** to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path:

Back to Factory Defaults

Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

19.4.1 Backup Configuration

Backup configuration allows you to back up (save) the P-320W v3’s current configuration to a file on your computer. Once your P-320W v3 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-320W v3’s current configuration to your computer.

19.4.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your P-320W v3.

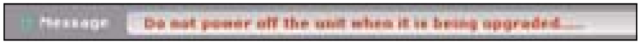
Table 82 Maintenance Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **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.

Note: Do not turn off the P-320W v3 while configuration file upload is in progress

After you see the following message in the screen, you must then wait one minute before logging into the P-320W v3 again.

Figure 109 Configuration Restore Successful



Do not power off the unit when it is being upgraded...

The P-320W v3 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 110 Temporarily Disconnected

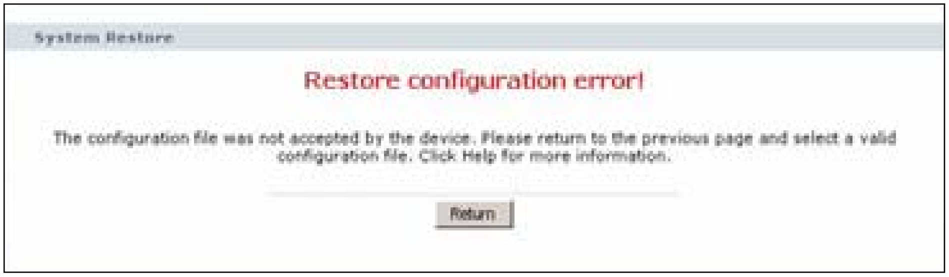
Local Area Connection

Network cable unplugged

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 P-320W v3 IP address (192.168.1.1). See Appendix C on page 217 for details on how to set up your computer's IP address.

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

Figure 111 Configuration Restore Error



System Restore

Restore configuration error!

The configuration file was not accepted by the device. Please return to the previous page and select a valid configuration file. Click Help for more information.

19.4.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the P-320W v3 to its factory defaults.

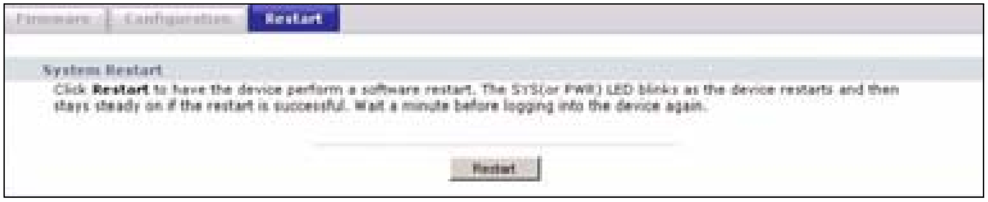
You can also press the **RESET** button on the rear panel to reset the factory defaults of your P-320W v3. Refer to the chapter about introducing the web configurator for more information on the **RESET** button.

19.5 Restart Screen

System restart allows you to reboot the P-320W v3 without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the P-320W v3 reboot. This does not affect the P-320W v3's configuration.

Figure 112 Maintenance > Tools > Restart



System Restart

Click **Restart** to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.

20

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-320W v3 Access and Login
- Internet Access
- Resetting the P-320W v3 to Its Factory Defaults
- Wireless Router Troubleshooting
- Advanced Features

20.1 Power, Hardware Connections, and LEDs

The P-320W v3 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the P-320W v3.
2. Make sure the power adaptor or cord is connected to the P-320W v3 and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the P-320W v3.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.4 on page 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 Disconnect and re-connect the power adaptor to the P-320W v3.

5 If the problem continues, contact the vendor.

20.2 P-320W v3 Access and Login

I don't know the IP address of my P-320W v3.

1 The default IP address is **192.168.1.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the P-320W v3 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-320W v3 (it depends on the network), so enter this IP address in your Internet browser. Login (see the Quick Start Guide for instructions) and go to the **Device Information** table in the **Status** screen. Your P-320W v3's IP address is available in the **Device Information** table.

If the **DHCP** setting under **LAN information** is **Enabled**. The P-320W v3 is a DHCP server on LAN.

3 If your P-320W v3 is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.

4 Reset your P-320W v3 to change all settings back to their default. This means your current settings are lost. See Section 20.4 on page 189 in the **Troubleshooting** for information on resetting your P-320W v3.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 20.4 on page 189.

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

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section 7.3 on page 102), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my P-320W v3.

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 A on page 199.

4 Make sure your computer is in the same subnet as the P-320W v3. (If you know that there are routers between your computer and the P-320W v3, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 7.3 on page 102.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the P-320W v3. See Section 7.3 on page 102.

5 Reset the device to its factory defaults, and try to access the P-320W v3 with the default IP address. See Section 7.3 on page 102.

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

Advanced Suggestions

- Try to access the P-320W v3 using another service, such as Telnet. If you can access the P-320W v3, check the remote management settings and firewall rules to find out why the P-320W v3 does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN**/**ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the P-320W v3.

1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the P-320W v3. Log out of the P-320W v3 in the other session, or ask the person who is logged in to log out.

3 Disconnect and re-connect the power adaptor or cord to the P-320W v3.

4 If this does not work, you have to reset the device to its factory defaults. See Section 20.4 on page 189.

20.3 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.

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

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

4 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 anymore. I had access to the Internet (with the P-320W v3), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.4 on page 23.

2 Reboot the P-320W v3.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.4 on page 23. If the P-320W v3 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 the P-320W v3 closer to the AP 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 Reboot the P-320W v3.

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

Advanced Suggestions

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.
- 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.

20.4 Resetting the P-320W v3 to Its Factory Defaults

If you reset the P-320W v3, you lose all of the changes you have made. The P-320W v3 re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the P-320W v3,

1 Make sure the **power LED** is on and not blinking.

2 Press and hold the **RESET** button for five to ten seconds. The default settings have been restored.

If the P-320W v3 restarts automatically, wait for the P-320W v3 to finish restarting, and log in to the web configurator. The password is "1234".

If the P-320W v3 does not restart automatically, disconnect and reconnect the P-320W v3's power. Then, follow the directions above again.

20.5 Wireless Router Troubleshooting

I cannot access the P-320W v3 or ping any computer from the WLAN (wireless router).

1 Make sure the wireless LAN is enabled on the P-320W v3

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-320W v3.

4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the P-320W v3.

5 Check that both the P-320W v3 and your wireless station are using the same wireless and wireless security settings.

6 Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the P-320W v3.

7 Make sure you allow the P-320W v3 to be remotely accessed through the WLAN interface. Check your remote management settings.

- See the chapter on Wireless LAN in the User's Guide for more information.

20.6 Advanced Features

I set up URL keyword blocking, but I can still access a website that should be blocked.

Make sure that you select the **Enable URL Keyword Blocking** check box in the Content Filtering screen. Make sure that the keywords that you type are listed in the **Keyword List**.

If a keyword that is listed in the **Keyword List** is not blocked when it is found in a URL, customize the keyword blocking using commands. See the Customizing Keyword Blocking URL Checking section in the Content Filter chapter.

21

Product Specifications

The following tables summarize the P-320W v3’s hardware and firmware features.

Table 83 Hardware Features

Dimensions (W x D x H)	162 x 115 x 33 mm
Weight	248 g
Power Specification	Input: 120~240 AC, 50~60 Hz Output: 5 V AC 1 A
Ethernet ports	Auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
4-5 Port Switch	A combination of switch and router makes your P-320W v3 a cost-effective and viable network solution. You can add up to four computers to the P-320W v3 without the cost of a hub when connecting to the Internet through the WAN port. You can add up to five computers to the P-320W v3 when you connect to the Internet in AP mode. Add more than four computers to your LAN by using a hub.
LEDs	PWR, LAN1-4, WAN, WLAN, WPS
Reset Button	The reset button is built into the rear panel. Use this button to restore the P-320W v3 to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings.
Antenna	The P-320W v3 is equipped with a 2dBi detachable antenna to provide clear radio transmission and reception on the wireless network.
Operation Environment	Temperature: 0º C ~ 40º C Humidity: 20% ~ 80% RH (Non-condensing)
Storage Environment	Temperature: -20º C ~ 70º C Humidity: 20% ~ 90% RH (Non-condensing)

Table 84 Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.33 to 192.168.1.64
Wireless Interface	Wireless LAN
Default Wireless SSID	Wireless LAN: ZyXEL
Default Wireless IP Address	Wireless LAN: Same as LAN (192.168.1.1)
Default Wireless Subnet Mask	Wireless LAN: Same as LAN (255.255.255.0)
Default Wireless DHCP Pool Size	Wireless LAN: Same as LAN (32 from 192.168.1.33 to 192.168.1.64)
Device Management	Use the web configurator to easily configure the rich range of features on the P-320W v3.
Wireless Functionality	Allows IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the P-320W v3 wirelessly. Enable wireless security (WEP, WPA, WPA-PSK) and/or MAC filtering to protect your wireless network. Note: The P-320W v3 may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator to put it on the P-320W v3. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the P-320W v3's configuration and put it back on the P-320W v3 later if you decide you want to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert a single public IP address to multiple private IP addresses for the computers on your network.
Firewall	You can configure firewall on the P-320W v3 for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.

Table 84 Firmware Features

FEATURE	DESCRIPTION
Content Filter	The P-320W v3 blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering. You can also subscribe to category-based content filtering that allows your P-320W v3 to check web sites against an external database.
Time and Date	Get the current time and date from an external server when you turn on your P-320W v3. You can also set the time manually. These dates and times are then used in logs.
Port Forwarding	If you have a server (mail or web server for example) on your network, then use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the P-320W v3 assign IP addresses, an IP default gateway and DNS servers to computers on your network.
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.
Logging	Use logs for troubleshooting.
PPPoE	PPPoE mimics a dial-up over Ethernet Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The P-320W v3 supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	The P-320W v3 can communicate with other UPnP enabled devices in a network.

PART VI
Appendices and Index

A

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

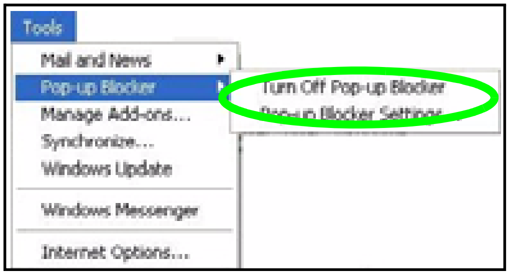
You may have to disable pop-up blocking to log into your device.

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 113 Pop-up Blocker

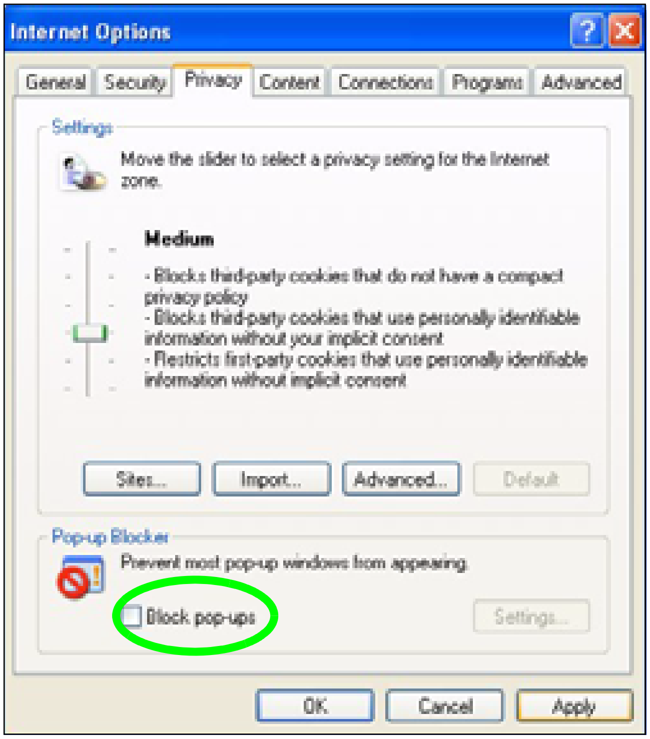


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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 114 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

☐ Block pop-ups

3 Click **Apply** to save this setting.

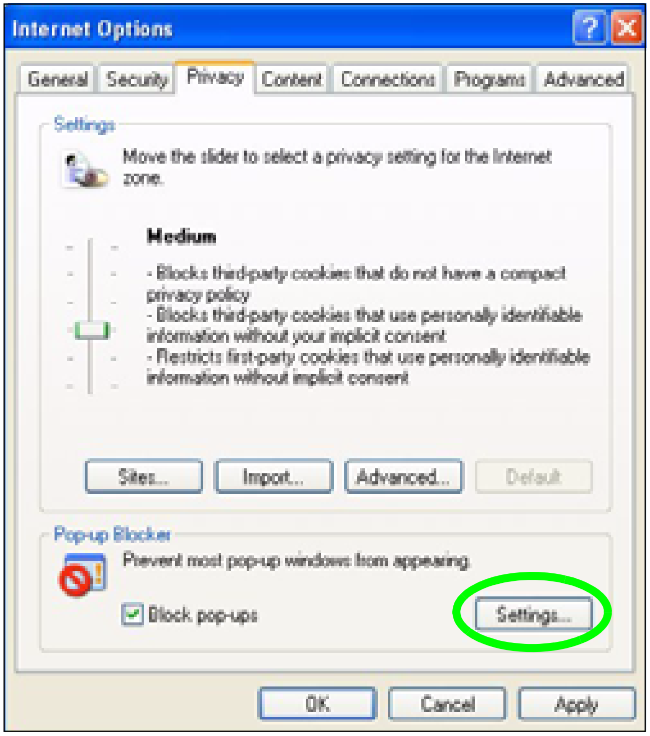
Enable pop-up Blockers with Exceptions

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 115 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

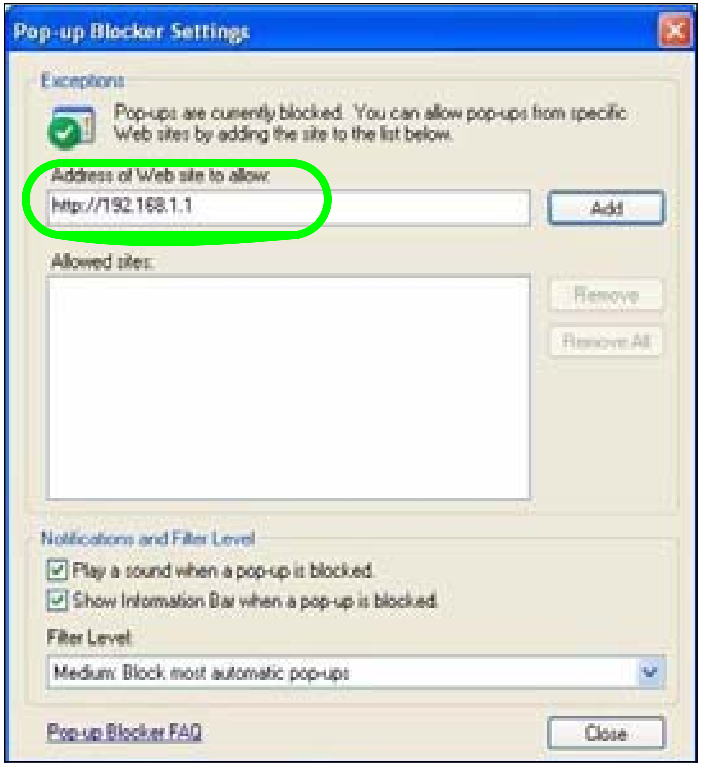
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 116 Pop-up Blocker Settings



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow:

http://192.168.1.1

Allowed sites:

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level:

Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

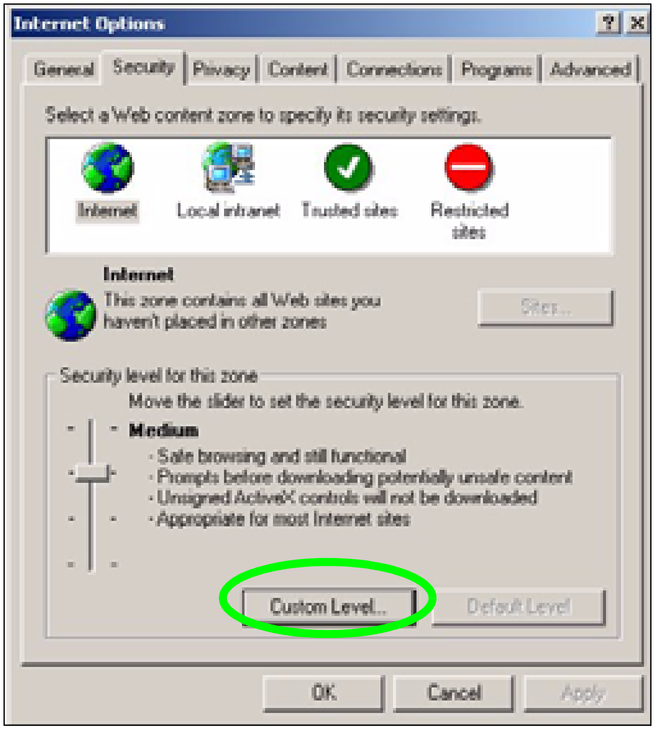
6 Click **Apply** to save this setting.

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 117 Internet Options: Security



Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Move the slider to set the security level for this zone.

Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

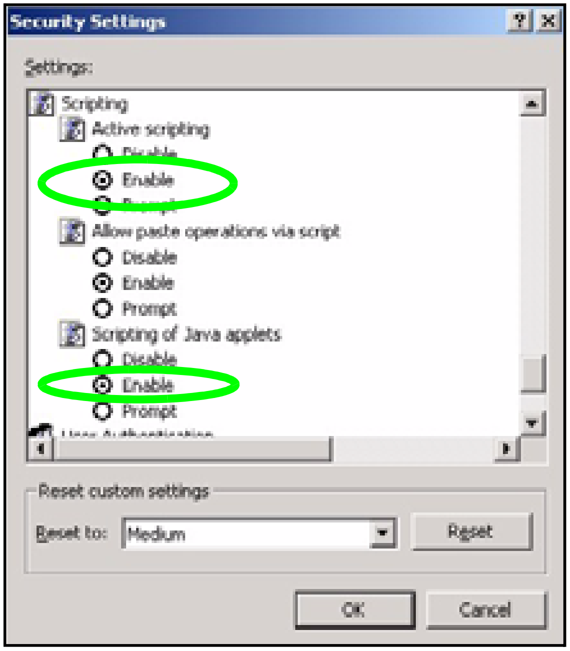
3 Scroll down to **Scripting**.

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 118 Security Settings - Java Scripting



Scripting
Active scripting
○ Disable
● Enable
○ Prompt
Allow paste operations via script
○ Disable
● Enable
○ Prompt
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication

Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

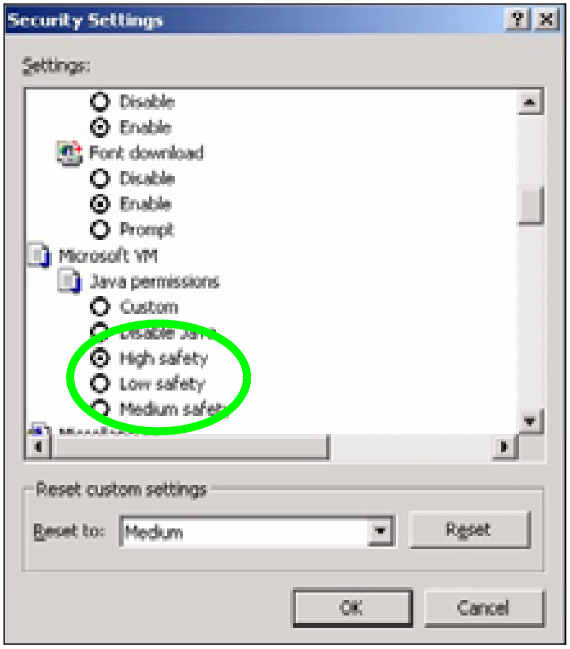
2 Click the **Custom Level...** button.

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 119 Security Settings - Java



Security Settings

Settings:

○ Disable
● Enable
Font download
○ Disable
● Enable
○ Prompt
Microsoft VM
Java permissions
○ Custom
○ Disable Java
● High safety
○ Low safety
○ Medium safety

Reset custom settings

Reset to: Medium

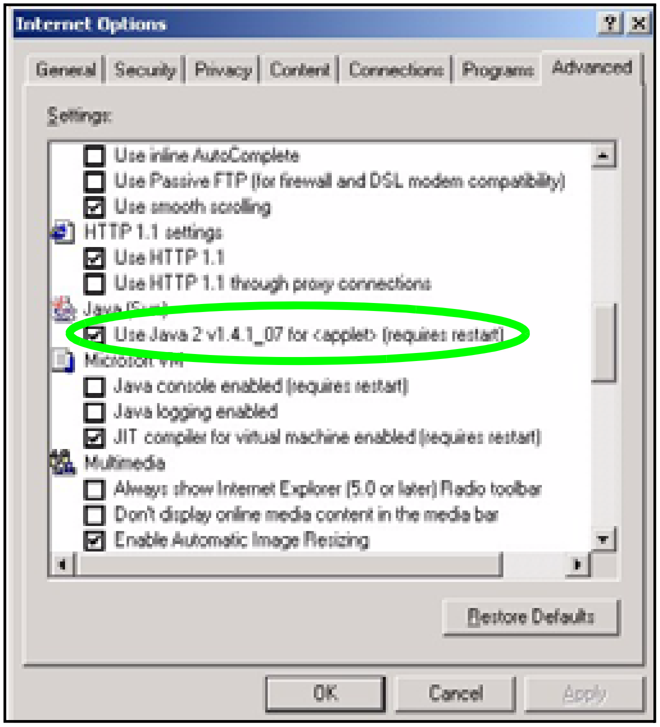
JAVA (Sun)

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 120 Java (Sun)



Internet Options

Settings:

- □ Use inline AutoComplete
- □ Use Passive FTP (for firewall and DSL modem compatibility)
- ☑ Use smooth scrolling

HTTP 1.1 settings

- ☑ Use HTTP 1.1
- □ Use HTTP 1.1 through proxy connections

Java (Sun)

- ☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)

Microsoft VM

- □ Java console enabled (requires restart)
- □ Java logging enabled
- ☑ JIT compiler for virtual machine enabled (requires restart)

Multimedia

- □ Always show Internet Explorer (5.0 or later) Radio toolbar
- □ Don't display online media content in the media bar
- ☑ Enable Automatic Image Resizing

B

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

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

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

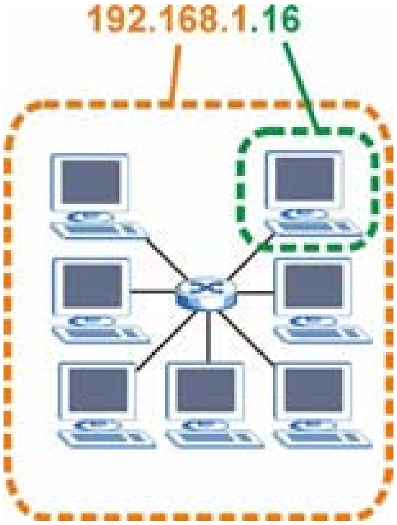
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 121 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 85 Subnet Mask - Identifying Network Number

	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

Table 85 Subnet Mask - Identifying Network Number

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
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 86 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 87 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 88 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

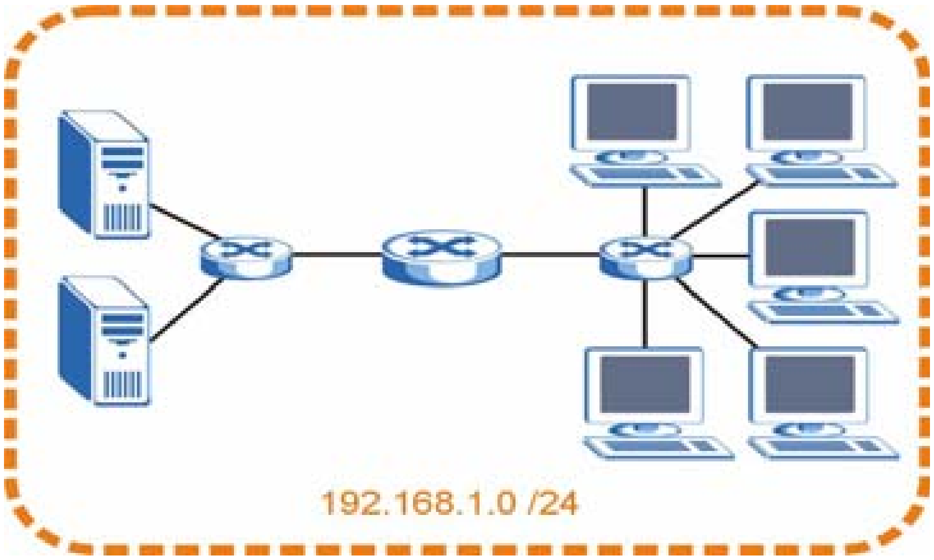
Subnetting

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 122 Subnetting Example: Before Subnetting

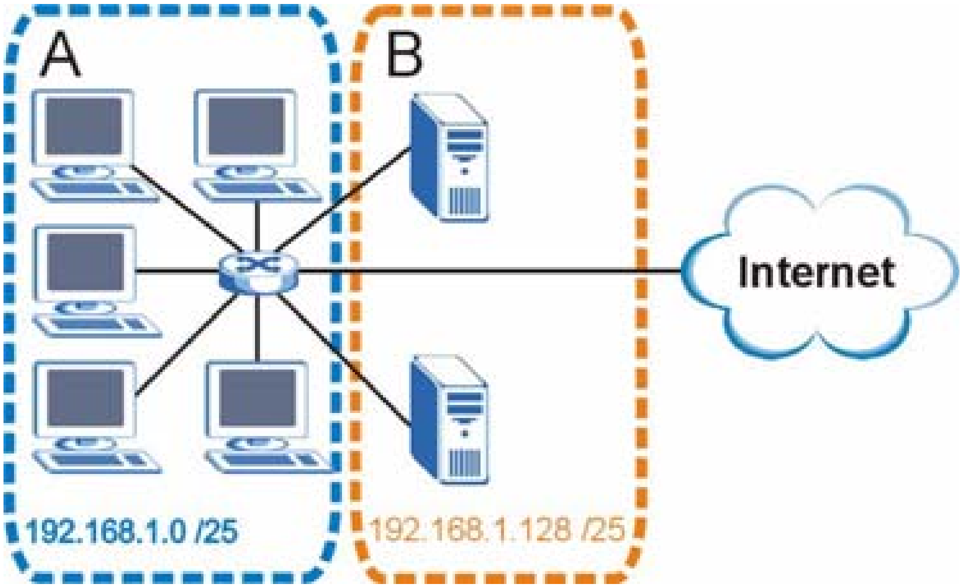


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 123 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 89 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 90 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 91 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 92 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

Table 92 Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
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 93 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 94 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 95 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-320W v3.

Once you have decided on the network number, pick an IP address for your P-320W v3 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-320W v3 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-320W v3 unless you are instructed to do otherwise.

Private IP Addresses

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

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

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

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

C

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

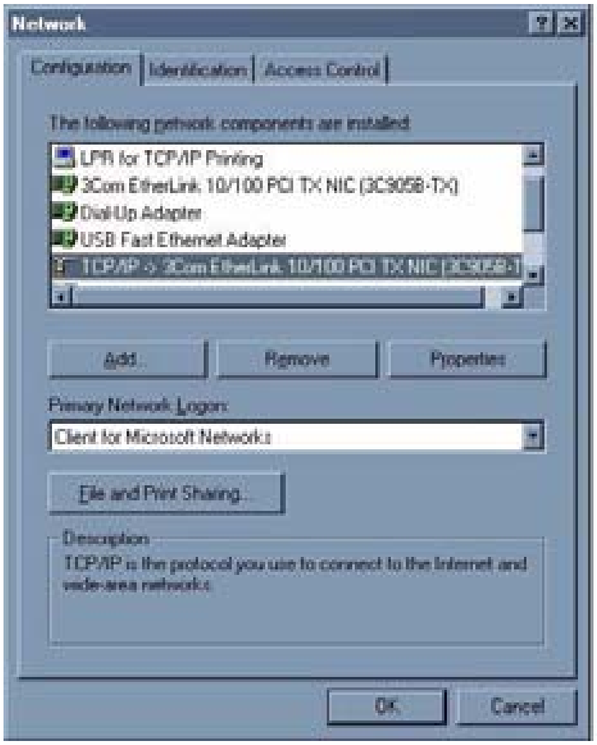
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 124 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

- LPR for TCP/IP Printing
- 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
- Dial-Up Adapter
- USB Fast Ethernet Adapter
- TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon:

Client for Microsoft Networks

Description

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.

2 Select **Adapter** and then click **Add**.

3 Select the manufacturer and model of your network adapter and then click **OK.**

If you need TCP/IP:

1 In the **Network** window, click **Add**.

2 Select **Protocol** and then click **Add**.

3 Select **Microsoft** from the list of **manufacturers**.

4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

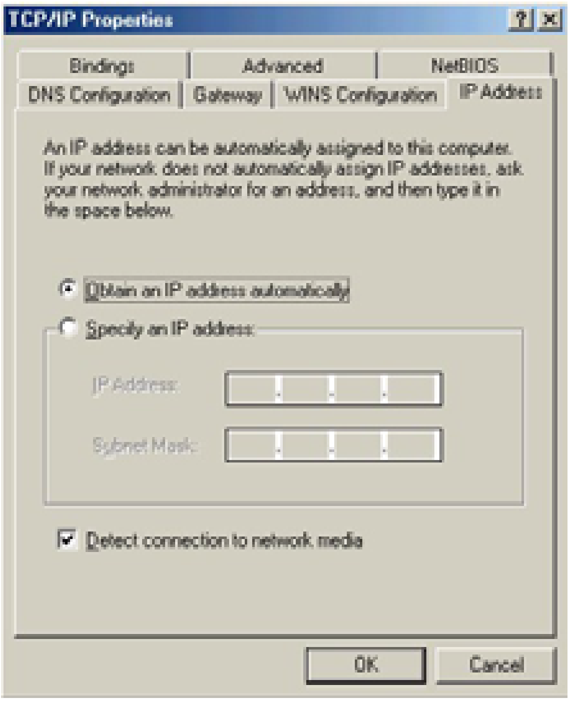
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 125 Windows 95/98/Me: TCP/IP Properties: IP Address



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

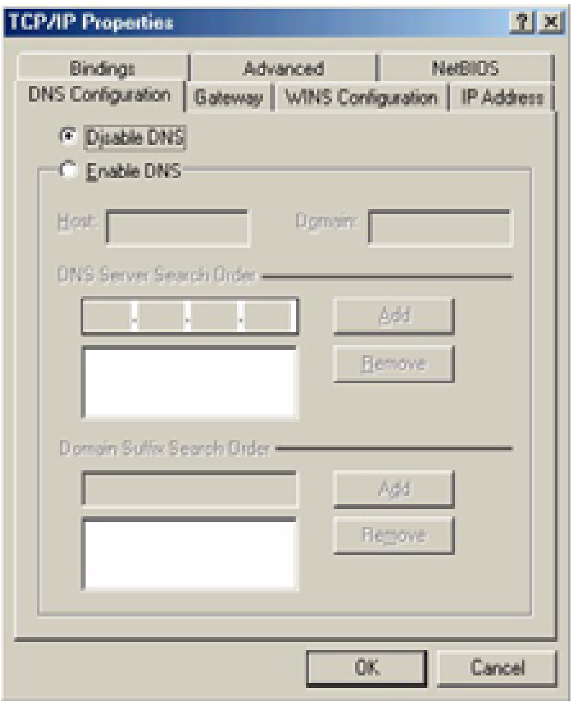
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 126 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your Prestige and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

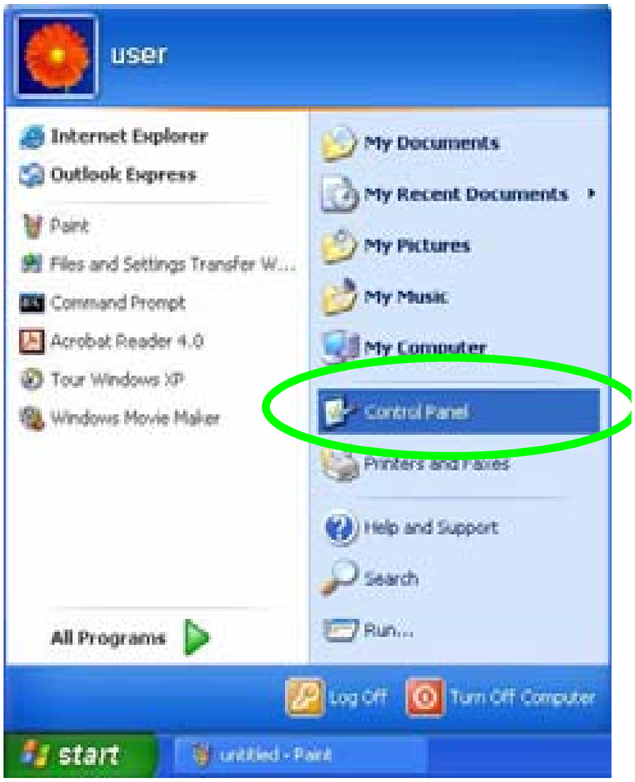
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

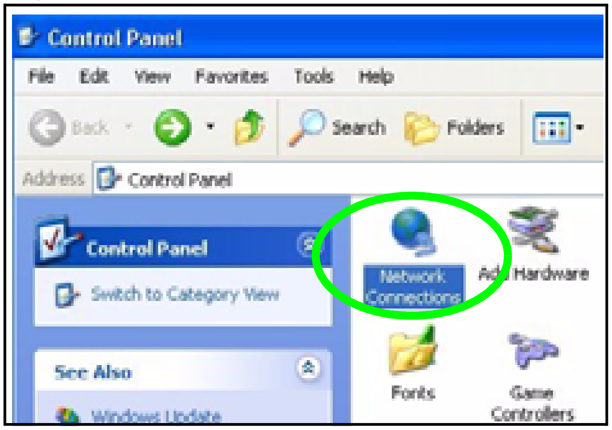
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 127 Windows XP: Start Menu



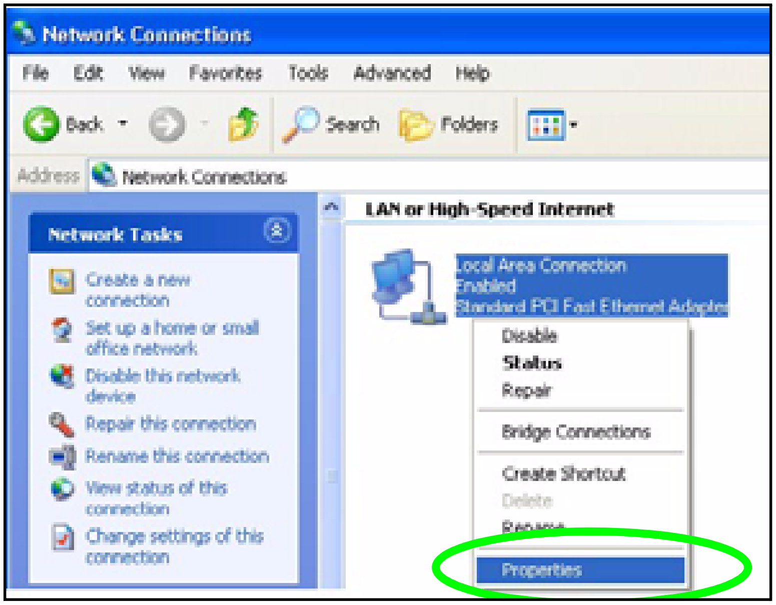
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 128 Windows XP: Control Panel



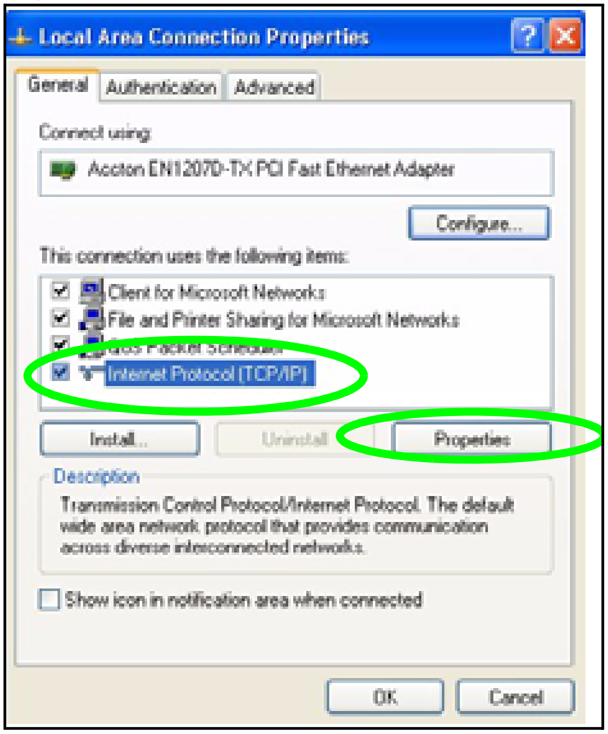
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 129 Windows XP: Control Panel: Network Connections: Properties


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
LAN or High-Speed Internet
Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties

4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 130 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

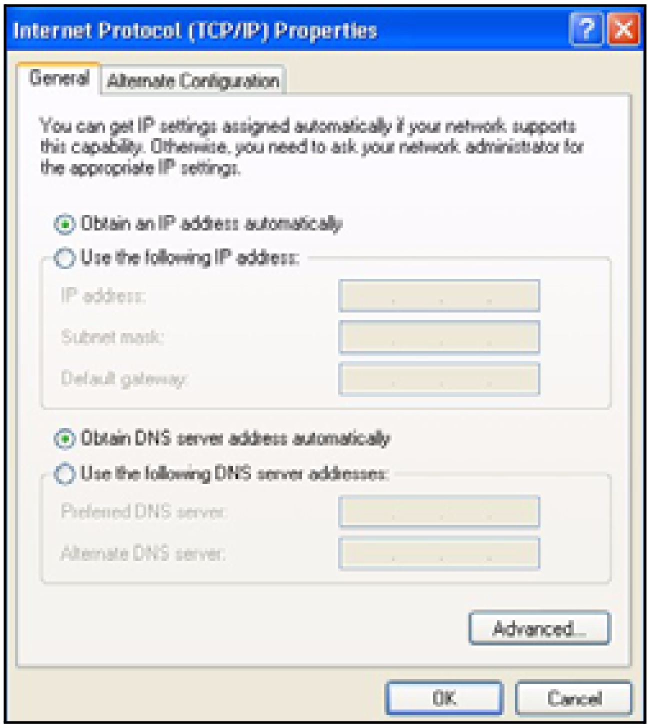
□ Show icon in notification area when connected

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

- Click **Advanced**.

Figure 131 Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

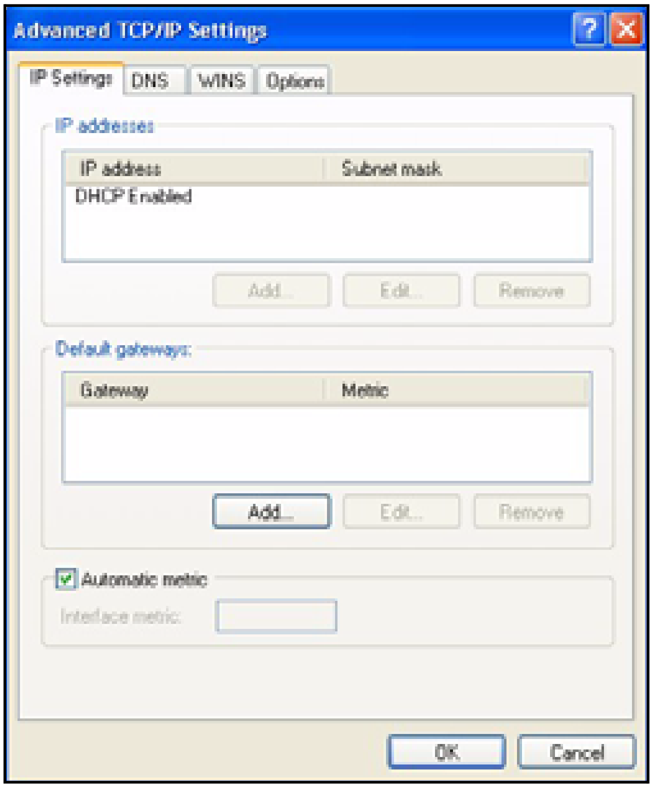
6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

Figure 132 Windows XP: Advanced TCP/IP Properties



DHCP Enabled

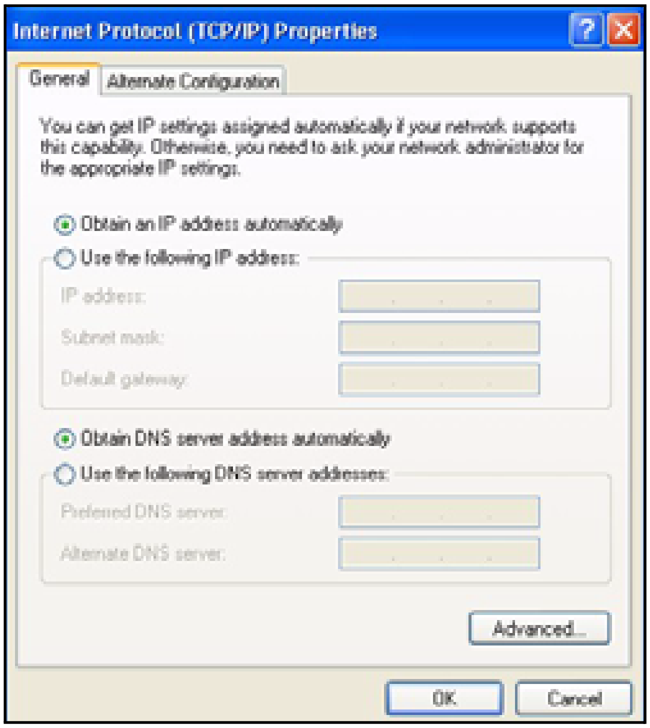
☑ Automatic metric

7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 133 Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

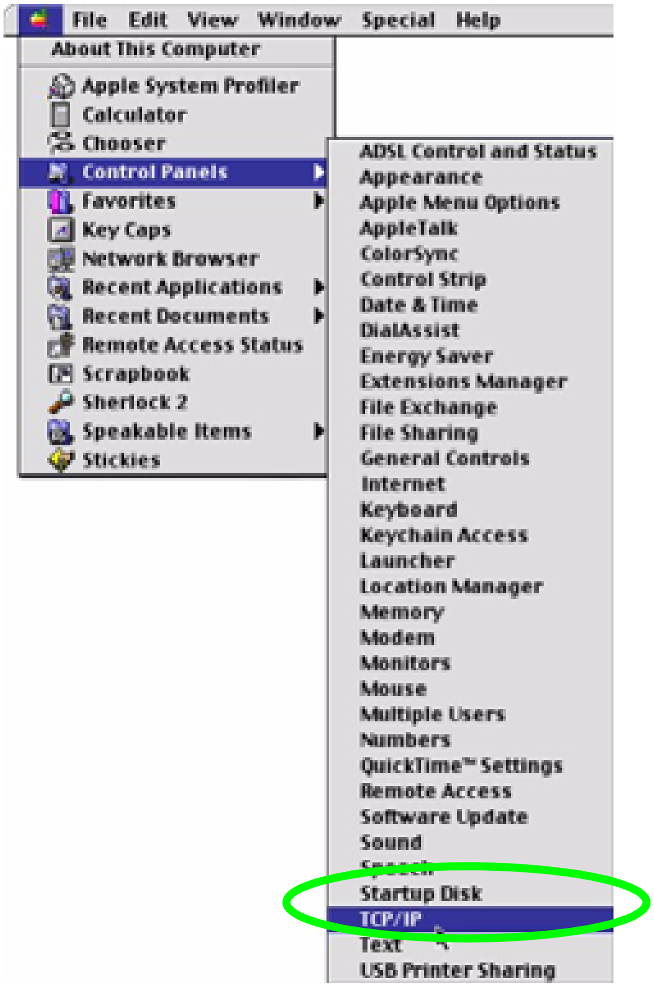
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

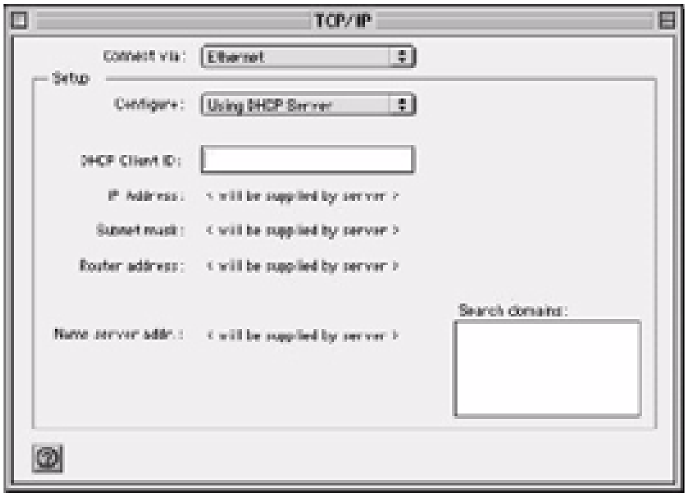
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/ IP Control Panel**.

Figure 134 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 135 Macintosh OS 8/9: TCP/IP



Connect via: Ethernet

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your Prestige and restart your computer (if prompted).

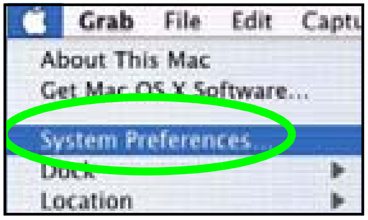
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 136 Macintosh OS X: Apple Menu

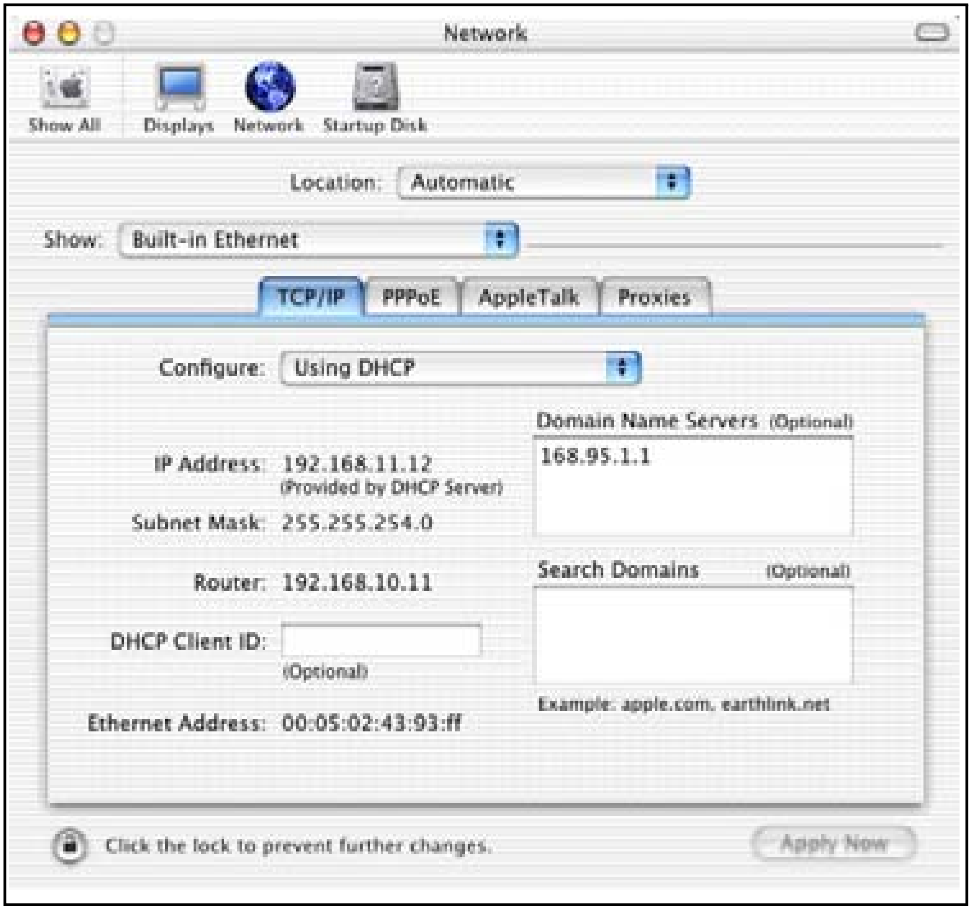


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 137 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

Domain Name Servers (Optional)
168.95.1.1

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

Search Domains (Optional)

DHCP Client ID:
(Optional)

Example: apple.com, earthlink.net

Ethernet Address: 00:05:02:43:93:ff

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

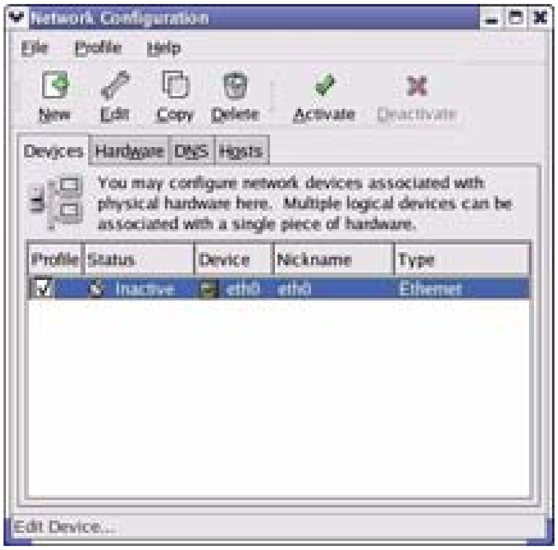
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 138 Red Hat 9.0: KDE: Network Configuration: Devices



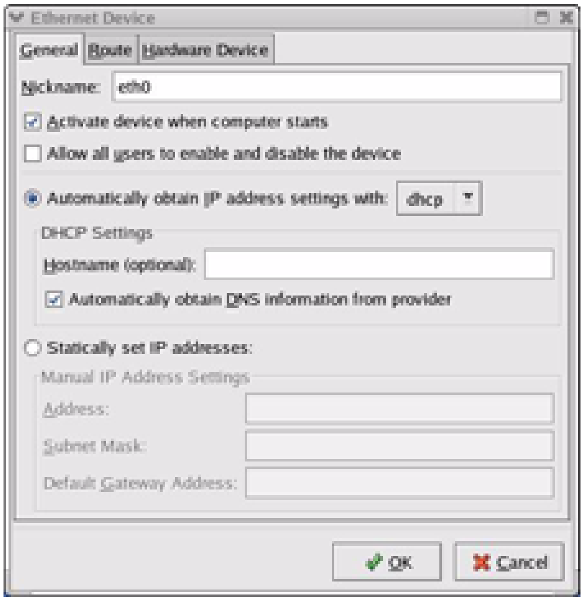
You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Inactive	eth0	eth0	Ethernet

Edit Device...

2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 139 Red Hat 9.0: KDE: Ethernet Device: General



Ethernet Device

General | Route | Hardware Device

Nickname: eth0

☑ Activate device when computer starts

☐ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

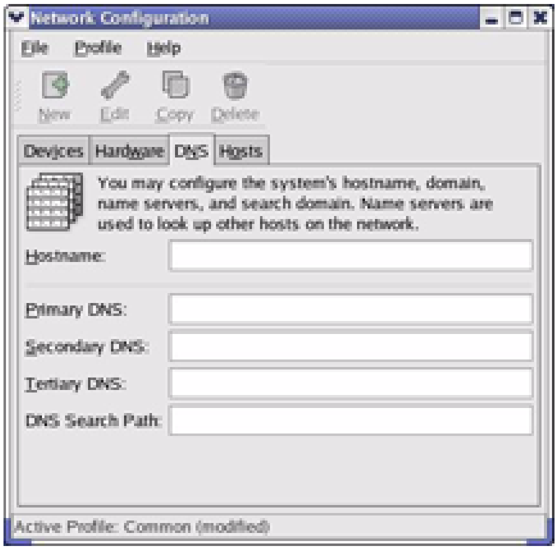
Default Gateway Address:

- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 140 Red Hat 9.0: KDE: Network Configuration: DNS



Network Configuration

Devices | Hardware | DNS | Hosts

You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

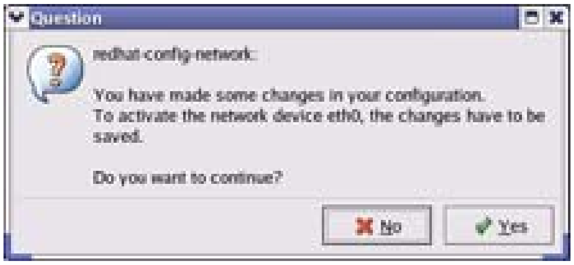
DNS Search Path:

Active Profile: Common (modified)

5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 141 Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.

Do you want to continue?

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 142 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 143 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 144 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 145 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                   [OK]
Shutting down loopback interface:               [OK]
Setting network parameters:                     [OK]
Bringing up loopback interface:                 [OK]
Bringing up interface eth0:                     [OK]
```

21.0.1 Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 146 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

D

Wireless LANs

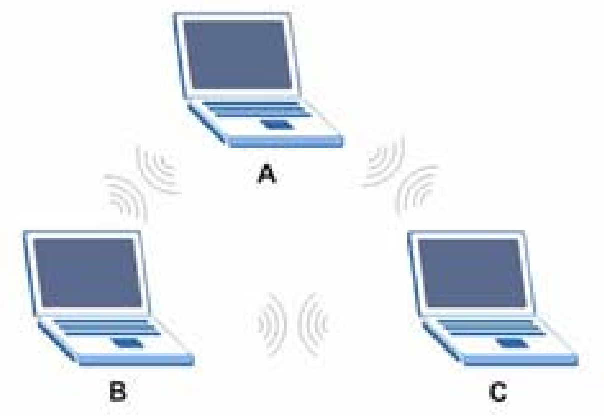
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (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 147 Peer-to-Peer Communication in an Ad-hoc Network

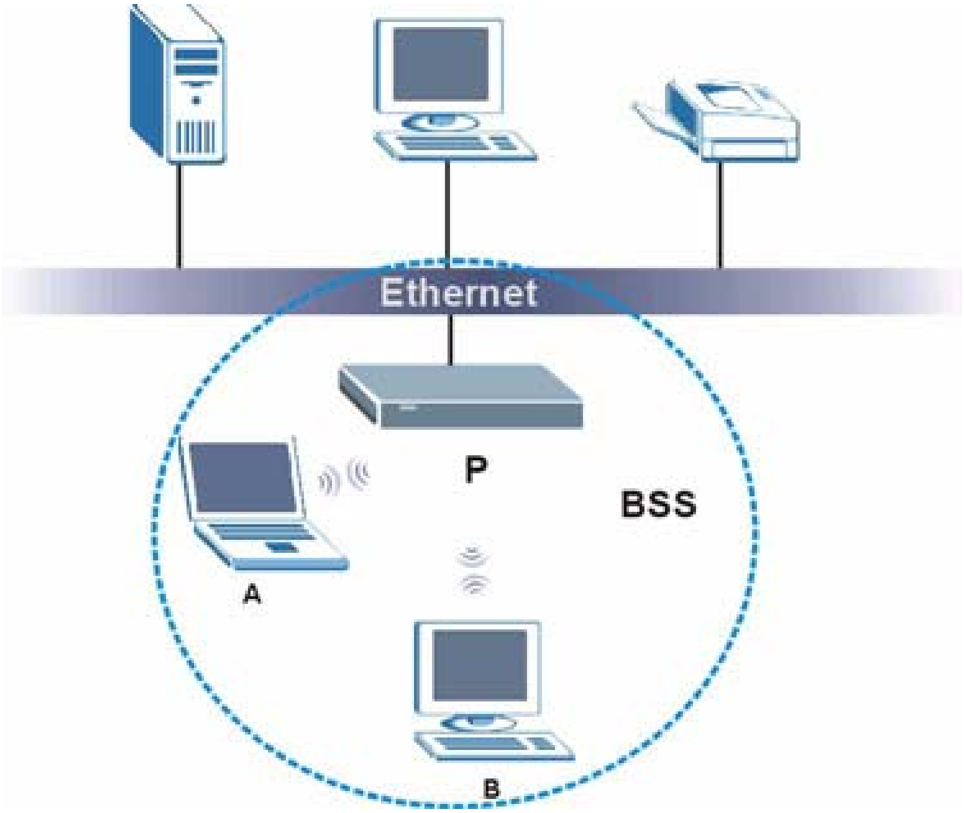


BSS

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

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

Figure 148 Basic Service Set



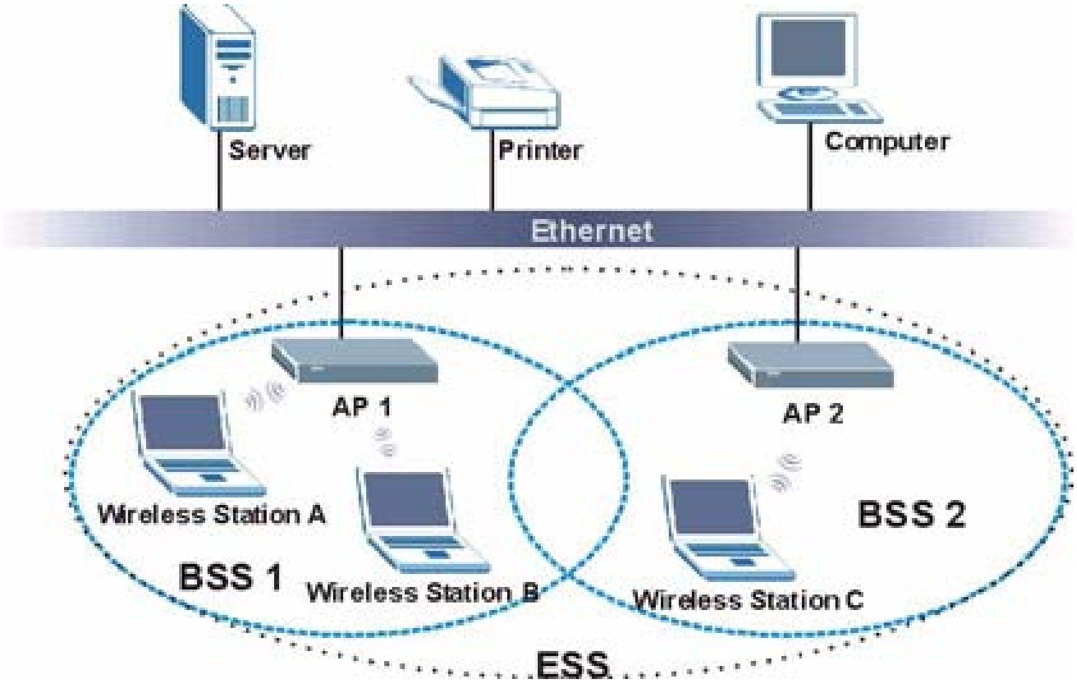
ESS

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 stations within the same ESS must have the same ESSID in order to communicate.

Figure 149 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

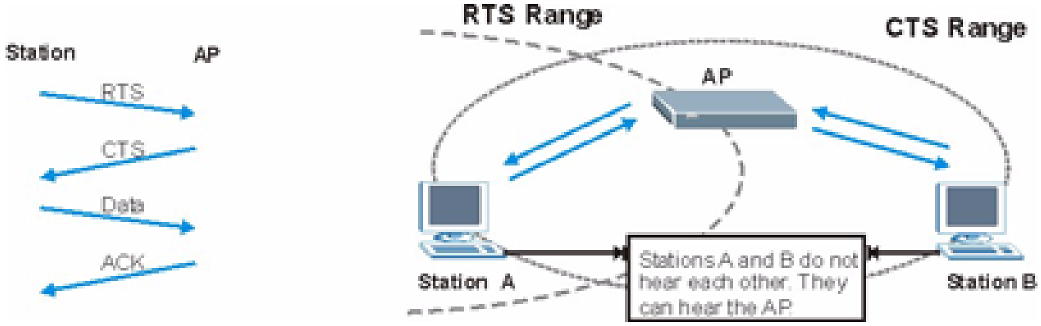
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

Note: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

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 150 RTS/CTS


Station
AP
RTS
CTS
Data
ACK
RTS Range
CTS Range
AP
Station A
Station B
Stations A and B do not hear each other. They can hear the AP.

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

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations 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 96 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)

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 stations.

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 station 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 Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station ‘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 stations 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 screen. You may still configure and store keys here, 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 97 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(2)

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(2) and WEP are improved data encryption and user authentication.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. In addition to TKIP, WPA2 also uses Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes 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.

TKIP regularly changes and rotates 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 pair-wise key 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.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

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), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

User Authentication

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

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.

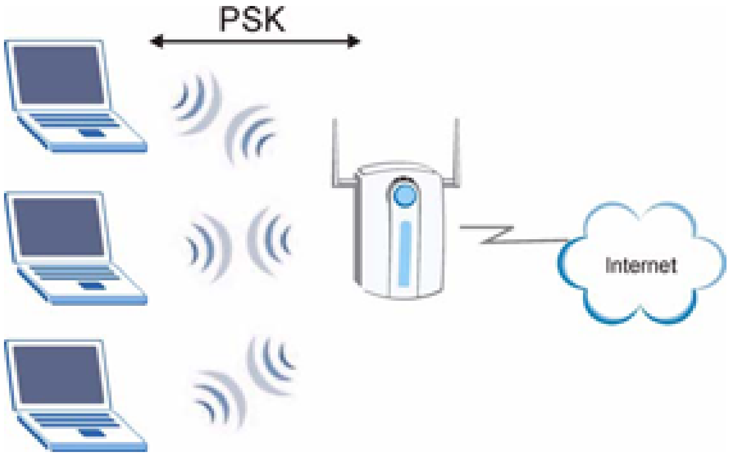
Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

21.0.2 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 (including spaces and symbols).
2. The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 151 WPA(2)-PSK Authentication



21.0.3 WPA(2) with RADIUS Application Example

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. 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 pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 98 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	No	Enable
WPA-PSK	TKIP	Yes	Enable
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Enable

E

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s**) is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 99 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer 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 purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.

Table 99 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.

Table 99 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

F

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

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.

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 materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

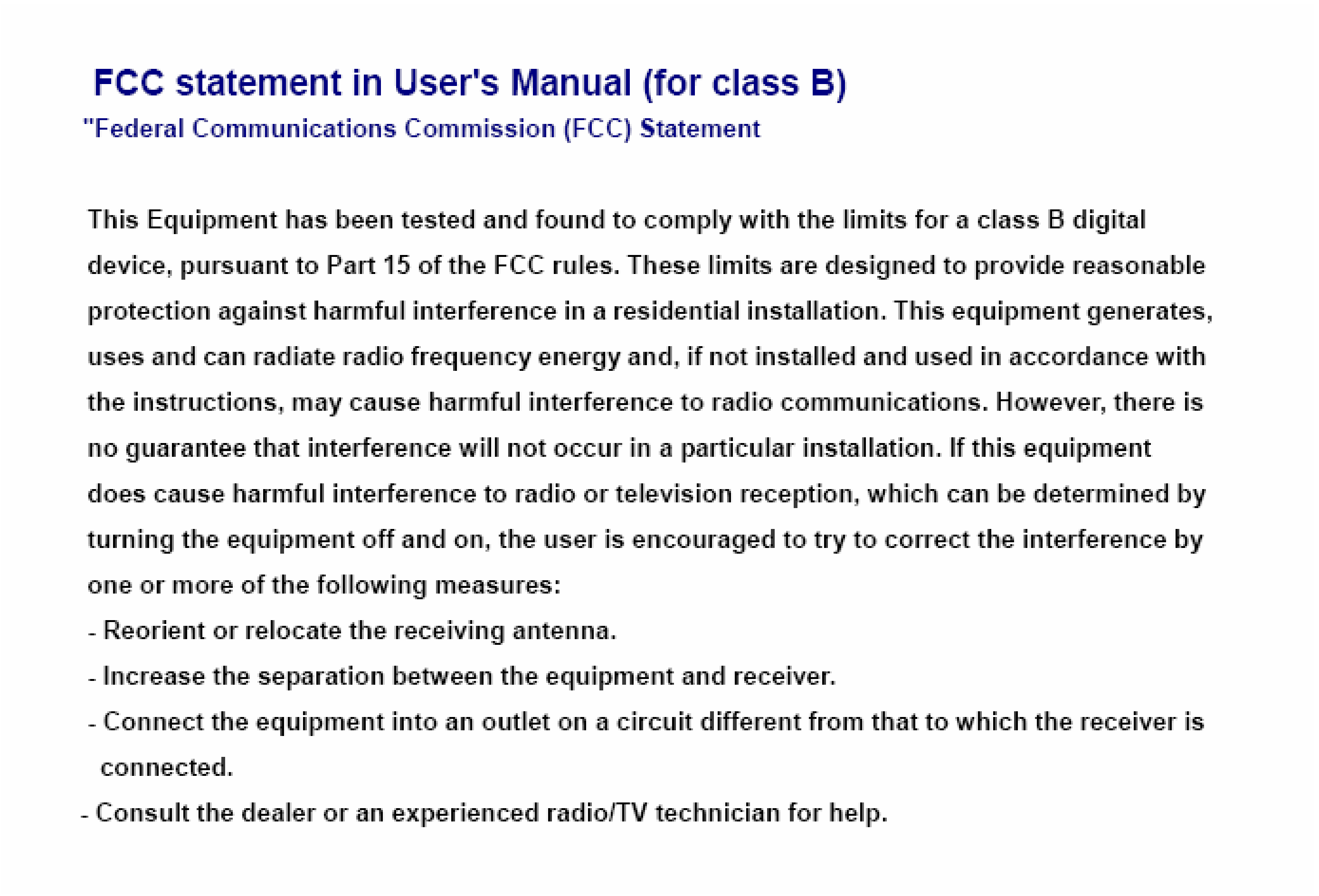
Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

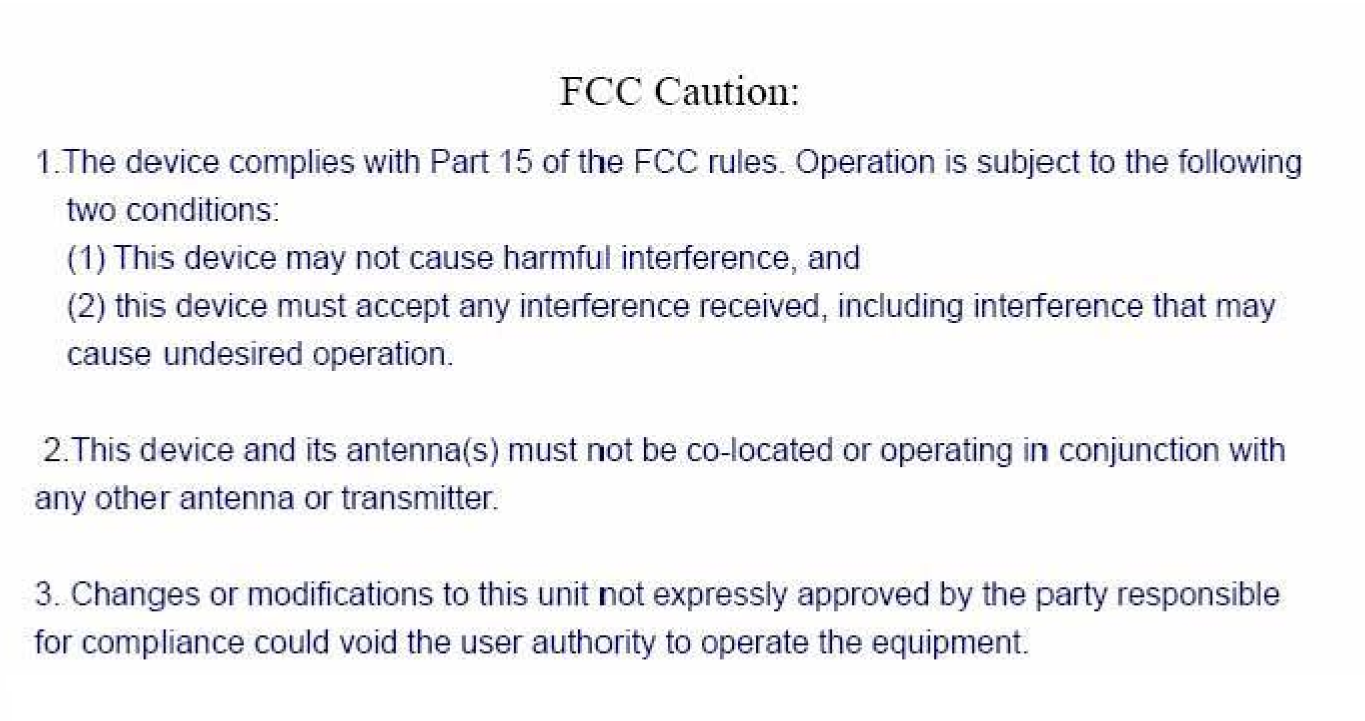


FCC statement in User's Manual (for class B)

"Federal Communications Commission (FCC) Statement

This Equipment 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 equipment 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 equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.



FCC Caution:

1.The device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

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

3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.