P-663HN-51

802.11n ADSL2+ Bonded 4-port Gateway

User's Guide

Default Login Details

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

Firmware Version 1.01
Edition 1, 7/2009

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator.

Related Documentation

Note: It is recommended you use the web configurator to configure the ZyXEL Device.

• Support 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.
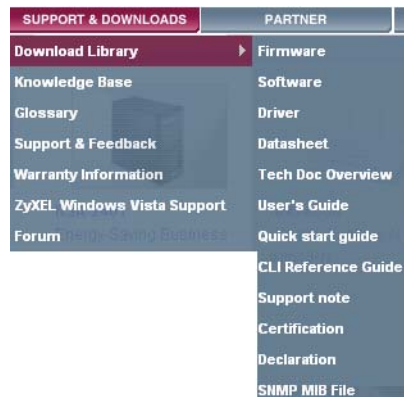
Documentation Feedback

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

Thank you!

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

Need More Help?

More help is available at www.zyxel.com.

- Download Library

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

- Knowledge Base

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

- Forum

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

Customer Support

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

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

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

Document Conventions

Warnings and Notes

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

> **Warnings tell you about things that could harm you or your device.**

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

Syntax Conventions

• The P-663HN-51 may be referred to as the "ZyXEL Device", the "device" 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. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device	Computer	Notebook computer
Server	DSLAM	Firewall
Telephone	Switch	Router

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- 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.
- Please use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.

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

Contents Overview

Table of Contents

PART I
Introduction

Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

1.1 Overview

The ZyXEL Device is an ADSL2+ pair bonding gateway that allows super-fast Internet access over analog (POTS) telephone lines. It bonds two ADSL2+ lines into a single logical connection to provide increased throughput at longer distances. The ZyXEL Device also provides IEEE 802.11b/g/n wireless networking to extend the range of your existing wired network without additional wiring.

In the ZyXEL Device product name, "H" denotes an integrated 4-port switch (hub). Model names ending in "1", for example P-663HN-51, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). The DSL RJ-11 (ADSL over POTS models) connects to your ADSL-enabled telephone lines.

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

The ZyXEL Device provides protection from attacks by Internet hackers. By default, the firewall blocks all incoming traffic from the WAN. See Chapter 29 on page 207 for a full list of features.

A typical Internet access application is shown below

Figure 1   Protected Internet Access Applications
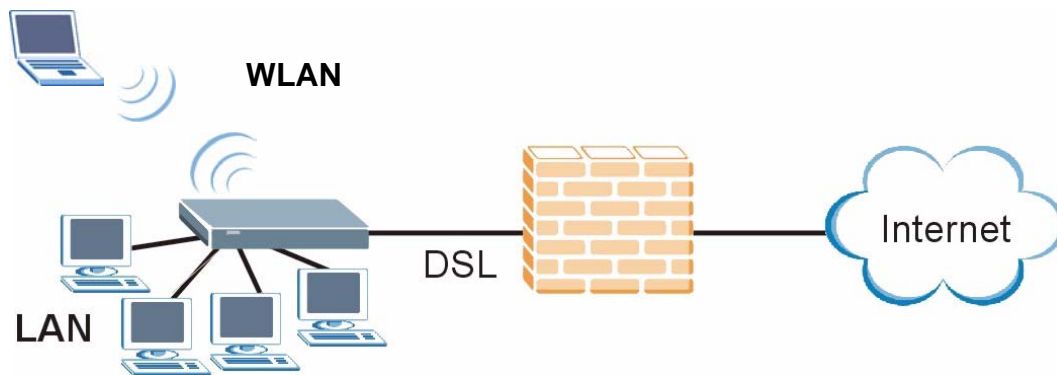
You can also use the ZyXEL Device to connect two geographically dispersed networks over the ADSL line. A typical LAN-to-LAN application example is shown as follows.

Figure 2   LAN-to-LAN Application Example
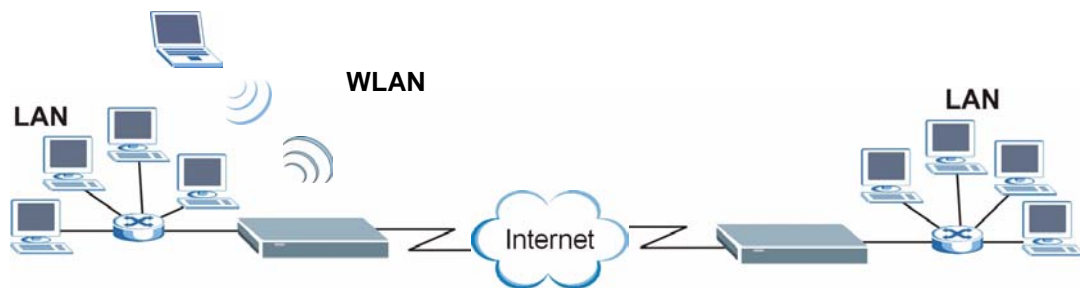
The ZyXEL Device is compatible with the ADSL/ADSL2/ADSL2+ standards (see Table 76 on page 207 for more details). Using ADSL2+, the ZyXEL Device can attain a maximum downstream rate of about 44 Mbps.[1]

Note: The standard your ISP supports determines the maximum upstream and downstream speeds attainable. Actual speeds attained also depend on the distance from your ISP, line quality, etc.

1.2 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

---

1.   This is the theoretical maximum rate under ideal conditions.

- Web Configurator. Use this for everyday management of the ZyXEL Device using a (supported) web browser.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

1.3 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

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

1.4 Hardware Connections

See the Quick Start Guide for the ZyXEL Device's main hardware connections.

1.4.1 Connecting POTS Splitters

Use POTS (Plain Old Telephone Service) splitters to separate the telephone and ADSL signals. This allows simultaneous Internet access and telephone service on the same line. A splitter also eliminates the destructive interference conditions caused by telephone sets.

Install the POTS splitters at the point where the telephone lines enter your premises.

1   Connect the side labeled "Phone" to your telephone.

2   Connect the side labeled "Modem" or "DSL" to your ZyXEL Device.

3   Connect the side labeled "Line" to the telephone wall jack.

1.4.2 Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The use of a telephone microfilter is optional.

1 Locate and disconnect each telephone.

2 Connect a cable from the wall jack to the "wall side" of the microfilter.

3 Connect the "phone side" of the microfilter to your telephone as shown in the following figure.

4 After you are done, make sure that your telephone works. If your telephone does not work, disconnect the microfilter and contact either your local telephone company or the provider of the microfilter.

Figure 3   Connecting a Microfilter
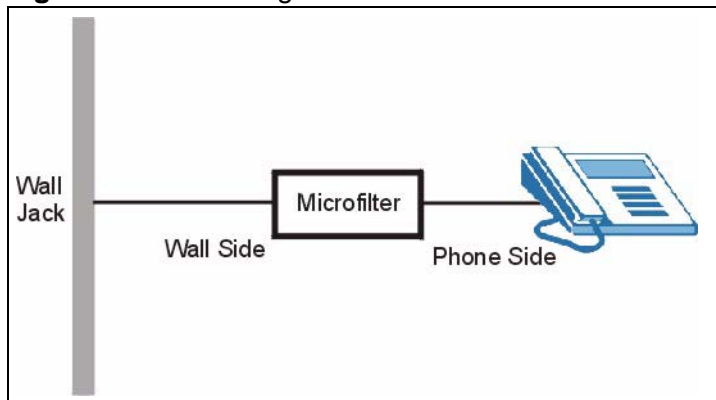
1.5 System Startup and LEDs

After you are done making the hardware connections, press the power button to the **ON** position. Look at the LEDs (lights) on the front panel. The following figure shows the ZyXEL Device's LEDs.

Figure 4   Front Panel
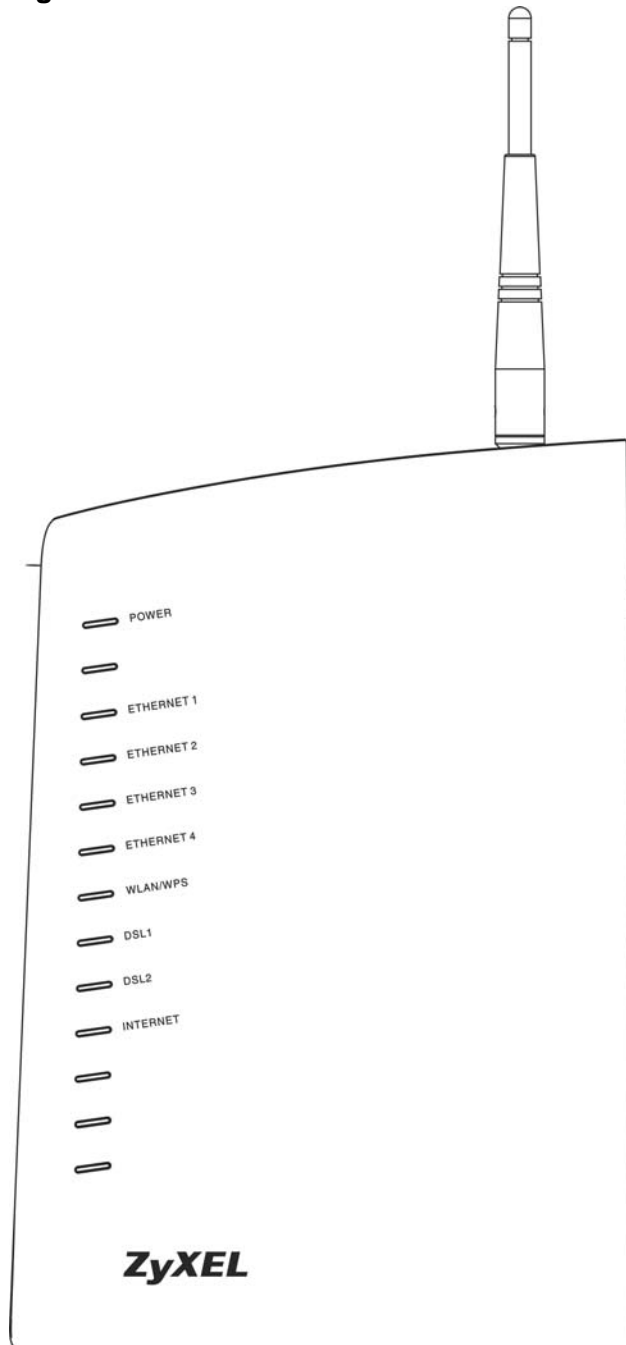
The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power.
		Blinking	The ZyXEL Device is performing a self-test.
		Off	The ZyXEL Device is not receiving power.
ETHERNET 1,2,3,4	Green	On	The ZyXEL Device has a successful Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
		Off	The ZyXEL Device is not connected to the LAN.
WLAN/WPS	Green	On	The ZyXEL Device's wireless interface is activated and operating.
		Blinking	The ZyXEL Device is communicating with other wireless clients.
	Orange	Blinking	The ZyXEL Device is setting up a WPS connection.
		Off	The ZyXEL Device's wireless interface is not activated.
DSL1, DSL2	Green	On	The respective DSL line is up.
		Blinking	Fast blinking means the ZyXEL Device is initializing the respective DSL line. Slow blinking means the respective DSL line is down.
INTERNET	Green	On	The ZyXEL Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
	Red	On	The ZyXEL Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The ZyXEL Device does not have an IP connection.

Introducing the Web Configurator

This chapter describes how to access and navigate the web configurator.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyXEL Device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2. See Appendix C on page 201 if you need to make sure pop-ups are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

The following describes how to access the ZyXEL Device from the LAN using the administrator or user account. See Section 25.5 on page 193 for information about the support account.

1 Make sure your ZyXEL Device hardware is properly connected (see Section 1.4 on page 23).

2 Assign your computer a static IP address (choose one from 192.168.1.2 to 192.168.1.254). See Appendix A on page 215 for how to change your computer's IP address.

3 Launch your web browser.

4 Type "192.168.1.1" as the URL.

5 A screen displays as shown.

Figure 5 Password Screen

2.2.1 User Access

The user account can only access the ZyXEL Device from the LAN. For user access, enter the user account's user name (**user**) and password (**1234** is the default) and click **OK** to view the status only. The following screen appears.

Figure 6 User Status Screen

2.2.2 Administrator Access

The **admin** account can only access the ZyXEL Device from the LAN.

For administrator access, enter the administrator user name (**admin**) and password (**1234** is the default) and click **OK** to enter the configuration screens.

Note: The management session automatically times out if it is left idle for five minutes. Simply log back into the ZyXEL Device if this happens.

2.3 Resetting the ZyXEL Device

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

2.3.1 Using the Reset Button

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

2 Press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the ZyXEL Device restarts.

2.4 Navigating the Web Configurator

After you log in, use the sub-menus on the navigation panel to go to other screens. Some fields or links are not available if you entered the user password in the login password screen (see Figure 5 on page 28).

Figure 7   Web Configurator: First Screen

Table 2   Web Configurator Screens Summary

LINK/ICON	SUB-LINK	FUNCTION
Device Info		
Summary		This screen shows general device information such as the firmware version, line rates, LAN IP address, default gateway, and DNS servers.
WAN		This screen displays information about the ZyXEL Device's WAN connections.
Statistics	LAN	This screen displays statistics about the ZyXEL Device's LAN connections.
	WAN	This screen displays statistics about the ZyXEL Device's WAN connections.
	ATM	This screen shows low-level ATM protocol statistics.
	ADSL	This screen displays statistics about the ZyXEL Device's ADSL connection.

Table 2 Web Configurator Screens Summary (continued)

LINK/ICON	SUB-LINK	FUNCTION
Route		This screen displays information about the ZyXEL Device's routes for sending traffic.
ARP		This screen displays the IP addresses and MAC addresses that the ZyXEL Device has resolved.
DHCP		This screen lists the ZyXEL Device's DHCP clients.
Advanced Setup		
WAN		Use these screens to view and configure the ZyXEL Device's WAN (Internet) connection settings.
LAN		Use this screen to configure LAN settings and the DHCP server.
NAT	Virtual Servers	Use this screen to configure NAT virtual server (port forwarding) entries to have the ZyXEL Device forward traffic from the WAN to LAN computers.
	Port Triggering	Use this screen to change your ZyXEL Device's port triggering settings.
	DMZ Host	Use this screen to configure a DMZ host IP address to receive packets from ports that are not specified in the virtual server configuration.
Security	IP Filtering	Configure outgoing IP filtering to block LAN users or applications from accessing the Internet. Configure incoming IP filtering to allow certain traffic to come in from the Internet to the LAN.
Parental Control		Configure days and times to block Internet access from specific MAC addresses.
Quality of Service		Use the first QoS screen to enable or disable QoS, and select a DSCP mark to use on all outgoing packets that do not match a QoS classification rule.
	Queue Config	This screen lists the QoS queues. A QoS queue sets the priority used for incoming packets that the QoS classifier has grouped into a flow.
	QoS Classification	Configure QoS classifiers to group upstream traffic into data flows according to specific criteria.
Routing	Default Gateway	Set the default gateway that helps the ZyXEL Device forward traffic to its destination.
	Static Route	Configure static routes to have the ZyXEL Device send data to devices not reachable through the default gateway.
	RIP	Configure RIP settings to have the ZyXEL Device exchange routing information with other routers.
DNS	DNS Server	Set how the ZyXEL Device selects a DNS server (for mapping domain names to IP addresses).
	Dynamic DNS	A dynamic DNS service lets the ZyXEL Device use a Web name like *.yourhost.dyndns.org while using a dynamic IP address. This lets others access the ZyXEL Device from the Internet without knowing it's IP address.

Table 2 Web Configurator Screens Summary (continued)

LINK/ICON	SUB-LINK	FUNCTION
DSL		Use this screen to configure the ZyXEL Device's DSL settings.
Interface Group		Use this screen to map ports to PVCs and create bridging groups.
Certificate		Use these screens to import Trusted CA certificates that the ZyXEL Device can use in authenticating wireless clients.
Wireless		
Basic		Use this screen to turn the wireless connection on or off and make other basic configuration changes.
Security		Use this screen to configure wireless security using WiFi Protected Setup (WPS) or manually.
MAC Filter		Use this screen to configure the MAC filter to block or allow wireless access based on the MAC addresses of the wireless stations.
Wireless Bridge		Use this screen to configure wireless connections between the ZyXEL Device and other APs.
Advanced		Use this screen to change the wireless mode, and make other advanced wireless configuration changes.
Station Info		Use this screen to view information about the wireless stations connected to the ZyXEL Device.
Diagnostics		Use this screen to test the connections to your LAN devices (Ethernet and wireless connections) and your ADSL connection. You can also test the connection to your Internet Service Provider.
Management		
Settings	Backup	Use this screen to save the ZyXEL Device's configuration to a computer.
	Update	Use this screen to save a previously saved configuration file from a computer to the ZyXEL Device.
	Restore Default	Use this screen to reset the factory defaults to your ZyXEL Device.
System Log	View System Log	Use this screen to display the logs.
	Configure System Log	Use this screen to change your ZyXEL Device's log settings.
SNMP Agent		Use this screen to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
TR-069 Client		Use this screen to allow a Auto-Configuration Server (ACS) to manage the ZyXEL Device.
Internet Time		Use this screen to configure how the ZyXEL Device synchronizes its internal clock with a time server on the Internet.

Table 2 Web Configurator Screens Summary (continued)

LINK/ICON	SUB-LINK	FUNCTION
Access Control	Services	Use this screen to enable or disable service access to the ZyXEL Device.
	IP Addresses	Use these screens to configure the IP addresses of trusted computers that may manage the ZyXEL Device.
	Passwords	Use this screen to change the passwords for the ZyXEL Device's accounts.
	Authentication	Use this screen to require users to use a password to log in before they can access the Internet.
Update Software		Use this screen to upload firmware to your ZyXEL Device.
Save/Reboot		Use this screen to save all of your ZyXEL Device's settings and reboot the ZyXEL Device without turning the power off.
Logout		Exit the web configurator.

Note: Click **Management > Logout** to exit the web configurator.

Initial Configuration

This chapter introduces the initial configuration that you may need to perform on the ZyXEL Device.

3.1 WAN Configuration

If you connect your ZyXEL Device and are able to access the Internet without configuring the ZyXEL Device, it may be that your ISP pre-configured the ZyXEL Device for you or the Internet connection works with the ZyXEL Device's default settings.

If you connect the ZyXEL Device and are not able to access the Internet, the ISP (Internet Service Provider) should have given you Internet connection information. This includes the connection type, VPI, VCI, and any values specific to your connection type (such as a user name and password). Click **Advanced Setup > WAN > Add** (or **Edit**). Use the following screen (and the ones that come after it) to configure your Internet connection. See for more information.

Figure 8   Advanced Setup > WAN > Add

3.2 QoS Configuration

If the ISP gave you QoS settings to use, click **Advanced Setup > QoS** and configure the ZyXEL Device to use them. See Chapter 10 on page 103 for details.

If the WAN connection uses VLAN multiplexing, you can apply different QoS settings to different VLANs within the same WAN connection. If you are not using VLAN multiplexing, you may need to configure separate WAN connections (using different PVCs) in order to give different traffic different priorities.

3.3 Changing the Login Password

It is highly recommended that you periodically change the password for accessing the ZyXEL Device. Click **Management > Access Control > Passwords** to display the screen shown next. Use this screen to change the password. See Section 25.5 on page 193 for details.

Figure 9   Management > Access Control > Passwords

Device Information

Use the **Device Info** screens to see information about your ZyXEL Device and its connections.

4.1 Device Information Summary

The **Device Info > Summary** screen displays when you log in. To get to it from another screen, just click **Device Info > Summary**. This screen displays general information about the ZyXEL Device.

Figure 10   Device Info > Summary

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

Table 3 Device Info > Summary

LABEL	DESCRIPTION
Product Name	This is your ZyXEL Device's model name.
Software Version	This is the number of the firmware release the ZyXEL Device is using.
Bootloader (CFE) Version	This is the number of the bootloader the ZyXEL Device is using.
Line Rate - Upstream (Kbps)	This is the speed of the upstream (outgoing) connection link.
Wireless Driver Version	This is the number of the driver that the ZyXEL Device's wireless chipset is using.
Line Rate - Downstream (Kbps)	This is the speed of the downstream (incoming) connection link.
LAN IPv4 Address	This is the IP (version 4) address of the LAN ports.
Default Gateway	This is the IP address of the default gateway, if applicable.
Primary DNS Server	This is the IP address of the server that the ZyXEL Device tries to use first when it needs to resolve a domain name (find the numeric IP address associated with the domain name).
Secondary DNS Server	If the primary server does not respond when the ZyXEL Device tries to resolve a domain name, the ZyXEL Device tries the server displayed in this field.
LAN IP Address	This is the IP address of the LAN ports.
Default Gateway	This is the IP address of the default gateway, if applicable.
Primary DNS Server	This is the IP address of the server that the ZyXEL Device tries to use first when it needs to resolve a domain name (find the numeric IP address associated with the domain name).
Secondary DNS Server	If the primary server does not respond when the ZyXEL Device tries to resolve a domain name, the ZyXEL Device tries the server displayed in this field.
Local Mac Address	This is the MAC (Media Access Control) address the ZyXEL Device uses for it's LAN connections.

4.2 WAN Information

Click **Device Info > WAN** to open the following screen. Each row in the table displays information about one of the ZyXEL Device's WAN connections.

Figure 11   Device Info > WAN

WAN Info										
Port/VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IPv4 Address
0/0/33	Off	1	UBR	mer_0_0_33	nas_0_0_33	MER	Disabled	Disabled	Enabled	ADSL Link Down	

The following table describes the labels in this screen.

Table 4   Device Info > WAN

LABEL	DESCRIPTION
Port/VPI/VCI	This field displays the WAN connection's DSL port, Virtual Path Identifier, and Virtual Channel Identifier. The DSL port is always 0 because the DSL ports are bonded into a single logical port.
VLAN Mux.	This field shows whether or not VLAN multiplexing is enabled. VLAN multiplexing allows multiple separate WAN connections within the same PVC.
Con. ID	This is the number of the WAN connection.
Category	This is the ATM traffic class the WAN connection is using.
Service	This displays the connection type, DSL port, Virtual Path Identifier, and Virtual Channel Identifier. For the connection types, pppoe stands for PPPoE, ipoa stands for IPoA, pppoa stands for PPPoA, mer stands for MAC Encapsulated Routing, and br stands for bridging.
Interface	This field displays the name of the WAN connection, followed by the DSL port, Virtual Path Identifier, and Virtual Channel Identifier.
Protocol	This is the type of network protocol the WAN interface is using for IP over Ethernet.
IGMP	This is whether or not the WAN connection is using IGMP multicast (if available).
QoS	This is whether or not packet level QoS is enabled for the WAN connection.
State	This is whether or the WAN connection is enabled.
Status	This is the WAN connection's current ADSL line state.
IPv4 Address	This is the WAN connection's IP (version 4) address.

4.3 LAN Statistics

Click **Device Info > Statistics > LAN** to open the following screen. This screen displays statistics about the ZyXEL Device's LAN connections.

Figure 12   Device Info > Statistics > LAN

The following table describes the labels in this screen.

Table 5   Device Info > Statistics > LAN

LABEL	DESCRIPTION
Interface	This field displays the type of LAN connection.
Received	These statistics are for traffic the ZyXEL Device has received on the interface.
Transmitted	These statistics are for traffic the ZyXEL Device has sent through the interface.
Bytes	This field displays the number of bytes received or sent.
Pkts	This field displays the number of packets received on or sent through the interface.
Errs	This field displays the number of error packets received on or sent through the interface.
Drops	This field displays the number of incoming or outgoing packets dropped.
Reset Statistics	Click this button to have the ZyXEL Device clear the current LAN interface statistics and start collecting them again.

4.4 WAN Statistics

Click **Device Info > Statistics > WAN** to open the following screen. Each row in the table displays statistics about a WAN connection.

Figure 13   Device Info > Statistics > WAN

The following table describes the labels in this screen.

Table 6   Device Info > Statistics > WAN

LABEL	DESCRIPTION
Service	If the WAN connection is using bridging, the name of the bridge displays here.
VPI/VCI	This field displays the WAN connection's Virtual Path Identifier, and Virtual Channel Identifier.
Protocol	This is the type of network protocol the WAN interface is using for IP over Ethernet.
Interface	This field displays the name of the WAN connection.
Received	These statistics are for traffic the ZyXEL Device has received on the WAN connection.
Transmitted	These statistics are for traffic the ZyXEL Device has sent through the WAN connection.
Bytes	This field displays the number of bytes received or sent.
Pkts	This field displays the number of packets received on or sent through the WAN connection.
Errs	This field displays the number of error packets received on or sent through the WAN connection.
Drops	This field displays the number of incoming or outgoing packets dropped.
Reset Statistics	Click this button to have the ZyXEL Device clear the current WAN statistics and start collecting them again.

4.5 ATM Statistics

Click **Device Info > Statistics > ATM** to open the following screen. This screen shows low-level ATM protocol statistics.

Figure 14 Device Info > Statistics > ATM

The following table describes the labels in this screen.

Table 7 Device Info > Statistics > ATM

LABEL	DESCRIPTION
ATM Interface Statistics	These are statistics for the ATM interface.
In Octets	How many octets the interface received.
Out Octets	How many octets the interface transmitted.
In Errors	How many cells the ZyXEL Device dropped because of uncorrectable HEC errors.
In Unknown	How many received cells the ZyXEL Device discarded during cell header validation. This includes cells with invalid cell header patterns or unrecognized VPI/VCI values. If the ZyXEL Device is set to discard cells with undefined PTI values, they are also included in this count.
In Hec Errors	How many cells the ZyXEL Device received with HEC errors in the ATM cell headers.
In Invalid Vpi Vci Errors	How many cells the ZyXEL Device received with an unregistered VCC (Virtual Channel Connection) address.
In Port Not Enable Errors	How many cells the ZyXEL Device received on disabled ports.
In PTI Errors	How many cells the ZyXEL Device received with an ATM header that had a Payload Type Indicator (PTI).
In Idle Cells	How many idle cells the ZyXEL Device received.

Table 7 Device Info > Statistics > ATM (continued)

LABEL	DESCRIPTION
In Circuit Type Errors	How many idle cells the ZyXEL Device received with illegal circuit types.
In OAM RM CRC Errors	How many Operational, Administration and Maintenance Function 5 (OAM) and RM (Rate Management) cells the ZyXEL Device received with a Cyclic Redundancy Check error.
In GFC Errors	How many cells the ZyXEL Device received with non-zero GFCs.
AAL5 Interface Statistics	These are statistics for the AAL5 interface.
In Octets	How many AAL5/AAL0 CPCS PDU octets the ZyXEL Device received.
Out Octets	How many AAL5/AAL0 CPCS PDU octets the ZyXEL Device transmitted.
In Ucast Pkts	How many received AAL5/AAL0 CPCS PDUs the ZyXEL Device passed to higher layers.
Out Ucast Pkts	How many AAL5/AAL0 CPCS PDUs the ZyXEL Device received for transmission from higher layers.
In Errors	How many AAL5/AAL0 CPCS PDUs the ZyXEL Device received that contained errors. Including CRC-32 errors, SAR timeouts, and oversised SDUs.
Out Errors	How many AAL5/AAL0 CPCS PDUs the ZyXEL Device could not transmit due to errors.
In Discards	How many AAL5/AAL0 CPCS PDUs the ZyXEL Device discarded due to input buffer overflows.
Out Discards	How many non-errored AAL5/AAL0 CPCS PDUs the ZyXEL Device discarded. (For example, the ZyXEL Device might do this to free up buffer space.)
AAL5 VCC Statistics	These are statistics for the ATM VCC (Virtual Channel Connection) interface.
VPI/VCI	A VCC (Virtual Channel Connection) is a VPI and VCI combination. Each row in this table represents a VCC. This field displays the Virtual Path Identifier, and Virtual Channel Identifier of each VCC.
CRC Errors	How many PDUs the ZyXEL Device received on the VCC with CRC-32 errors.
SAR Timeouts	How many partially-reassembled PDUs the ZyXEL Device discarded because they were not fully reassembled during the allotted time period. This value is zero if the re-assembly timer is not supported.
Oversized SDUs	How many PDUs with corresponding SDUs that were too large (so the ZyXEL Device discarded them).
Short Packet Errors	How many PDUs that had a length shorter than the size of the AAL5 trailer (so the ZyXEL Device discarded them).
Length Errors	How many PDUs the ZyXEL Device discarded because the length in the AAL5 trailer did not match the PDU length.
Reset Statisitcs	Click this button to have the ZyXEL Device clear the current ATM statistics and start collecting them again.

4.6 ADSL Statistics

Click **Device Info > Statistics > ADSL** to open the following screen. This screen displays statistics about the ZyXEL Device's ADSL connection.

Figure 15 Device Info > Statistics > ADSL

The following table describes the labels in this screen.

Table 8 Device Info > Statistics > ADSL

LABEL	DESCRIPTION
Mode	This is the ADSL mode that the ADSL link is using.
Type	This shows whether it is an "interleaved" (uses interleaving to aid in error correction) or "fast" (no interleaving) ADSL link.
Line Coding	This shows whether the ADSL link is using Trellis coding or Reed-Solomon error correction. Trellis coding helps to reduce the noise in ADSL transmissions. Trellis may reduce throughput but it makes the connection more stable. "RS" coding stands for Reed-Solomon error correction.
Status	This shows the ADSL link's connection status.

Table 8   Device Info > Statistics > ADSL (continued)

LABEL	DESCRIPTION
Link Power State	This is the ADSL connection's current power management mode.
SNR Margin (dB)	This is the upstream and downstream Signal-to-Noise Ratio Margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the ZyXEL Device still being able to meet its transmission targets.
Attenuation (dB)	This is the downstream and upstream Line Attenuation (in dB).
Output Power (dBm)	This field displays the amount of power being used to transmit to the other end of the ADSL link. Output power varies with the line length and quality. The longer the line is or the more interference there is on the line, the more power is needed.
Attainable Rate (Kbps)	These are the downstream and upstream highest theoretically possible transfer rates (in Kbps).
Aggregate Rate (Kbps)	These are the combined downstream and upstream rates (in Kbps) of the two DSL ports.
DSL1 Rate (Kbps)	These are the downstream and upstream rates (in Kbps) at which the DSL1 port has been receiving and sending data.
DSL2 Rate (Kbps)	These are the downstream and upstream rates (in Kbps) at which the DSL2 port has been receiving and sending data.
Super Frames	These are the downstream and upstream numbers of downstream and upstream super frames.
Super Frame Errors	These are the downstream and upstream numbers of errored super frames sent and received.
RS Words	These are the downstream and upstream numbers of Reed-Solomon error correction words.
RS Correctable Errors	These are the downstream and upstream numbers of Reed-Solomon errors.
RS Uncorrectable Errors	The number of downstream and upstream uncorrectable Reed-Solomon errors.
HEC Errors	These are the downstream and upstream numbers of Header Error Control errors.
OCD Errors	These are the downstream and upstream numbers of Out of Cell Delineation errors.
LCD Errors	The number of 1-second intervals since reset where loss of cell delineation occurred.
Total Cells	The total numbers of downstream and upstream ATM cells.
Data Cells	The total numbers of downstream and upstream data cells.

Table 8 Device Info > Statistics > ADSL (continued)

LABEL	DESCRIPTION
Bit Errors	The total numbers of downstream and upstream bit errors.
Total ES	The number of Errored SecondS that have occurred within the period.
Total SES	The number of Severely Errored Seconds that have occurred within the period.
Total UAS	The number of UnAvailable Seconds that have occurred within the period.
ADSL BER Test	Click this button to perform an ADSL Bit Error Rate Test to measure the quality of the ADSL connection.
Reset Statisitcs	Click this button to have the ZyXEL Device clear the current ADSL statistics and start collecting them again.

4.7 ADSL BER Test

Click **Device Info > Statistics > ADSL > ADSL BER Test** to open the following screen. Perform an ADSL Bit Error Rate Test to measure the quality of the ADSL connection.

Figure 16 Device Info > Statistics > ADSL > ADSL BER Test

Select for how many seconds to perform the test and click **Start**.

Figure 17 Device Info > Statistics > ADSL > ADSL BER Test: Results

The ADSL BER test results show how many bits were sent, how many of the transferred bits were errored, and the error ratio.

Click **Close** when you are done.

4.8 Route Info

Click **Device Info > Route** to open the following screen. This screen displays information about the ZyXEL Device's routes for sending traffic.

Figure 18   Device Info > Route

The following table describes the labels in this screen.

Table 9   Device Info > Route

LABEL	DESCRIPTION
Destination	The route applies to traffic going to this network address.
Gateway	This is the router the ZyXEL Device sends traffic to in order to forward the traffic to the destination listed in the route.
Subnet Mask	This is the network number of the gateway to which this route forwards traffic.
Flag	This displays more information about the route. U - up ! -reject G - gateway H - host R - reinstate D - dynamic (redirect) M - modified (redirect)
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

Table 9 Device Info > Route (continued)

LABEL	DESCRIPTION
Service	This displays what type of traffic this route is for. The field is blank when the route is for all types of service.
Interface	This route has the ZyXEL Device send traffic through this interface.

4.9 ARP Info

Click **Device Info > ARP** to open the following screen. This screen displays information about the IP addresses the ZyXEL Device has resolved into MAC addresses.

Figure 19 Device Info > ARP

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.10	Complete	02:10:18:01:00:07	br0
192.168.1.2	Complete	00:0F:FE:1E:4A:E0	br0

The following table describes the labels in this screen.

Table 10 Device Info > ARP

LABEL	DESCRIPTION
IP Address	This is the IP address that the ZyXEL Device resolved into a MAC address.
Flags	This field shows more information about the IP address entry. **Complete** means it is a valid entry. **Incomplete** means it is an invalid entry. **Permanent** means the entry will not expire. **Public** means it is an entry that the ZyXEL Device acquired by listening.
HW Address	This is the MAC (Media Access Control) address to which the ZyXEL Device resolved the IP address.
Device	This identifies the interface to which the device with the listed IP address is connected.

4.9.1 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 ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If

DHCP service is disabled, there must be another DHCP server, or else the computer must be manually configured.

Click **Device Info > DHCP** to display the following screen. This is only available when the ZyXEL Device's DHCP server function is enabled. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the ZyXEL Device's DHCP server.

Figure 20   Device Info > DHCP

Device Info -- DHCP Leases			
Hostname	**MAC Address**	**IP Address**	**Expires In**
twpc11746-01	00:0F:FE:1E:4A:E0	192.168.1.2	23 hours, 55 minutes, 10 seconds

The following table describes the labels in this screen.

Table 11   Device Info > DHCP

LABEL	DESCRIPTION
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.
IP Address	This field displays the IP address assigned to the DHCP client.
Expires In	This field displays for how much longer the host has the lease for the assigned IP address.

PART II
Advanced

5

WAN Setup

5.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

5.1.1 VPI and VCI

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

5.1.2 Multiplexing

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

5.1.2.1 VC-based Multiplexing

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

5.1.2.2 LLC-based Multiplexing

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

5.2 Traffic Shaping

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

Note: Traffic shaping controls outgoing (upstream) traffic, not incoming (downstream).

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

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

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

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

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

Figure 21   Example of Traffic Shaping
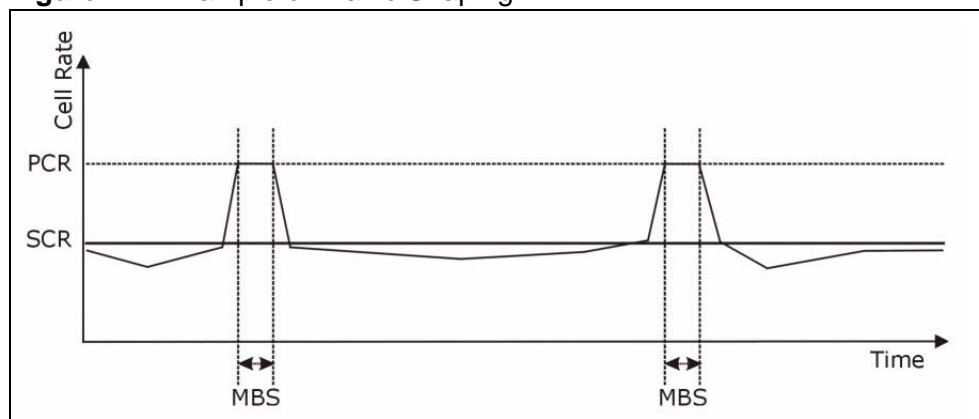
5.2.1 ATM Traffic Classes

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

5.2.1.1 Constant Bit Rate (CBR)

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

5.2.1.2 Variable Bit Rate (VBR)

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

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

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

5.2.1.3 Unspecified Bit Rate (UBR)

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

5.3 WAN

Click **Advanced Setup > WAN** to open the following screen. This screen displays your ZyXEL Device's WAN Internet access settings. You can also edit those settings and add more settings. The screen differs by the encapsulation.

See for more information.

Figure 22 Advanced Setup > WAN

The following table describes the labels in this screen.

Table 12 Advanced Setup > WAN

LABEL	DESCRIPTION
Port/VPI/VCI	This field displays the WAN connection's DSL port, Virtual Path Identifier, and Virtual Channel Identifier. The DSL port is always 0 because the DSL ports are bonded into a single logical port.
VLAN Mux.	This field shows whether or not VLAN multiplexing is enabled. VLAN multiplexing allows multiple separate WAN connections within the same PVC.
Con. ID	This is the number of the WAN connection.
Category	This is the ATM traffic class the WAN connection is using.
Service	This displays the connection type, DSL port, Virtual Path Identifier, and Virtual Channel Identifier. For the connection types, pppoe stands for PPPoE, ipoa stands for IPoA, pppoa stands for PPPoA, mer stands for MAC Encapsulated Routing, and br stands for bridging.
Interface	This field displays the name of the WAN connection, followed by the DSL port, Virtual Path Identifier, and Virtual Channel Identifier.
Protocol	This is the type of network protocol the WAN interface is using for IP over Ethernet.
IGMP	This is whether or not the WAN connection is using IGMP multicast (if available).
QoS	This is whether or not packet level QoS is enabled for the WAN connection.
State	This is whether or the WAN connection is enabled.
Remove	To remove a WAN connection, select its **Remove** check box and click the **Remove** button.
Edit	Click this button to go to a screen where you can modify the WAN connections settings.
Add	Click this button to go to a screen where you can configure settings for a new WAN connection.
Remove	To remove a WAN connection, select its **Remove** check box and click the **Remove** button.
Save/Reboot	Click this button to apply and save your changes. The ZyXEL Device restarts.

5.4 WAN ATM PVC Configuration and QoS

Click **Advanced Setup > WAN > Add** (or **Edit**) to open the following screen. Use this screen to configure ATM PVC settings and enable or disable QoS. The screen differs by the service category.

See for more information.

Figure 23 Advanced Setup > WAN > Add

The following table describes the labels in this screen.

Table 13 Advanced Setup > WAN > Add

LABEL	DESCRIPTION
ATM PVC Configuration	The PORT (interface), VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define an ATM PVC (Permanent Virtual Circuit). Refer to the appendix for more information.
VPI	Enter the VPI assigned to you for this WAN connection.
VCI	Enter the VCI assigned to you for this WAN connection.
VLAN Mux.	Select the check box to use VLAN multiplexing to allow multiple separate protocols to use the same PVC. Selecting this enables IEEE 802.1q. Separate VLANs can be used to give different priorities to the traffic from different ports.
802.1Q VLAN ID	When you enable VLAN multiplexing, type the VLAN ID that the ZyXEL Device is to add to the traffic sent through this WAN connection.

Table 13 Advanced Setup > WAN > Add (continued)

LABEL	DESCRIPTION
Service Category	Select **UBR** (unspecified bit rate) for applications that are non-time sensitive, such as e-mail. Use it with PCR if you want to specify a maximum rate at which the sender can send cells. Select **CBR** (constant bit rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Realtime VBR** for bursty traffic connections that require closely controlled delay and delay variation (like video conferencing). Use **Non Realtime VBR** for bursty connections that do not require closely controlled delay and delay variation (like non-time sensitive data file transfers).
Peak Cell Rate	The Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. PCR applies with all of the ATM traffic classes. Type a number of (ATM) cells per second (1~255000).
Sustainable Cell Rate	The Sustained Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. SCR applies with the **VBR** traffic classes. Type a number of (ATM) cells per second. The SCR must be less than the PCR.
Maximum Burst Size	The Maximum Burst Size (MBS) sets the maximum number of cells that the port should handle without any discards. Type the MBS here (1~1000000). MBS applies with the **VBR** traffic classes.
Enable Quality of Service	Enable the (packet level) QoS if you need to provide improved performance for certain classes of applications (like VoIP or video conferencing).
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.5 Connection Types

Be sure to use the connection type required by your ISP. Here is background information on the connection types the ZyXEL Device supports.

5.5.1 PPPoA

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

5.5.2 PPPoE

PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. The ZyXEL Device bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to ADSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the appendices.

5.5.3 MER

MER (MAC Encapsulated Routing) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells.

5.5.4 IPoA

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

5.5.5 Bridging

With bridging the ZyXEL Device has a static IP address for the connection. The ZyXEL Device passes traffic through to another device (a computer or router for example) that handles authenticating with the ISP.

5.6 Encapsulation

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

5.6.1 LLC-based Encapsulation

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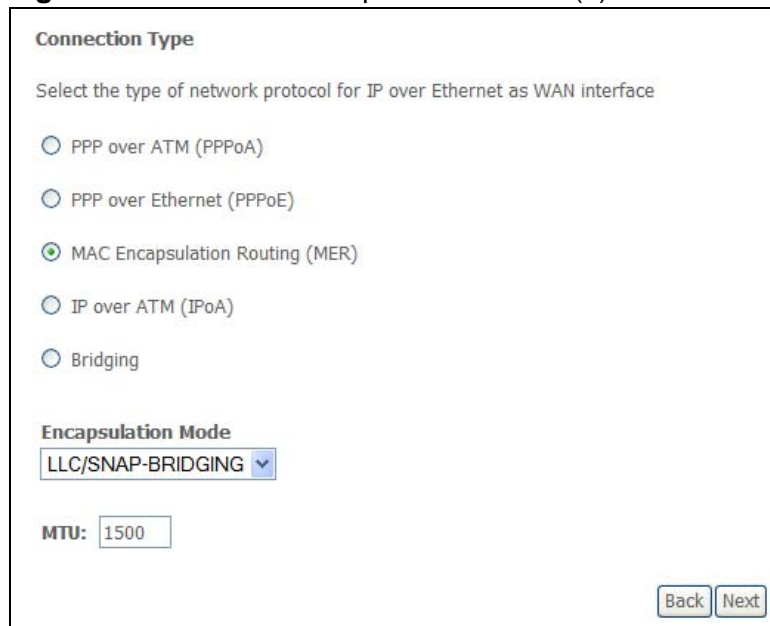
5.6.2 VC-based Encapsulation

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

5.7 WAN Connection Type and Encapsulation Mode

This is the second WAN setup add (or edit) screen. Use this screen to configure WAN connection type and encapsulation mode.

Figure 24   Advanced Setup > WAN > Add (2)

The following table describes the labels in this screen.

Table 14   Advanced Setup > WAN

LABEL	DESCRIPTION
Connection Type	Select the type of network protocol the ISP uses for IP over Ethernet.
Encapsulation Mode	Select the encapsulation mode that your ISP uses.
MTU	This field applies to the PPPoE and MER encapsulation types. Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can go through this interface. If a larger packet arrives, the ZyXEL Device divides it into smaller fragments. For PPPoE you can enter 512 to 1492. For MER you can enter 512 to 1500.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.8 NAT

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

5.9 Nailed-Up Connection (PPP)

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

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

5.10 PPPoA WAN Connection Setup

When you select PPPoA in the second WAN setup add (or edit) screen, this screen displays next. Use this screen to configure PPPoA connection settings.

Figure 25   Advanced Setup > WAN > Add (3: PPPoA)

The following table describes the labels in this screen.

Table 15   Advanced Setup > WAN > Add (3: PPPoA)

LABEL	DESCRIPTION
PPP User Name	Enter the login name that your ISP gives you.
PPP Password	Enter the password associated with the user name above.

Table 15 Advanced Setup > WAN > Add (3: PPPoA) (continued)

LABEL	DESCRIPTION
Authentication Method	The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO** - Your ZyXEL Device accepts either CHAP, PAP, or MSCHAP when requested by this remote node. **CHAP** - Your ZyXEL Device accepts CHAP only. **PAP** - Your ZyXEL Device accepts PAP only. **MSCHAP** - Your ZyXEL Device accepts MSCHAP (Microsoft CHAP) only.
Enable NAT	Turn on NAT to translate IP addresses between two different networks (so you can have a private LAN with IP addresses that are different from the public IP addresses on the WAN. See Chapter 7 on page 83 for more details.
Enable Fullcone NAT	This field displays when you enable NAT. In full cone NAT, all requests from the same private IP address and port are mapped to the same public source IP address and port. Someone on the Internet only needs to know the mapping scheme in order to send packets to a device behind the ZyXEL Device. The ZyXEL Device uses restricted cone NAT when you disable full cone NAT.
Enable Firewall	Select this to turn on the ZyXEL Device's Stateful Packet Inspection (SPI) firewall. By default the firewall blocks traffic originating from the WAN from going to the LAN. See Chapter 8 on page 93 for how to configure firewall rules.
Dial on demand	Select **Dial on demand** when you don't want the connection up all the time and specify an idle time-out (in seconds) in the **Inactivity Timeout** field. Clear the **Dial on demand** option to keep the connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
PPP IP extension	Only select this option if your service provider requires it. The following conditions apply to a connection using PPP IP extension. • Only one computer can be connected on the LAN. • The ISP only assigns a single public IP address and the LAN computer uses it on its LAN interface. • The firewall and NAT features are disabled. • The ZyXEL Device uses DHCP to tell the LAN computer that the ZyXEL Device is its default gateway and DNS server. • The ZyXEL Device extends the ISP's IP subnet to the LAN computer. • The ZyXEL Device bridges packets between the DSL and LAN interface, except for packets destined for the ZyXEL Device's LAN IP address.

Table 15 Advanced Setup > WAN > Add (3: PPPoA) (continued)

LABEL	DESCRIPTION
Use Static IP Address	If the ISP gave you a static (fixed) IP address, select this option and enter it in the **IP Address** field. If the ISP did not give you a static IP address, clear the **Use Static IP Address** option. The ISP automatically assigns the WAN connection an IP address when it connects.
Enable PPP debug mode	Select this to turn on the debug mode for the PPP connection.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.11 PPPoE WAN Connection Setup

When you select PPPoE in the second WAN setup add (or edit) screen, this screen displays next. Use this screen to configure PPPoE connection settings.

Figure 26   Advanced Setup > WAN > Add (3: PPPoE)

The following table describes the labels in this screen.

Table 16   Advanced Setup > WAN > Add (3: PPPoE)

LABEL	DESCRIPTION
PPP User Name	Enter the login name that your ISP gives you.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the PPPoE service name given to you by your ISP. PPPoE uses a service name to identify and reach the PPPoE server.

Table 16 Advanced Setup > WAN > Add (3: PPPoE) (continued)

LABEL	DESCRIPTION
Authentication Method	The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.
	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:
	AUTO - Your ZyXEL Device accepts either CHAP, PAP, or MSCHAP when requested by this remote node.
	CHAP - Your ZyXEL Device accepts CHAP only.
	PAP - Your ZyXEL Device accepts PAP only.
	MSCHAP - Your ZyXEL Device accepts MSCHAP (Microsoft CHAP) only.
Enable NAT	Turn on NAT to translate IP addresses between two different networks (so you can have a private LAN with IP addresses that are different from the public IP addresses on the WAN. See Chapter 7 on page 83 for more details.
Enable Fullcone NAT	This field displays when you enable NAT. In full cone NAT, all requests from the same private IP address and port are mapped to the same public source IP address and port. Someone on the Internet only needs to know the mapping scheme in order to send packets to a device behind the ZyXEL Device.
	The ZyXEL Device uses restricted cone NAT when you disable full cone NAT.
Enable Firewall	Select this to turn on the ZyXEL Device's Stateful Packet Inspection (SPI) firewall. By default the firewall blocks traffic originating from the WAN from going to the LAN. See Chapter 8 on page 93 for how to configure firewall rules.
Dial on demand	Select **Dial on demand** when you don't want the connection up all the time and specify an idle time-out (in seconds) in the **Inactivity Timeout** field.
	Clear the **Dial on demand** option to keep the connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
PPP IP extension	Only select this option if your service provider requires it. The following conditions apply to a connection using PPP IP extension.
	• Only one computer can be connected on the LAN.
	• The ISP only assigns a single public IP address and the LAN computer uses it on its LAN interface.
	• The firewall and NAT features are disabled.
	• The ZyXEL Device uses DHCP to tell the LAN computer that the ZyXEL Device is its default gateway and DNS server.
	• The ZyXEL Device extends the ISP's IP subnet to the LAN computer.
	• The ZyXEL Device bridges packets between the DSL and LAN interface, except for packets destined for the ZyXEL Device's LAN IP address.

Table 16 Advanced Setup > WAN > Add (3: PPPoE) (continued)

LABEL	DESCRIPTION
Use Static IP Address	If the ISP gave you a static (fixed) IP address, select this option and enter it in the **IP Address** field. If the ISP did not give you a static IP address, clear the **Use Static IP Address** option. The ISP automatically assigns the WAN connection an IP address when it connects.
Enable PPP debug mode	Select this to turn on the debug mode for the PPP connection.
Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)	This feature is available when you do not select **PPP IP extension**. In addition to the ZyXEL Device's built-in PPPoE client, you can enable this to pass PPPoE through in order to allow LAN hosts to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.12 MER WAN Connection Setup

When you select MER in the second WAN setup add (or edit) screen, this screen displays next. Use this screen to configure MER connection settings.

Figure 27   Advanced Setup > WAN > Add (3: MER)

The following table describes the labels in this screen.

Table 17   Advanced Setup > WAN > Add (3: MER)

LABEL	DESCRIPTION
Obtain an IP address automatically	The WAN connection's IP address identifies the ZyXEL Device on the Internet. If the ISP did not give you a static IP address, select **Obtain an IP address automatically**. The ISP automatically assigns the WAN connection an IP address when it connects.
Use the following IP address	If the ISP gave you a static (fixed) IP address, select this option and enter the connection's IP address and subnet mask.
Obtain default gateway automatically	The default is a neighboring router that helps the ZyXEL Device forward traffic to its destination. If the ISP did not give you the IP address of the default gateway, select **Obtain default gateway automatically**. The ISP automatically assigns the WAN connection an IP address when it connects.
Use the following default gateway	Select this option to use a specific default gateway. Either enter the gateway's IP address or select the WAN interface to use to connect to it.

Table 17 Advanced Setup > WAN > Add (3: MER) (continued)

LABEL	DESCRIPTION
Obtain DNS server addresses automatically	The ZyXEL Device uses a DNS server to resolve a domain name (find the numeric IP address associated with the domain name). Select this option if the ISP did not give you a specific DNS server IP address. The ISP automatically assigns the DNS server IP addresses when the ZyXEL Device connects.
Use the following DNS server addresses	If the ISP gave you DNS server IP addresses, select this option and enter them in the fields below.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.13 IPoA WAN Connection Setup

When you select IPoA in the second WAN setup add (or edit) screen, this screen displays next. Use this screen to configure IPoA connection settings.

Figure 28 Advanced Setup > WAN > Add (3: IPoA)

The following table describes the labels in this screen.

Table 18 Advanced Setup > WAN > Add (3: IPoA)

LABEL	DESCRIPTION
WAN IP Address	Enter the IP address from the ISP. Use dotted decimal notation (like 192.168.1.1 for example).
WAN Subnet Mask	Enter the subnet mask from the ISP. Use dotted decimal notation (like 255.255.0.0 for example).

Table 18   Advanced Setup > WAN > Add (3: IPoA) (continued)

LABEL	DESCRIPTION
Use the following default gateway	The default is a neighboring router that helps the ZyXEL Device forward traffic to its destination. Select this option and enter the gateway's IP address or select the WAN interface to use to connect to it.
Use the following DNS server addresses	The ZyXEL Device uses a DNS server to resolve a domain name (find the numeric IP address associated with the domain name). Select this option. Enter the DNS server addresses from the ISP in the fields below.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.14 Bridge WAN Connection Setup

When you select bridge in the second WAN setup add (or edit) screen, this screen displays next. Use this screen to configure bridge connection settings.

Figure 29   Advanced Setup > WAN > Add (3: Bridge)

The following table describes the labels in this screen.

Table 19   Advanced Setup > WAN > Add (3: Bridge)

LABEL	DESCRIPTION
Enable Bridge Service	Select this to turn on bridging for this DSL connection.
Service Name	If the ISP specified a service name to use for the DSL connection, enter it here. Otherwise leave the default generated text.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.15 IGMP Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network).

Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

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

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

5.16 NAT, IGMP Multicast, and WAN Service

This is the fourth WAN screen to display for every connection type except bridging (for which this is the third screen). This screen varies depending on the connection type. Use this screen to configure NAT, IGMP multicast, and WAN service settings.

Figure 30   Advanced Setup > WAN > Add (4: MER)

The following table describes the labels in this screen.

Table 20   Advanced Setup > WAN > Add (4: MER)

LABEL	DESCRIPTION
Enable NAT	Turn on NAT to translate IP addresses between two different networks (so you can have a private LAN with IP addresses that are different from the public IP addresses on the WAN. See Chapter 7 on page 83 for more details.
Enable Fullcone NAT	This field displays when you enable NAT. In full cone NAT, all requests from the same private IP address and port are mapped to the same public source IP address and port. Someone on the Internet only needs to know the mapping scheme in order to send packets to a device behind the ZyXEL Device. The ZyXEL Device uses restricted cone NAT when you disable full cone NAT.
Enable Firewall	Select this to turn on the ZyXEL Device's Stateful Packet Inspection (SPI) firewall. By default the firewall blocks traffic originating from the WAN from going to the LAN. See Chapter 8 on page 93 for how to configure firewall rules.
Enable IGMP Multicast	IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Turn this on to allow multicast traffic and have the ZyXEL Device act as an IGMP proxy.
Enable WAN Service	Select this option to use this WAN connection or clear the option to not use this WAN connection.

Table 20 Advanced Setup > WAN > Add (4: MER) (continued)

LABEL	DESCRIPTION
Service Name	This is the name for the WAN connection. Use the default or define your own.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.17 WAN Setup Summary

This is the last WAN setup screen to display. Use this screen to check your settings before saving them. Click **Back** if you need to make any changes. If the settings are OK, click **Save** to save the settings. Use the **Save/Reboot** button in the **Advanced Setup > WAN** screen to restart the ZyXEL Device and use the WAN connection settings.

Figure 31 Advanced Setup > WAN > Add (Summary: MER)

6

LAN Setup

This chapter describes how to configure LAN settings.

6.1 LAN Overview

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

See to configure the **LAN** screens.

6.1.1 LAN, WAN and the ZyXEL Device

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

Figure 32   LAN and WAN IP Addresses
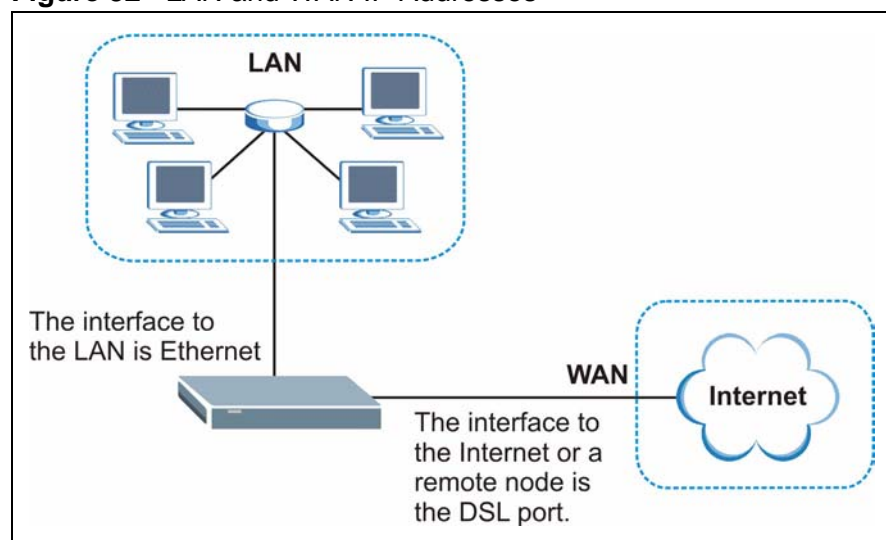
6.1.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured. Do not assign static IP addresses from the DHCP pool to your LAN computers.

6.2 LAN TCP/IP

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

6.2.1 IP Address and Subnet Mask

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

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

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

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

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP

address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

6.2.1.1 Private IP Addresses

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

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

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

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

6.3 Multicast

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

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

to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

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

6.4 Introducing Universal Plug and Play

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.

6.4.1 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.

6.4.2 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.

6.4.3 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 ZyXEL Device allows multicast messages only on the LAN.

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

You must have IIS (Internet Information Services) enabled on the Windows web server for UPnP to work.

6.5 LAN Setup

Click **Advanced Setup > LAN** to open the **IP** screen. See Section 6.1 on page 75 for background information. Some fields may not display depending on your WAN configuration.

Figure 33   Advanced Setup > LAN

The following table describes the fields in this screen.

Table 21   Advanced Setup > LAN

LABEL	DESCRIPTION
IP Address	Enter the LAN IP address of your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask.

Table 21 Advanced Setup > LAN (continued)

LABEL	DESCRIPTION
Enable UPnP	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 ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Enable IGMP Snooping	Turn on IGMP snooping to reduce network traffic by having the ZyXEL Device only forward multicast traffic to ports connected to computers or devices that belong to the specific multicast group. Use standard mode to flood unknown multicast traffic. Use blocking mode to discard unknown multicast traffic.
Disable/Enable DHCP Server	Turn on the DHCP server to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to DHCP clients on the LAN. Enter IP addresses in the **Start** and **End IP Address** fields to set a range of IP addresses for the ZyXEL Device to give to the DHCP clients. Enter an IP address in the **Start IP Address** field and a subnet mask in the **Subnet Mask** field to set a subnet of IP addresses for the ZyXEL Device to give to the DHCP clients. **Leased Time** sets how many hours to let a DHCP client use an IP before re-assigning it an IP address.
Static IP Lease List	Configure static IP addresses the ZyXEL Device's DHCP server assigns to specific LAN computers. If a computer's MAC address is in the LAN's static DHCP table, the ZyXEL Device assigns the corresponding IP address. Otherwise, the ZyXEL Device assigns an IP address dynamically.
MAC Address	This is the MAC address of a LAN computer.
IP Address	This is the IP address the ZyXEL Device assigns to the device with this entry's MAC address.
Remove	Select this for one or more entries and click **Remove Entries** to remove the entries.
Add Entries	Click this to go to the screen where you can configure a static DHCP IP entry.
Remove Entries	Select **Remove** for one or more entries and click this to remove the entries.
Configure the second IP address and subnet mask for LAN interface	Select this option to let the ZyXEL Device use a second IP address on the LAN interface. You can also use this second IP address to access the ZyXEL Device for management. Enter the LAN IP address of your ZyXEL Device in dotted decimal notation, for example, 10.0.0.1. Type the subnet mask.
Save	Click **Save** to save your changes to the ZyXEL Device.
Save/Reboot	Click this button to apply and save your changes. The ZyXEL Device restarts.

6.6 The DHCP Static Lease Screen

In the **Advanced Setup > LAN** screen, click **Add Entries** to open the **DHCP Static Lease** screen. Use this screen to configure the list of static IP addresses the ZyXEL Device assigns to computers connected to the interface. If a computer's MAC address is in the LAN's static DHCP table, the ZyXEL Device assigns the corresponding IP address. Otherwise, the ZyXEL Device assigns an IP address dynamically using the interface's **Start Address** and **Pool Size**.

You must click **Save/Apply** in this screen and then **Save** in the LAN setup screen to save your changes.

Figure 34 DHCP Static IP Lease

The following table describes this screen.

Table 22 Static DHCP

LABEL	DESCRIPTION
MAC Address	Enter the MAC address to which to assign this entry's IP address.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
Save/Apply	Click this to save your changes.

Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the ZyXEL Device.

7.1 NAT Overview

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

7.2 NAT Virtual Servers

Configure NAT virtual server (port forwarding) entries to have the ZyXEL Device forward traffic from the WAN to LAN computers.

You might do this to get particular games or services to work through NAT. You can also make servers, for example, web or FTP, visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

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

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.

7.2.1 Virtual Server: Services and Port Numbers

See for commonly used port numbers.

7.2.2 Virtual Servers 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 35   Multiple Servers Behind NAT Example
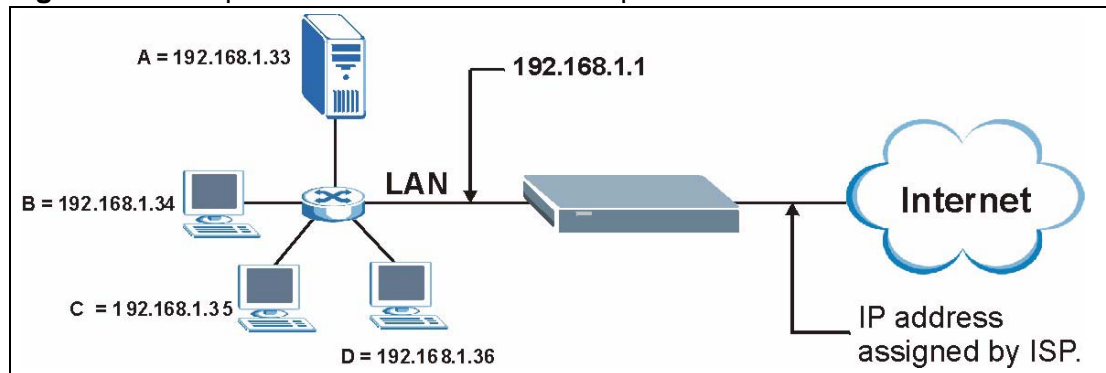
7.3 Configuring Virtual Servers

Note: The NAT screens are available only when you enable NAT in the WAN configuration.

Click **Advanced Setup > NAT > Virtual Servers** to open the following screen.

Figure 36 Advanced Setup > NAT > Virtual Servers

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Add   Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
Diablo II	4000	4000	TCP	4000	4000	192.168.1.100	☐
Diablo II	6112	6119	UDP	6112	6119	192.168.1.100	☐

See Appendix E on page 279 for port numbers commonly used for particular services. The following table describes the fields in this screen.

Table 23 NAT Port Forwarding

LABEL	DESCRIPTION
Add	Click this button to go to a screen where you can configure a new entry.
Remove	To remove an entry(ies), select its **Remove** check box and click the **Remove** button.
Server Name	This name identifies the virtual server entry.
External Port Start, External Port End	These are the ports of traffic coming in from the WAN to which this virtual server entry applies.
Protocol	This is the underlying protocol of the traffic to which this virtual server entry applies.
Internal Port Start, Internal Port End	These are the ports the ZyXEL Device uses for the traffic that it forwards based on this virtual server entry.
Server IP Address	This is the LAN IP address to which the ZyXEL Device forwards the incoming traffic.

7.3.1 Virtual Server Rule Add

To create a virtual server rule, click **Advanced Setup > NAT > Virtual Servers > Add** to open the following screen.

Figure 37 Advanced Setup > NAT > Virtual Servers > Add

The following table describes the fields in this screen.

Table 24 Advanced Setup > NAT > Virtual Servers > Add

LABEL	DESCRIPTION
Server Name	Either select a pre-defined service or select **Custom Server** and enter a name manually.
Server IP Address	Enter the LAN IP address to which the ZyXEL Device should forward the traffic.
Save/Apply	When using a pre-defined service, if you do not want to modify the port numbers, you can click this button to save the changes and have the ZyXEL Device start using them.

Table 24 Advanced Setup > NAT > Virtual Servers > Add (continued)

LABEL	DESCRIPTION
External Port Start	Enter a port number in this field.
	To forward only one port, enter the port number again in the **External Port End** field.
	To forward a series of ports, enter the start port number here and the end port number in the **External Port End** field.
External Port End	Enter a port number in this field.
	To forward only one port, enter the port number again in the **Start Port** field above and then enter it again in this field.
	To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above.
Protocol	This is the underlying protocol of the traffic to which this virtual server entry applies.
Internal Port Start	Specify the starting port the ZyXEL Device uses for the traffic that it forwards based on this virtual server entry (or leave it the same as the External
Internal Port End	The ZyXEL Device automatically determines this port number.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

7.4 Port Triggering

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 ZyXEL Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyXEL Device's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyXEL Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 38 Trigger Port Forwarding Process: Example
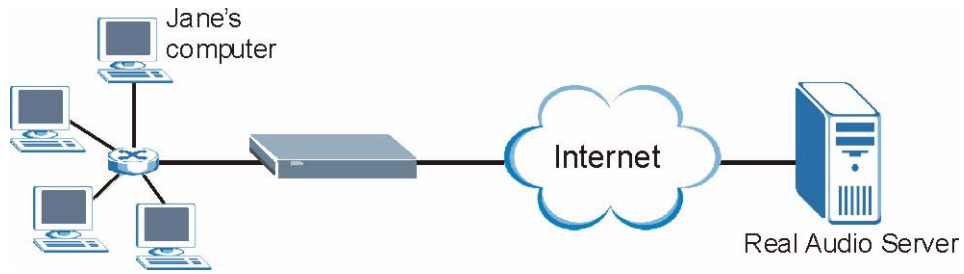
1 Jane (A) requests a file from the Real Audio server (port 7070).

2 Port 7070 is a "trigger" port and causes the ZyXEL Device to record Jane's computer IP address. The ZyXEL Device 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 ZyXEL Device forwards the traffic to Jane's computer IP address.

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

Click **Advanced Setup > NAT** > **Port Triggering** to open the following screen. Use this screen to change your ZyXEL Device's trigger port settings.

Figure 39 Advanced Setup > NAT > Port Triggering

The following table describes the labels in this screen.

Table 25 Advanced Setup > NAT > Port Triggering

LABEL	DESCRIPTION
Add	Click this button to go to a screen where you can configure a new entry.
Remove	To remove an entry(ies), select its **Remove** check box and click the **Remove** button.
Application	Name for identification purposes.
Trigger	The trigger port is a protocol and port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Open	Open is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.

7.5 Port Triggering Add

Click **Advanced Setup > NAT** > **Port Triggering > Add** to open the following screen. Use this screen to change your ZyXEL Device's trigger port settings.

Figure 40   Advanced Setup > NAT > Port Triggering > Add

89

The following table describes the labels in this screen.

Table 26 Advanced Setup > NAT > Port Triggering > Add

LABEL	DESCRIPTION
Application Name	Either select a pre-defined application or select **Custom Application** and enter a name manually.
Save/Apply	When using a pre-defined service, if you do not want to modify the port numbers, you can click this button to save the changes and have the ZyXEL Device start using them.
Trigger	The trigger port is a protocol and port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Trigger Port Start	Type a port number or the starting port number in a range of port numbers.
Trigger Port End	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the protocol.
Open	Open is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Open Start Port	Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the protocol.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

7.6 DMZ Host

In addition to the virtual servers for specified services, NAT supports a DMZ host IP address. The DMZ host receives packets from ports that are not specified in the applications in the virtual server configuration.

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

Click **Advanced Setup > NAT** > **DMZ Host** to open the following screen. Use this screen to specify a DMZ host IP address.

Figure 41 Advanced Setup > NAT > DMZ Host

NAT -- DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

Save/Apply

The following table describes the labels in this screen.

Table 27 Advanced Setup > NAT > Port Triggering > Add

LABEL	DESCRIPTION
DMZ Host IP Address	Specify the IP address of the LAN computer to which you want to send packets from ports that are not specified in the applications in the virtual server configuration.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

8

Security

This chapter describes how to configure security settings.

8.1 Outgoing IP Filtering

By default, the ZyXEL Device allows traffic from the LAN to go to the Internet. Click **Advanced Setup > Security > IP Filtering > Outgoing** to open the following screen. This screen lists the currently configured filtering entries.

Figure 42   Advanced Setup > Security > IP Filtering > Outgoing

The following table describes the labels in this menu.

Table 28   Advanced Setup > Security > IP Filtering > Outgoing

LABEL	DESCRIPTION
Filter Name	This is the name configured to identify the filter entry.
Protocol	This is the type of packets to which this entry applies.
Source Address / Mask	This is the IP address and subnet mask of a LAN computer to which this entry applies.
Source Port	This is the source port for traffic (from the LAN) to which this entry applies.
Dest. Address / Mask	This is the IP address and subnet mask of a computer on the Internet to which this entry applies.
Dest. Port	This is the destination port for traffic to which this entry applies.
Remove	To remove a rule, select its **Remove** check box and click the **Remove** button.

Table 28 Advanced Setup > Security > IP Filtering > Outgoing

LABEL	DESCRIPTION
Add	Click this button to go to a screen where you can configure settings for a new entry.
Remove	To remove a WAN connection, select its **Remove** check box and click the **Remove** button.

8.2 Adding Outgoing IP Filtering Rules

To add an outgoing IP filtering rule, click **Advanced Setup > Security > IP Filtering > Outgoing > Add**. The screen appears as shown.

Figure 43 Advanced Setup > Security > IP Filtering > Outgoing > Add

The following table describes the labels in this menu.

Table 29 Advanced Setup > Security > IP Filtering > Outgoing > Add

LABEL	DESCRIPTION
Filter Name	Type the name configured to identify the filter entry.
Protocol	Select the type of packets to which this entry applies (TCP, UDP, or both).
Source IP Address	Type the IP address of a LAN computer to which this entry applies.
Source Subnet Mask	Type the subnet mask of a LAN computer to which this entry applies.
Source Port	Type the source port for traffic (from the LAN) to which this entry applies.
Destination IP Address	This is the IP address and subnet mask of a computer on the Internet to which this entry applies.
Destination Subnet Mask	Type the subnet mask of a computer on the Internet to which this entry applies.

Table 29 Advanced Setup > Security > IP Filtering > Outgoing > Add

LABEL	DESCRIPTION
Destination Port	Type the destination port for traffic to which this entry applies.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

8.3 Incoming IP Filtering

By default, the ZyXEL Device blocks traffic from the Internet from going to the LAN. Use incoming IP filtering to allow certain traffic to come in from the Internet to the LAN. For example, you could allow access to a web server on your LAN to let people access a website that it is hosting. Click **Advanced Setup > Security > IP Filtering > Incoming** to open the following screen. This screen lists the currently configured filtering entries.

Figure 44 Advanced Setup > Security > IP Filtering > Incoming

The following table describes the labels in this menu.

Table 30 Advanced Setup > Security > IP Filtering > Incoming

LABEL	DESCRIPTION
Filter Name	This is the name configured to identify the filter entry.
VPI/VCI	This is the WAN connection's Virtual Path Identifier, and Virtual Channel Identifier.
Protocol	This is the type of packets to which this entry applies.
Source Address / Mask	This is the IP address and subnet mask of a computer (on the Internet) to which this entry applies.
Source Port	This is the source port for traffic (from the Internet) to which this entry applies.
Dest. Address / Mask	This is the IP address and subnet mask of a LAN computer to which this entry allows traffic from the Internet.
Dest. Port	This is the destination port for traffic to which this entry applies.
Remove	To remove a rule, select its **Remove** check box and click the **Remove** button.

Table 30   Advanced Setup > Security > IP Filtering > Incoming

LABEL	DESCRIPTION
Add	Click this button to go to a screen where you can configure settings for a new entry.
Remove	To remove a WAN connection, select its **Remove** check box and click the **Remove** button.

8.4 Adding Incoming IP Filtering Rules

To add an incoming IP filtering rule, click **Advanced Setup > Security > IP Filtering > Incoming > Add**. The screen appears as shown.

Figure 45   Advanced Setup > Security > IP Filtering > Incoming > Add

The following table describes the labels in this menu.

Table 31   Advanced Setup > Security > IP Filtering > Incoming > Add

LABEL	DESCRIPTION
Filter Name	Type the name configured to identify the filter entry.
Protocol	Select the type of packets to which this entry applies (TCP, UDP, or both).
Source IP Address	Type the IP address of a computer on the Internet to which this entry applies.
Source Subnet Mask	Type the subnet mask of a computer on the Internet to which this entry applies.
Source Port	Type the source port for traffic (from the Internet) to which this entry applies.

Table 31 Advanced Setup > Security > IP Filtering > Incoming > Add

LABEL	DESCRIPTION
Destination IP Address	This is the IP address and subnet mask of a LAN computer to which this entry allows access.
Destination Subnet Mask	Type the subnet mask of the LAN computer to which this entry applies.
Destination Port	Type the destination port for traffic to which this entry applies.
WAN Interfaces	Select the WAN interface(s) to which this rule applies.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

Parental Control (Blocking Schedule)

Click **Advanced Setup > Security > Parental Control** to display the following screen. This screen shows policies controlling which days and times Internet access is blocked from specific MAC addresses.

Figure 46 Advanced Setup > Security > Parental Control

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
example	00:0f:fe:1e:4a:e0						x	x	00:00	00:00	☐

Time of Day Restrictions -- A maximum 16 entries can be configured.

Add   Remove

The following table describes the labels in this screen.

Table 32 Advanced Setup > Security > Parental Control

LABEL	DESCRIPTION
Username	This name identifies to whom the blocking schedule applies.
MAC	This is the MAC address of the computer to which this blocking schedule applies.
Mon ~ Sun	These fields show to which days of the week the blocking schedule applies.
Start	This is the beginning time for the blocked access period.
Stop	This is the ending time for the blocked access period.
Add	Click this button to go to a screen where you can configure settings for a new entry.
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.

9.1 Adding Parental Control (Blocking Schedule) Entries

Click **Advanced Setup > Security > Parental Control > Add** to display the following screen. Use this screen to configure which days and times Internet access is blocked from a specific MAC address.

Figure 47 Advanced Setup > Security > Parental Control > Add

The following table describes the labels in this screen.

Table 33 Advanced Setup > Security > Parental Control > Add

LABEL	DESCRIPTION
Username	Enter a name to identify to whom the blocking schedule applies.
Browser's MAC	Select this to use the MAC address of the computer you are currently using to manage the ZyXEL Device.
Other MAC Address	Select this to manually enter the MAC address of a computer.
Days of the week	Select to which days of the week the blocking schedule applies.
Start Blocking Time	This is the beginning time for the blocking period. Include a two-digit number of hours followed by a colon and a. two-digit number of hours.

Table 33   Advanced Setup > Security > Parental Control > Add

LABEL	DESCRIPTION
End Blocking Time	This is the ending time for the blocking period. Include a two-digit number of hours followed by a colon and a. two-digit number of hours.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

10

Quality of Service (QoS)

This chapter contains information about configuring QoS, editing classifiers and viewing the ZyXEL Device's QoS packet statistics.

10.1 QoS Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

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

1 Configure classifiers to sort traffic into different flows.

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

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

Note: The ZyXEL Device applies QoS to upstream traffic (going out through the WAN interface).

10.1.1 IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the

12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

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

Table 34   IEEE 802.1p Priority Level and Traffic Type

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

10.1.2 IP Precedence

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

10.1.3 DiffServ

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

DiffServ (Differentiated Services) is a Class of Service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices

to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

10.1.3.1 DSCP and Per-Hop Behavior

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

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

DSCP (6 bits)	Unused (2 bits)
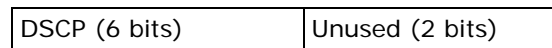
The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

10.2 Configuring QoS General Screen

Click **Advanced > Quality of Service** to open the screen as shown next.

Use this screen to enable or disable QoS, and select a DSCP mark to use on all outgoing packets that do not match a QoS classification rule.

Figure 48   Advanced > Quality of Service

The following table describes the labels in this screen.

Table 35   Advanced > Quality of Service

LABEL	DESCRIPTION
Enable QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
Select Default DSCP Mark	Select a DSCP mark to use on all outgoing packets that do not match a QoS classification rule. You can select a specific DSCP mark to use or have the ZyXEL Device automatically select a DSCP mark to use.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

10.3 Queue Configuration

Click **Advanced > Quality of Service** > **Queue Configuration** to open the following screen. This screen lists the QoS queues. A QoS queue sets the priority used for incoming packets that the QoS classifier has grouped into a flow.

Figure 49   Advanced > Quality of Service > Queue Configuration

The following table describes the labels in this screen.

Table 36   Advanced > Quality of Service > Queue Configuration

LABEL	DESCRIPTION
Interface name	This field displays to which interface the queue applies. If it is a WAN connection, the WAN connection's DSL port, Virtual Path Identifier, and Virtual Channel Identifier display here.
Description	This field displays any extra configured identification information.
Precedence	This shows the queue's priority relative to the other queues. The lower the number, the higher the priority.
Queue Key	This is the queue entry's index number.
Enable	Select the check box to enable this classifier.
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new QoS queue.
Remove	To remove an entry select its **Remove** check box and click the **Remove** button.
Save/Reboot	Click this button to apply and save your changes. The ZyXEL Device restarts.

10.4 Adding a Queue

Click **Advanced > Quality of Service** > **Queue Configuration > Add** to open the following screen. Use this screen to configure a QoS queue. A QoS queue sets the priority used for incoming packets that the QoS classifier has grouped into a flow.

Note: You can only add QoS queues for WAN interfaces that have QoS enabled.

Figure 50   Advanced > Quality of Service > Queue Configuration > Add

The following table describes the labels in this screen.

Table 37   Advanced > Quality of Service > Queue Configuration > Add

LABEL	DESCRIPTION
Queue Configuration Status	Select **Enable** to turn on this queue.
Queue	Select the WAN connection's DSL port, Virtual Path Identifier, and Virtual Channel Identifier.
Description	This field displays any extra configured identification information.
Queue Precedence	Set the queue's priority relative to the other queues. The lower the number, the higher the priority. 1 is the highest priority. 4 is the lowest.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

10.5 Class Setup

Click **Advanced > Quality of Service** > **QoS Classification** to open the following screen.

This screen lists the QoS classifiers. A classifier groups upstream traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow. The classifier also assigns a specific QoS queue, DSCP mark, and/or IEEE 802.1p tag.

Figure 51   Advanced > Quality of Service > QoS Classification

The following table describes the labels in this screen.

Table 38   Advanced > Quality of Service > QoS Classification

LABEL	DESCRIPTION
Class Name	This is the name of the classifier.
MARK	These columns are the QoS setting the ZyXEL Device uses for or assigns to the packets of upstream traffic that match this QoS classifier.
DSCP Mark	This is the DSCP mark the ZyXEL Device assigns to the packets of upstream traffic that match this QoS classifier.
Queue ID	This is the QoS queue the ZyXEL Device uses for the packets of upstream traffic that match this QoS classifier.
802.1P Mark	This is the IEEE 802.1p mark the ZyXEL Device assigns to the packets of upstream traffic that match this QoS classifier.
TRAFFIC CLASSIFICATION RULES	These columns identify the upstream traffic to which the QoS classifier applies.
Lan Port	This is the source Ethernet port of the traffic.
Protocol	This is the type of packets.
DSCP	This is the DSCP mark.
Source Addr./Mask	This is the IP address (and optionally the subnet mask) of the device that sent the traffic.
Source Port	This is the port number that a device used to send the traffic.

Table 38 Advanced > Quality of Service > QoS Classification (continued)

LABEL	DESCRIPTION
Dest. Addr./Mask	This is the IP address (and optionally the subnet mask) of the device that the traffic is going to.
Dest. Port	This is the port number on a device to which the traffic is going.
Source MAC Addr./Mask	This is the MAC address (and optionally the subnet mask) of the device that sent the traffic.
Dest. MAC Addr./ Mask	This is the MAC address (and optionally the subnet mask) of the device that the traffic is going to.
802.1P	This is the IEEE 802.1p mark on the traffic.
Order	This is the classifier's place in the classifiers list.
Enable / Disable	The classifier is active when this check box is selected.
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new QoS queue.
Remove	To remove an entry select its **Remove** check box and click the **Remove** button.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

10.5.1 Configuring a QoS Class

Click **Advanced > Quality of Service** > **QoS Classification** and then the **Add** or **Edit** button to configure a classifier. There are two sets of classification rules. Set-1 is based on different fields within the TCP/UDP/IP layer plus the physical

LAN port. Set-2 is based on the MAC layer IEEE 802.1p priority field. Use one set or the other for a class (not both sets).

Figure 52 QoS Class Configuration

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

Table 39 QoS Class Configuration

LABEL	DESCRIPTION
Traffic Class Name	Type a name for the classifier.
Rule Order	Select the classifier's place in the classifiers list.
Rule Status	Select whether or not the classifier is to be active.

Table 39   QoS Class Configuration (continued)

LABEL	DESCRIPTION
Assign Classification Queue	Select the QoS queue the ZyXEL Device uses for the packets of upstream traffic that match this QoS classifier.
Assign Differentiated Services Code Point (DSCP) Mark	Select the DSCP mark the ZyXEL Device assigns to the packets of upstream traffic that match this QoS classifier.
Mark 802.1p if 802.1q is enabled	Select the IEEE 802.1p mark the ZyXEL Device assigns to the packets of upstream traffic that match this QoS classifier. This only applies when IEEE 802.1q is enabled. You enable IEEE 802.1q by enabling VLAN multiplexing in the WAN screens (see Section 5.3 on page 55).
Physical LAN Port	Select the source Ethernet port of the traffic.
Protocol	Select the type of packets.
Differentiated Services Code Point (DSCP) Check	Select the DSCP mark to check upstream traffic for.
IP Address/ Vendor Class ID (DHCP Option 60)/ User class ID (DHCP option 77)	Select whether to check for a source IP address, vendor class ID, or user class ID. Then specify the source IP address, vendor class ID, or user class ID.
Source Subnet Mask	Specify the subnet mask of the device that sent the traffic.
UDP/TCP Source Port (port or port:port)	This is the port number that a device used to send the traffic.
Destination IP Address	Specify the IP address of the device that the traffic is going to.
Destination Subnet Mask	Specify the subnet mask of the device that the traffic is going to.
UDP/TCP Destination Port (port or port:port)	Specify the port number on a device to which the traffic is going.
Source MAC Address	Specify the MAC address of the device that sent the traffic.
Source MAC Mask	Specify the MAC address subnet mask of the device that sent the traffic.
Destination MAC Address	Specify the MAC address of the device that the traffic is going to.
Destination MAC Mask	Specify the MAC address subnet mask of the device that the traffic is going to.
802.1p Priority	Specify the IEEE 802.1p mark on the traffic.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

Routing

This chapter shows you how to configure the default gateway and static routes for your ZyXEL Device.

11.1 Default Gateway Setup

The default gateway is a neighboring router that helps the ZyXEL Device forward traffic to its destination. Click **Advanced > Routing > Default Gateway** to open the following screen. Use this screen to change the ZyXEL Device's default gateway settings.

Figure 53   Advanced Setup > Routing > Default Gateway

The following table describes the labels in this screen.

Table 40   Advanced Setup > Routing > Default Gateway

LABEL	DESCRIPTION
Enable Automatic Assigned Default Gateway	Select this option if the ISP did not give you the IP address of the default gateway. The ISP automatically assigns the WAN connection an IP address when it connects.
Use Default Gateway IP Address	If the ISP gave you a static (fixed) IP address, select this option and enter the connection's IP address.

Table 40 Advanced Setup > Routing > Default Gateway (continued)

LABEL	DESCRIPTION
Use Interface	To have the ZyXEL Device use a specific WAN interface for sending traffic to the default gateway, select this option and choose the WAN interface from the drop-down list box.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

11.2 Static Route

The ZyXEL Device usually uses the default gateway to route outbound traffic from local computers to the Internet. To have the ZyXEL Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the ZyXEL Device's LAN interface. The ZyXEL Device routes most traffic from **A** to the Internet through the 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 54 Example of Static Routing Topology
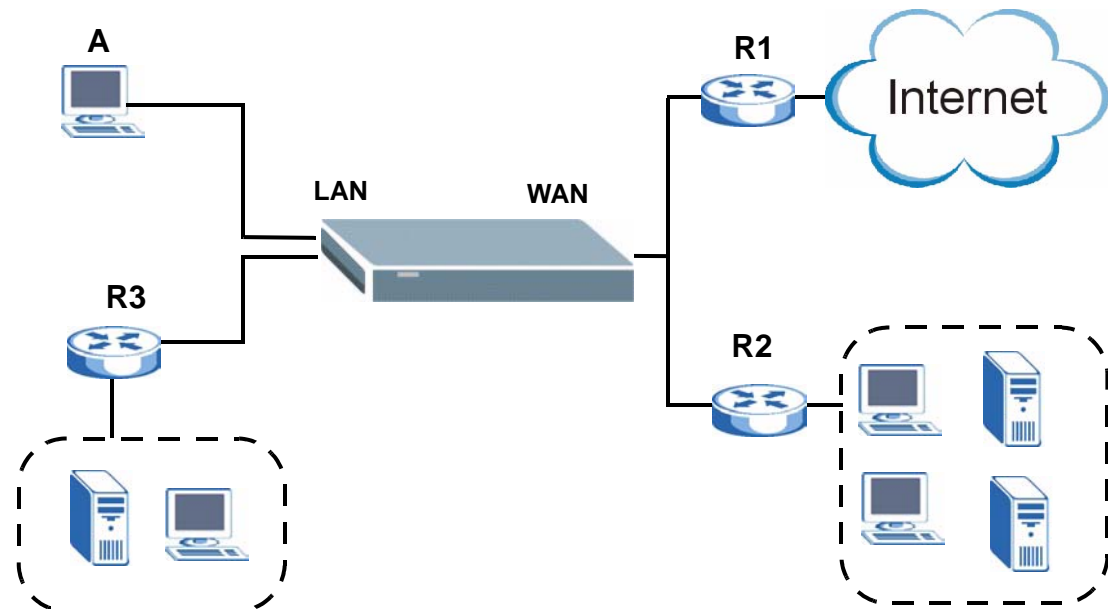
11.3 Configuring Static Route

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

Figure 55   Advanced > Routing > Static Route

Routing -- Static Route (A maximum 32 entries can be configured)

| Destination | Subnet Mask | Gateway | Interface | Remove |

Add   Remove

The following table describes the labels in this screen.

Table 41   Advanced > Routing > Static Route

LABEL	DESCRIPTION
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	This is the IP subnet mask.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	If the static route should send traffic through a specific ZyXEL Device interface, it displays here.
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new static route.
Remove	To remove an entry select its **Remove** check box and click the **Remove** button.

11.3.1 Static Route Add

Click **Advanced > Routing > Static Route > Add** to open the following screen. Use this screen to configure the required information for a static route.

Figure 56   Advanced > Routing > Static Route > Add

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.

Destination Network Address:
Subnet Mask:

☐ Use Gateway IP Address
☐ Use Interface

Save/Apply

The following table describes the labels in this screen.

Table 42 Advanced > Routing > Static Route > Add

LABEL	DESCRIPTION
Destination Network 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 of the destination network here.
Use Gateway IP Address	If you have a specific gateway IP address to enter, select this option and enter it in the field provided. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	If the static route should send traffic through a specific ZyXEL Device interface, select this option and choose the interface.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

12

RIP

This chapter covers configuring the RIP settings for your ZyXEL Device.

12.1 RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the ZyXEL Device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

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

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

Click **Advanced > Routing > RIP** to open the following screen. Use this screen to change the ZyXEL Device's RIP settings.

Figure 57 Advanced Setup > Routing > RIP

Routing -- RIP Configuration

To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

Global RIP Mode ⦿ Disabled ○ Enabled

Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	☐
ppp_0_0_33_1	0/0/33	2	Passive	☐

Save/Apply

The following table describes the labels in this screen.

Table 43 Advanced Setup > Routing > RIP

LABEL	DESCRIPTION
Global RIP Mode	Use these fields to turn RIP on or off for the whole ZyXEL Device. When you disable RIP, the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.
Interface	This field displays the name of the WAN connection.
VPN/VCI	The port (interface), VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) identify the ATM PVC (Permanent Virtual Circuit) to which these settings apply. "LAN" appears for a bridged connection.
Version	This field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.
Operation	RIP operation controls the sending and receiving of RIP packets. When set to **Active** the ZyXEL Device periodically broadcasts its routing table. When set to **Passive**, the ZyXEL Device uses the RIP information that it receives, but does not broadcast its routing table.
Enabled	Select or clear this field to turn RIP on or off for the interface.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

13

DNS Setup

This chapter describes how to configure DNS settings.

13.1 DNS Server Address

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

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

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

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

The ZyXEL Device acts as a DNS proxy when the **Primary** and **Secondary DNS Server** fields are left blank in the **LAN Setup** screen.

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

13.2 DNS Setup

Click **Advanced Setup > DNS > DNS Server** to open the following screen.

Figure 58   Advanced Setup > DNS > DNS Server

The following table describes the fields in this screen.

Table 44   Advanced Setup > DNS > DNS Server

LABEL	DESCRIPTION
Enable Automatic Assigned DNS	Select this option to have the ZyXEL Device accept and use the first DNS server IP address it gets from a WAN connection.
Primary DNS server	These fields are available when you clear **Enable Automatic Assigned DNS**.
Secondary DNS server	Enter the IP addresses of the DNS servers the ZyXEL Device is to use.
Save	Click **Save** to save your changes to the ZyXEL Device.

14

Dynamic DNS Setup

This chapter discusses how to configure your ZyXEL Device to use Dynamic DNS.

14.1 Dynamic DNS Overview

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

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

14.1.1 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.

See Section 14.2 on page 124 for configuration instruction.

14.2 Dynamic DNS

Click **Advanced Setup > DNS > Dynamic DNS** to open the following screen.

Figure 59   Advanced Setup > DNS > Dynamic DNS

The following table describes the fields in this screen.

Table 45   Advanced Setup > DNS > Dynamic DNS

LABEL	DESCRIPTION
Host Name	This is the domain name assigned to your ZyXEL Device by your Dynamic DNS provider.
User Name	This is the user name for the host name's DDNS account.
Service	This is the name of your Dynamic DNS service provider.
Interface	This is the ZyXEL Device's WAN connection that uses this DDNS host name.
Remove	To remove a DDNS entry, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new DDNS entry.
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.

14.3 Configuring Dynamic DNS

Click **Advanced Setup > DNS > Dynamic DNS > Add** to open the following screen.

Figure 60   Advanced Setup > DNS > Dynamic DNS > Add

The following table describes the fields in this screen.

Table 46   Advanced Setup > DNS > Dynamic DNS > Add

LABEL	DESCRIPTION
D-DNS Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your dynamic DNS provider.
Interface	Select the ZyXEL Device's WAN connection that uses this DDNS host name.
Active Dynamic DNS	Select this check box to use dynamic DNS.
Username	Type your user name for this DDNS host name.
Password	Type the password assigned for this DDNS host name.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

DSL Setup

This chapter explains how to configure ADSL port settings.

15.1 DSL Setup

Click **Advanced > DSL** to open the following screen where you can configure the ZyXEL Device's DSL settings.

Figure 61   Advanced > DSL

The following table describes the labels in this screen.

Table 47 Advanced > DSL

LABEL	DESCRIPTION
Select the modulation below	Select the port's ADSL operational mode. Select multiple modes to let the ZyXEL Device and the DSLAM automatically determine the mode to use. **AnnexL** (reach extended ADSL2) is an ADSL2+ mode that allows increased connection distances. **AnnexM** (double upstream mode) is an ADSL2+ mode that has the upstream connection use tones 6 to 63. The DSLAM's port must also be set to use Annex M or the **DSL2** port will not link up.
Bitswap Enable	Enable bit-swapping to allow the ZyXEL Device to adapt to line changes. It is recommended that you leave this enabled.
SRA Enable	Enable Seamless Rate Adaptation (SRA) to have the ZyXEL Device automatically adjust the connection's data rate according to line conditions without interrupting service.
Single Line Enable	Select this if you are using only one DSL line. This has the ZyXEL Device disable **DSL1** and only use **DSL2**.
Save/Reboot	Click this button to save the changes and have the ZyXEL Device restart and use them.

Interface Group

16.1 Interface Groups Overview

Interface Groups let you map ports to PVCs and create bridging groups.

16.2 Interface Groups Setup

Click **Advanced Setup > Interface Groups** to open the following screen. Use this screen to map ports to PVCs and create bridging groups.

Figure 62   Advanced Setup > Interface Groups

The following table describes the labels in this screen.

Table 48 Advanced Setup > Interface Groups

LABEL	DESCRIPTION
Enable virtual ports on	Select this option to treat the LAN ports as separate (virtual) interfaces.
Group Name	This is the name configured to identify the group.
Remove	To remove an entry, select its **Remove** check box and click the **Save/Apply** button.
Edit	Click Edit to configure the group's settings.
Interfaces	These are the interfaces that belong to the group.
Add	Click **Add** to open a screen where you can add a new entry.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

16.3 Adding an Interface Group

Click **Advanced Setup > Interface Groups > Add** to open the following screen. Use this screen to map ports to PVCs and create bridging groups.

Figure 63 Advanced Setup > Interface Groups > Add

The following table describes the labels in this screen.

Table 49 Advanced Setup > Interface Groups > Add

LABEL	DESCRIPTION
Group Name	Configure a name to identify the group.
Grouped Interfaces Available Interfaces	Select interfaces to add to the group.

Table 49   Advanced Setup > Interface Groups > Add (continued)

LABEL	DESCRIPTION
Automatically Add Clients With the following DHCP Vendor IDs	If you want LAN clients to get public IP addresses, you can list their DHCP vendor IDs here.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

CHAPTER 17
Certificates

17.1 Overview

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

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

Figure 64 Certificates Example
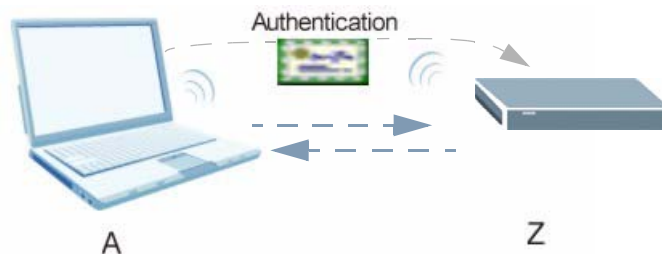
In the figure above, the ZyXEL Device (Z) checks the identity of the notebook (A) using a certificate before granting it access to the network.

17.1.1 What You Can Do in the Certificates Screens

- Use the **Trusted CAs** screens (Section 17.2 on page 134) to save CA certificates to the ZyXEL Device.

17.1.2 What You Need to Know About Certificates

Certification Authority

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

Certificate File Formats

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

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyXEL Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

Finding Out More

See Section 17.3 on page 137 for technical background information on certificates.

17.2 Trusted CA Certificates Screen

This screen displays a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities. Click **Advanced Setup > Certificate** to open the following screen.

Figure 65   Trusted CAs
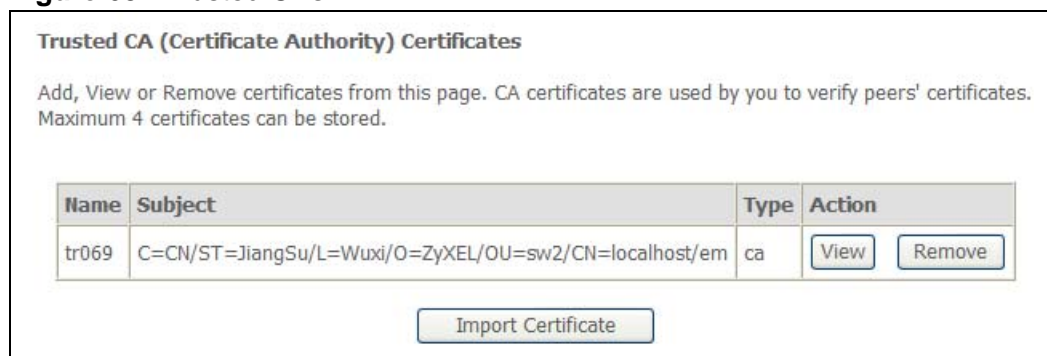
The following table describes the labels in this screen.

Table 50 Trusted CAs

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Action	Click **View** to see an imported CA certificate's details. Click **Remove** to delete the imported CA certificate from the ZyXEL Device.
Import Certificate	Click this to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.

17.2.1 Trusted CA Details

Use this screen to view in-depth information about the certification authority's certificate. Click **Advanced Setup > Certificate** to open the Trusted CAs screen. Then click a certificate's View button to open the details screen.

Figure 66 Trusted CA Details

The following table describes the labels in this screen.

Table 51 Trusted CA Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Certificate	This is the certificate's information displayed in plain text.
Back	Click this to return to the previous screen.

17.2.2 Trusted CA Import

Click **Advanced Setup > Certificate** to open the **Trusted CA** screen and then click **Import Certificate** to open the following screen. Use this screen to save a trusted certification authority's certificate to the ZyXEL Device.

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

Figure 67   Trusted CA Import

The following table describes the labels in this screen.

Table 52   Trusted CA Import

LABEL	DESCRIPTION
Certificate Name	Enter the name of the CA certificate.
Certificate	Open the trusted CA certificate in notepad and copy its information and paste it into this field.
Apply	Click this to save the certificate on the ZyXEL Device.

17.3 Certificates Technical Reference

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

17.3.1 Certificates Overview

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

The ZyXEL Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

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

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyXEL Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyXEL Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (Public-Key Infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

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

Self-signed Certificates

You can have the ZyXEL Device act as a certification authority and sign its own certificates.

17.3.2 Private-Public Certificates

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

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

1 Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).

2 Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.

3 Tim uses his private key to sign the message and sends it to Jenny.

4 Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

17.3.3 Verifying a Trusted Remote Host's Certificate

Certificates issued by certification authorities have the certification authority's signature for you to check. Self-signed certificates only have the signature of the host itself. This means that you must be very careful when deciding to import (and thereby trust) a remote host's self-signed certificate.

Trusted Remote Host Certificate Fingerprints

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to use a certificate's fingerprint to verify that you have the remote host's correct certificate.

139

1 Browse to where you have the remote host's certificate saved on your computer.

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

Figure 68 Remote Host Certificates
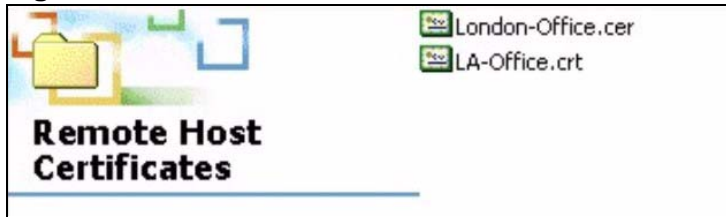
3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 69 Certificate Details
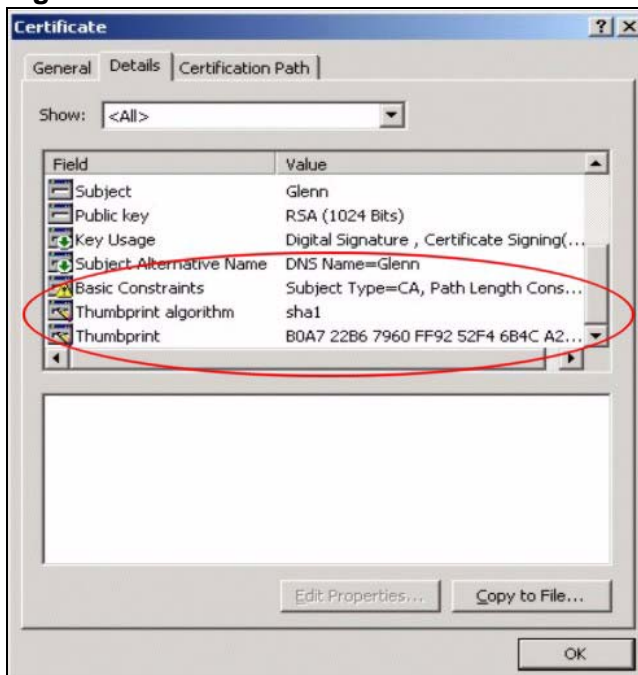
4 Verify (over the phone for example) that the remote host has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields.

18

Wireless LAN

18.1 Overview

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

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

See Section 18.10 on page 160 for advanced technical information on wireless networks.

18.1.1 What You Can Do in this Chapter

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

- The **Basic** screen lets you turn the wireless connection on or off and make other basic configuration changes (Section 18.4 on page 144).
- Use the **Security** screen (Section 18.5 on page 147) to configure wireless security using WiFi Protected Setup (WPS) or manually.
- The **MAC Filter** screen lets you configure the MAC filter to allow or block access to the ZyXEL Device based on the MAC addresses of the wireless stations (Section 18.6 on page 152).
- Use the **Wireless Bridge** screen (Section 18.7 on page 154) to configure wireless connections between the ZyXEL Device and other APs.
- The **Advanced Setup** screen lets you change the wireless mode and make other advanced wireless configuration changes (Section 18.8 on page 155).
- Use the **WPS Station** screen (Section 18.9 on page 159) to view information about the wireless stations connected to the ZyXEL Device.

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

18.2 What You Need to Know

Wireless Basics

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

Wireless Network Construction

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

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

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

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

Network Names

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

Radio Channels

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

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

Wireless Security

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

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

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

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

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your

mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

Signal Problems

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

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

18.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See Section 18.2 on page 142 if some of the terms used here do not make sense to you.

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

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

18.4 Wireless Basic

Click **Wireless** to open the **Basic** screen.

Note: If you have a wireless connection to the ZyXEL Device and you change the ZyXEL Device's SSID or country settings, you will lose your wireless connection when you click **Save/Apply**. You must then change your wireless client's settings to match the ZyXEL Device's new settings.

Figure 70 Wireless > Basic

The following table describes the labels in this screen.

Table 53 Wireless > Basic

LABEL	DESCRIPTION
Enable Wireless	Select this to turn on the wireless LAN.
Hide Access Point	Select this to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Clients Isolation	Select this to stop wireless clients from communicating directly with each other through the ZyXEL Device's wireless interface. This is also known as layer-2 isolation.
Disable WMM Advertise	WMM (Wifi MultiMedia) automatically prioritizes services according to the ToS value in the IP header of packets. Turn off WMM advertising if your wireless clients are not able to associate with an AP using WMM.

145

Table 53   Wireless > Basic

LABEL	DESCRIPTION
SSID	This is the name of the ZyXEL Device's wireless network. The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or channel 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 ZyXEL Device's new settings.
BSSID	This shows the MAC address of the wireless interface on the ZyXEL Device when wireless LAN is enabled.
Country	Select the country where the ZyXEL Device is located or the operating frequency/channel of your particular region. This sets the radio frequency the ZyXEL Device uses for wireless communications.
Max Clients	Specify the greatest number of wireless clients allowed to simultaneously connect to this wireless network on the ZyXEL Device.
Wireless - Guest/Virtual Access Points:	Use this part of the screen to configure up to three more wireless networks for guest users.
Enabled	Select this to turn on the wireless LAN.
SSID	This is the name of the ZyXEL Device's wireless network. The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or channel 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 ZyXEL Device's new settings.
Hidden	Select this to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Isolate Clients	Select this to stop wireless clients from communicating directly with each other through the ZyXEL Device's wireless interface. This is also known as layer 2 isolation.
Disable WMM Advertise	WMM (Wifi MultiMedia) automatically prioritizes services according to the ToS value in the IP header of packets. Turn off WMM if your wireless clients are not able to associate with an AP using WMM.
Max Clients	Specify the greatest number of wireless clients allowed to simultaneously connect to this wireless network on the ZyXEL Device.

Table 53 Wireless > Basic

LABEL	DESCRIPTION
BSSID	This shows the MAC address of the wireless interface on the ZyXEL Device when wireless LAN is enabled.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

18.5 Wireless Security

Click **Wireless > Security** to open the **Wireless Security** screen. Use this screen to configure wireless security settings.

Note: If you have a wireless connection to the ZyXEL Device and you change the ZyXEL Device's security settings, you will lose your connection when you click **Save/Apply**. You must then change your wireless client's settings to match the ZyXEL Device's new settings.

Figure 71 Wireless > Security

The following table describes the labels in this screen.

Table 54 Wireless > Security

LABEL	DESCRIPTION
WPS Setup	Use WiFi Protected Setup (WPS) to quickly set up a wireless network without having to manually configure settings. Set up each WPS connection between two devices at a time.
Enable WPS	Turn WPS on or off.

Table 54 Wireless > Security

LABEL	DESCRIPTION
Push Button	Select this to use the PBC (Push Button Configuration) method to send the ZyXEL Device's wireless settings to your wireless stations.
	Click **Add Enrollee** to start WPS-aware wireless station scanning and the wireless security information synchronization.
	Note: After you click **Add Enrollee**, you have 2 minutes to click a similar button in the wireless station's utility.
	To add a second wireless station, wait for the 2 minutes to pass and click the **Add Enrollee** button again. Then click the WPS button in the second wireless station's utility. Repeat for as many wireless clients as you need to add.
PIN	Select this to use the PIN configuration method to configure a wireless station's wireless settings. Enter the PIN of the device that you are setting up a WPS connection with and click **Add Enrollee** to authenticate and add the wireless device to your wireless network.
	You can find the PIN either on the outside of the device, or by checking the device's settings.
	Note: You must also activate WPS on the other device within two minutes to have it present its PIN to the ZyXEL Device.
WPS AP Mode	**Configured** uses the ZyXEL Device's current wireless security settings for WPS.
	Note: If the ZyXEL Device's wireless security is set to **Open**, selecting **Configured** and using WPS sets up a wireless network with no security.
	Unconfigured has the ZyXEL Device change its wireless security settings when you do one of the following:
	• Add a wireless enrollee. The ZyXEL Device automatically uses WPA2-PSK and a random key. The **WPS AP Mode** automatically changes to **Configured**.
	• Use **Setup AP** to have an external registrar (like Windows Vista) configure the ZyXEL Device's wireless security settings. The **WPS AP Mode** automatically changes to **Configured**.
	• Manually configure the ZyXEL Device's wireless security settings. Then you can manually set the **WPS AP Mode** to **Configured**.
Setup AP	This is available when you set the **WPS AP Mode** to **Unconfigured**.
	Click **Config AP** to have an external registrar configure the ZyXEL Device's wireless security settings. See Section 18.10.5 on page 170 for how to use Windows Vista as an external registrar. **Push Button** and **PIN** are reserved for future use and have no effect at the time of writing.
	Note: After you click **Config AP** you must enter the ZyXEL Device's PIN in the external registrar within two minutes.

149

Table 54 Wireless > Security

LABEL	DESCRIPTION
Device PIN	This shows the ZyXEL Device's PIN (Personal Identification Number). Enter this PIN in the external registrar within two minutes of clicking **Config AP**.
WSC Add External Registrar	This is available when you set the **WPS AP Mode** to **Configured**. Click **Start AddER** to have an external registrar to authenticate wireless clients using WPS. See Section 18.10.5 on page 170 for how to use Windows Vista as an external registrar. Note: After you click **Start AddER** you must enter the ZyXEL Device's PIN in the external registrar within two minutes. Then click **Finish AddER**.
Manual Setup AP	Use these fields to manually configure security settings for wireless clients that do not support WPS.The fields that display vary based on the type of network authentication you select.
Select SSID	Select the wireless network for which you want to configure security settings.
Network Authentication	Select the type of wireless network security to use for this network. **Open** - allows wireless devices to communicate with the access points without any authentication. **Shared** - encrypts the wireless communications using a shared (WEP) password. **802.1X** - encrypts the wireless communications using a shared (WEP) password and use an external RADIUS authentication server to authenticate each wireless client. With **WPA** or **WPA2** each user can have a separate user name and password. The ZyXEL Device uses an external RADIUS server to authenticate wireless client's user name and password. With **WPA-PSK** or **WPA2-PSK** the wireless clients share a common password instead of the ZyXEL Device using a RADIUS server. **Mixed WPA2/WPA** supports WPA and WPA2 on the network simultaneously. **Mixed WPA2/WPA-PSK** supports WPA and WPA2 on the network simultaneously.
WPA Pre-Shared Key	This field is available only with WPA-PSK or WPA2-PSK network authentication. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal digits. Click the link to see the key in plain text.
WPA2 Preauthentication	This field is available only with WPA2 network authentication. Turn on pre-authentication to enable fast roaming by allowing the wireless client (already connected to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Table 54 Wireless > Security

LABEL	DESCRIPTION
Network Re-auth Interval	This field is available only with WPA2 network authentication. Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 0 and 4294967295 seconds. 0 disables the re-authentication. Note: The re-authentication timer on the RADIUS server has priority over your setting here.
WPA Group Rekey Interval	This field is available only with WPA or WPA2 network authentication. The **Group Key Update Timer** is the rate at which the AP (if using **WPA(2)-PSK** key management) or **RADIUS** server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-PSK** mode. 0 disables the re-keying.
RADIUS Server IP Address	The RADIUS fields are required with 802.1X and WPA/WPA2 network authentication. Enter the IP address of the external authentication server in dotted decimal notation.
RADIUS Port	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.
RADIUS Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
WPA Encryption	Select the encryption type (TKIP, AES, or both) for data encryption. Select **TKIP** if your wireless clients can all use TKIP. Select **AES** if your wireless clients can all use AES. Select **TKIP + AES** to allow the wireless clients to use either TKIP or AES.
WEP Encryption	WEP encryption is optional with **Open** network authentication. It is required with **Shared** or **802.1X** network authentication. WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network.
Encryption Strength	If you are using WEP encryption, select **64-bit** or **128-bit** to set the length of the encryption key.

Table 54 Wireless > Security

LABEL	DESCRIPTION
Network Key 1 to Key 4	These fields are required when you use WEP encryption. If you set the **Encryption Strength** field to **64-bit**, enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you set the **Encryption Strength** field to **128-bit**, enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

18.6 The MAC Filter Screen

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

Use this screen to change your ZyXEL Device's MAC filter settings.Click **Wireless > MAC Filter**. The following screen displays.

Figure 72 Wireless > MAC Filter

The following table describes the labels in this screen.

Table 55 Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Select SSID	Select the wireless network for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the table below. Select **Disabled** to turn off MAC address filtering. Select **Allow** to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device. Select **Deny** to block access to the ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device
MAC Address	This column displays the MAC addresses of the wireless devices that are allowed or denied access to the ZyXEL Device.
Remove	Select the entry(ies) that you want to delete in the **Remove** column, then click the **Remove** button.
Add	Click this to open a screen where you can add a MAC address entry to the table.

18.6.1 The MAC Filter Add Screen

Use this screen to add MAC address entries. Click **Wireless > MAC Filter > Add** to open the following screen.

Figure 73 Wireless > MAC Filter > Add

The following table describes the labels in this screen.

Table 56 Wireless > MAC Filter > Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of the wireless device that is to be allowed or denied access to the ZyXEL Device. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

18.7 Wireless Bridge Screen

The ZyXEL Device can wirelessly connect APs. This is also known as a Wireless Distribution System (WDS). In the following figure a wireless client connects to access point **AP 1**. **AP 1** has no wired Internet connection, but it can establish a bridge link to access point **AP 2**, which has a wired Internet connection. This lets the notebook computer access the Internet through **AP 2**.

Figure 74   Wireless Bridge Example

Note: The peer wireless device must also support bridge mode and be using the same security settings as the ZyXEL Device.

Click **Wireless** > **Bridge** to open the following screen. Set your ZyXEL Device to **Access Point** mode for AP and bridge functionality or **Bridge** mode for bridge functionality only. You can also list the MAC addresses of the peer APs with which to establish wireless links.

Figure 75   Wireless > Bridge

The following table describes the labels in this screen.

Table 57 Wireless > Bridge

LABEL	DESCRIPTION
AP Mode	Select the operating mode for your ZyXEL Device. • **Access Point -** The ZyXEL Device functions as a bridge and access point simultaneously. • **Bridge** - The ZyXEL Device acts as a wireless network bridge and establishes wireless links with other APs. To disable wireless bridging, set the **Bridge Restrict** field to **Enabled** and do not list any remote bridge MAC addresses.
Bridge Restrict	Select how to restrict which devices can form wireless bridges with the ZyXEL Device. **Enabled** - Only allow bridges listed in the **Remote Bridges MAC Address** fields. You manually enter the MAC addresses in the **Remote Bridges MAC Address** fields. **Enabled (Scan)** - Only allow bridges listed in the **Remote Bridges MAC Address** fields. The ZyXEL Device scans and lists the SSIDs and MAC addresses of neighboring wireless devices. Select the ones that you want to be able to form wireless bridges with the ZyXEL Device. **Disabled** - Any wireless bridge is allowed to form wireless bridges with the ZyXEL Device.
Remote Bridges MAC Address	These are the MAC addresses of the peer wireless devices that can make wireless bridge connections with your ZyXEL Device. If you set the **Bridge Restrict** field to **Enabled**, manually enter the MAC addresses in the **Remote Bridges MAC Address** fields. If you set the **Bridge Restrict** field to **Enabled (Scan)**, the ZyXEL Device scans and lists the SSIDs and MAC addresses of neighboring wireless devices. Select the ones that you want to be able to form wireless bridges with the ZyXEL Device.
Refresh	Click **Refresh** to reload the previous configuration for this screen.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

18.8 The Advanced Setup Screen

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

Note: If have a wireless connection to the ZyXEL Device and you change the ZyXEL Device's wireless settings, you may lose your wireless connection when you click **Save/Apply**. You must then change your wireless client's settings to match the ZyXEL Device's new settings.

Figure 76 Wireless LAN > Advanced Setup

The following table describes the labels in this screen.

Table 58 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
Band	Select an operating band to use.
Channel	Select an operating channel to use. The choices depend on your particular region. Either select a channel or use **Auto** to have the ZyXEL Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible.

Table 58 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
Auto Channel Timer	If you set the channel to **Auto**, specify the interval in minutes for how often the ZyXEL Device scans for the best channel. Enter 0 to disable the periodical scan.
802.11n/EWC	Select whether to enable (**Auto**) or disable (**Disabled**) the use of the wireless 802.11n modes defined by the Enhanced Wireless Consortium (EWC). These modes can enhance speeds although the wireless clients must also support the EWC modes.
Bandwidth	**20MHz in Both Bands** uses a single radio channel in the 2.4 GHz band and a single radio channel in the 5.0 GHz band. Use this if the wireless clients do not support channel bonding. **40MHz in Both Bands** bonds two adjacent radio channels in the 2.4 GHz band and two adjacent radio channels in the 5.0 GHz band. Note: The 5.0 GHz band is reserved for future use and not supported at the time of writing. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. **20MHz in 2.4G Band and 40MHz in 5G Band** uses a single radio channel in the 2.4 GHz band and bonds two adjacent radio channel in the 5.0 GHz band. Use this if you have IEEE 802.11b and/or g clients that do not support 40 MHz and IEEE 802.11n clients that do.
Control Sideband	This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz in Both Bands**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
802.11n Protection	Enable this feature to help prevent collisions in mixed-mode networks (networks with both IEEE 802.11n and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11n performance. Select **Off** to disable IEEE 802.11n protection. The transmission rate of your ZyXEL Device might be reduced in a mixed-mode network.
Support 802.11n Client Only	Select this to only allow IEEE 802.11n wireless clients to connect to the ZyXEL Device. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the ZyXEL Device.
54g™ Rate	This field is available when **802.11n/EWC** is set to **Disabled**. Select a fixed wireless transmission rate or let the ZyXEL Device and the wireless client automatically select a rate.
Multicast Rate	Select a data rate at which the ZyXEL Device transmits wireless multicast traffic. If you select a high rate, multicast traffic may occupy all the bandwidth and cause network congestion.
Basic Rate	Select a minimum transmission rate.

Table 58 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
RTS Threshold	Use CTS/RTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions).
	A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS equal to or higher than the fragmentation threshold to turn RTS off.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with
	the network. This value can be set from 1 to 100.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again.
	The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 20ms to 1000ms. A high value helps save current consumption of the access point.
Global Max Clients	Specify the maximum number (from 1 to 64) of the wireless stations that may connect to the ZyXEL Device.
XPress™ Technology	Select this for higher speeds, especially if you have both IEEE 802.11b and IEEE 802.11g wireless clients. The wireless clients do not have to support XPress™ Technology, although the performance enhancement is greater if they do.
Afterburner Technology	Select this for higher speeds if the wireless clients also support afterburner technology.
Transmit Power	Set the output power of the ZyXEL Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs.
WMM (Wi-Fi Multimedia)	Use WMM (Wifi MultiMedia) to prioritize services in wireless traffic.
	Select **Auto** to automatically prioritize services according to the ToS value in the IP header of packets.
	Select **Enable** to prioritize services according to the ZyXEL Device's Quality of Service settings.
	Select **Disable** to not prioritize services in wireless traffic.
WMM No Acknowledgement	When using WMM, you can enable this to have the ZyXEL Device not re-send data if an error occurs. This can increase throughput speed but may also increase errors, especially in an environment with a lot of Radio Frequency (RF) noise. Otherwise leave it disabled.

Table 58 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
WMM APSD	When using WMM, enable APSD (Automatic Power Save Delivery) to have the ZyXEL Device manage radio usage to help increase battery life for battery-powered wireless clients. APSD uses a longer beacon interval when transmitting traffic that does not require a short packet exchange interval. For example, web browsing or using e-mail does not require a short packet exchange interval but Voice Over IP (VoIP) does. The wireless client must also support APSD for there to be any affect on the battery life.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

18.9 Wireless Station Info

The station monitor displays the connection status of the wireless clients connected to (or trying to connect to) the ZyXEL Device. To open the station monitor, click **Wireless** > **Station Info**. The screen appears as shown.

Figure 77 Wireless > Station Info
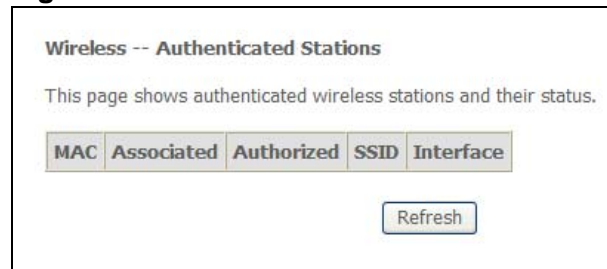
The following table describes the labels in this menu.

Table 59 Wireless > Station Info

LABEL	DESCRIPTION
MAC Address	This displays the MAC address (in XX:XX:XX:XX:XX:XX format) of a connected wireless station.
Associated	This is the time that the wireless client associated with the ZyXEL Device.
Authorized	This is the time that the wireless client's connection to the ZyXEL Device was authorized.
Strength	This displays the strength of the wireless client's radio signal. The signal strength mainly depends on the antenna output power and the wireless client's distance from the ZyXEL Device.
SSID	This is the name of the wireless network on the ZyXEL Device to which the wireless client is connected.
Interface	This is the name of the wireless LAN interface on the ZyXEL Device to which the wireless client is connected.
Refresh	Click this button to update the information in the screen.

18.10 Technical Reference

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

18.10.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 78   Example of a Wireless Network
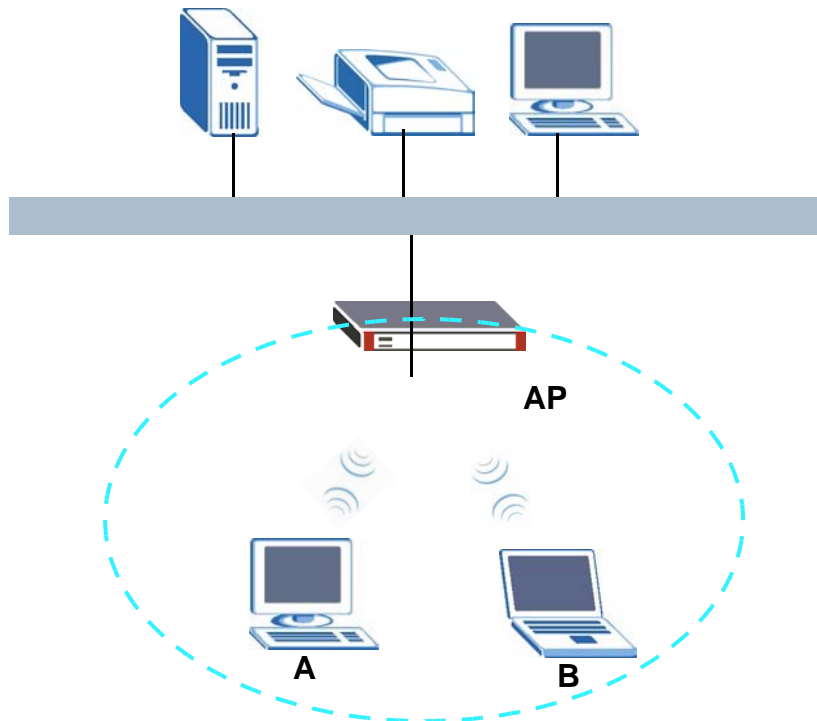
The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines.

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

  The SSID is the name of the wireless network. It stands for Service Set IDentity.

- If two wireless networks overlap, they should use a different channel.

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

- Every device in the same wireless network must use security compatible with the AP.

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

18.10.2 Additional Wireless Terms

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

Table 60   Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the ZyXEL Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the ZyXEL Device.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the ZyXEL Device does, it cannot communicate with the ZyXEL Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

18.10.3 Wireless Security Overview

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

18.10.3.1 SSID

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

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

18.10.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[2] A MAC address is usually written using twelve hexadecimal characters[3]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

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

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

18.10.3.3 User Authentication

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

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

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

---

2. 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.

3. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

18.10.3.4 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See Section 18.10.3.3 on page 162 for information about this.)

Table 61   Types of Encryption for Each Type of Authentication

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

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

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

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

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

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

18.10.4 WiFi Protected Setup

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

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

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

18.10.4.1 Push Button Configuration

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

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

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

1 Ensure that the two devices you want to set up are within wireless range of one another.

2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button.

3 Press the button on one of the devices (it doesn't matter which). For the ZyXEL Device you must press the WPS button for more than three seconds.

4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

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

18.10.4.2 PIN Configuration

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

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

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

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

1 Ensure WPS is enabled on both devices.

2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.

3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface.

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

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

5 Start WPS on both devices within two minutes.

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

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

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

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

Figure 79 Example WPS Process: PIN Method
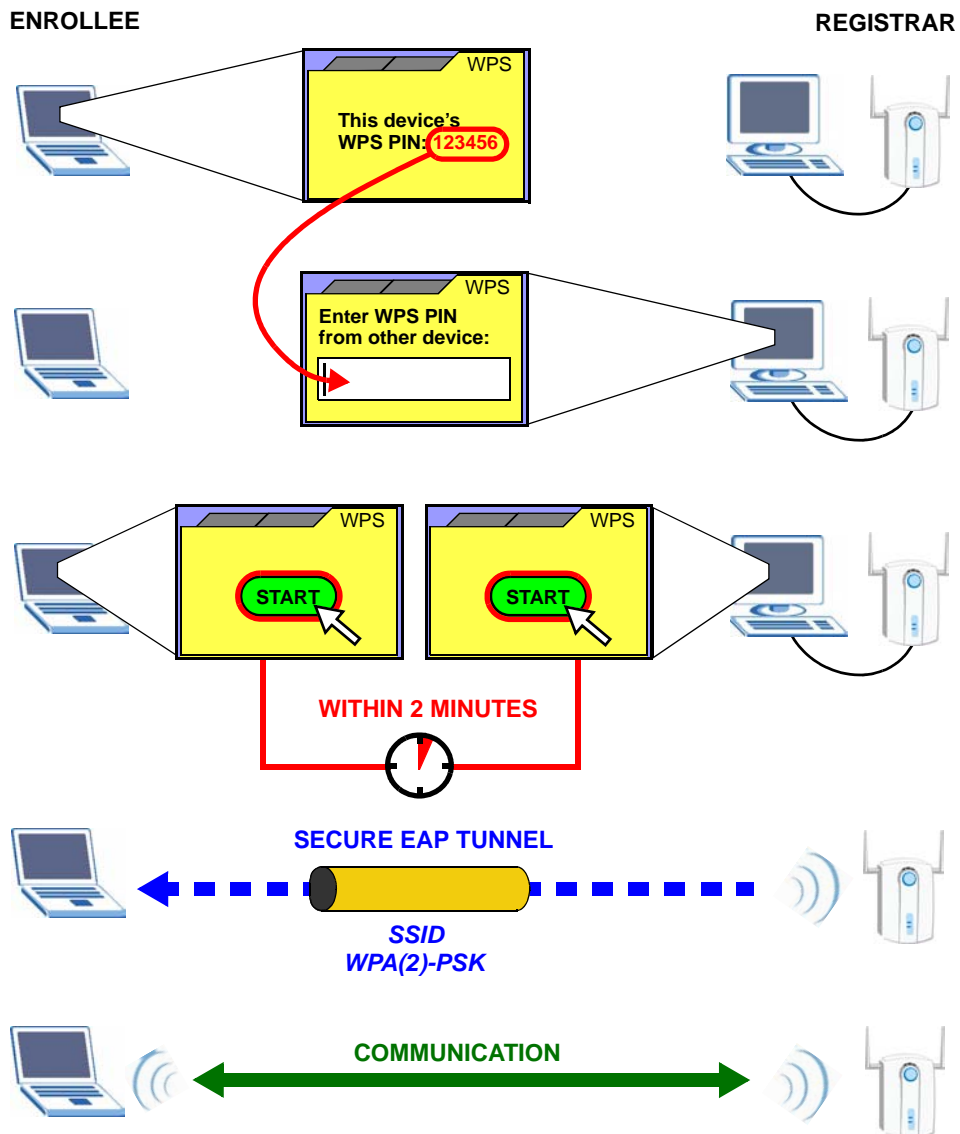
18.10.4.3 How WPS Works

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

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

Figure 80   How WPS works
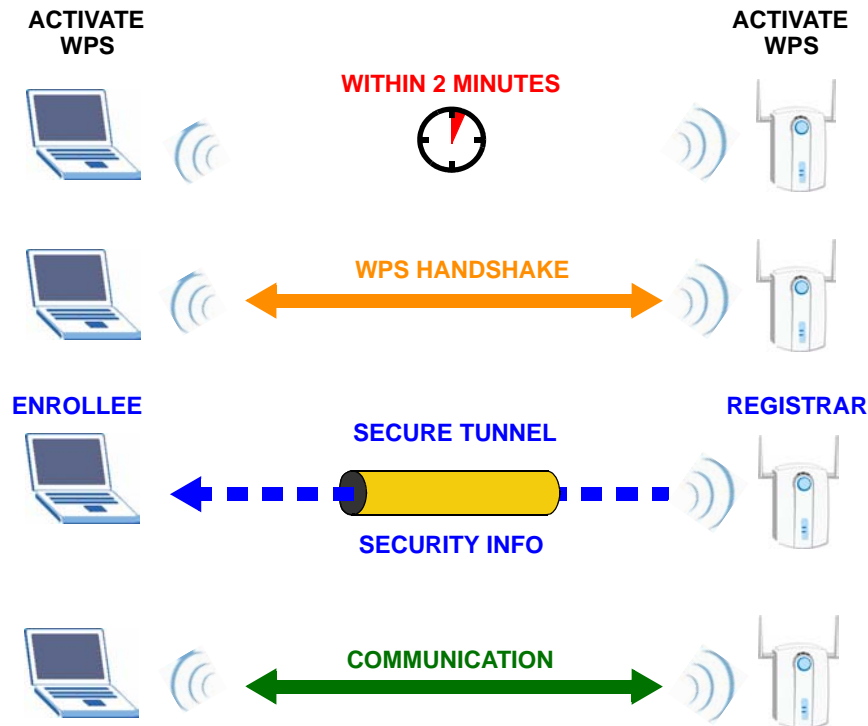
The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

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

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

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

18.10.4.4 Example WPS Network Setup

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

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

Figure 81   WPS: Example Network Step 1
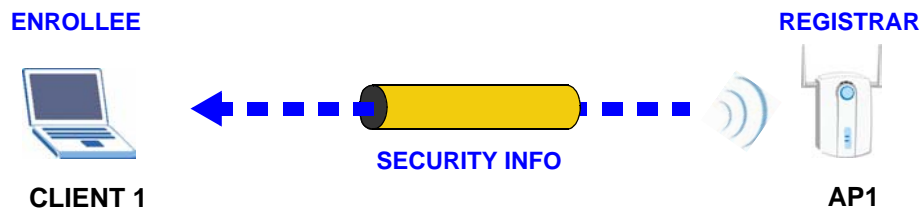
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.
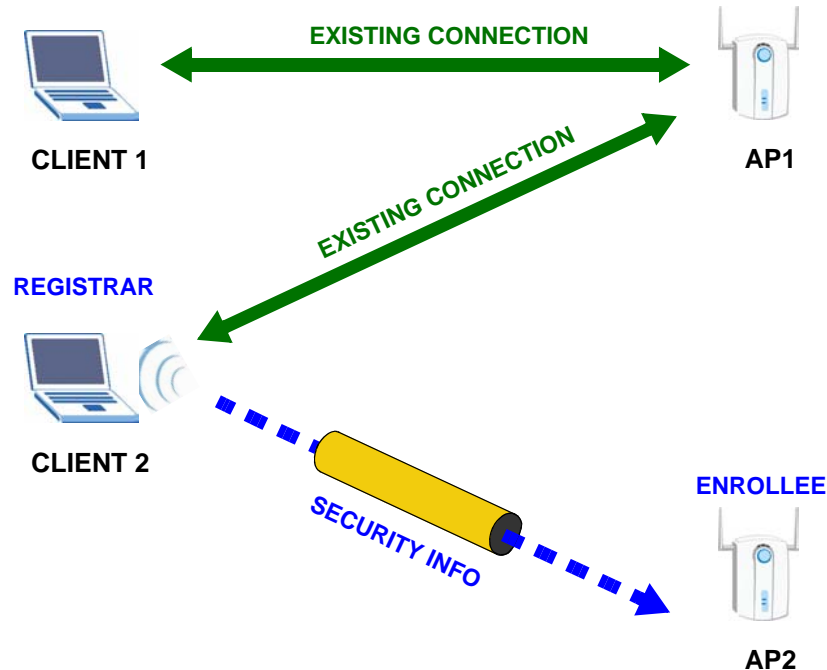
Figure 82   WPS: Example Network Step 2
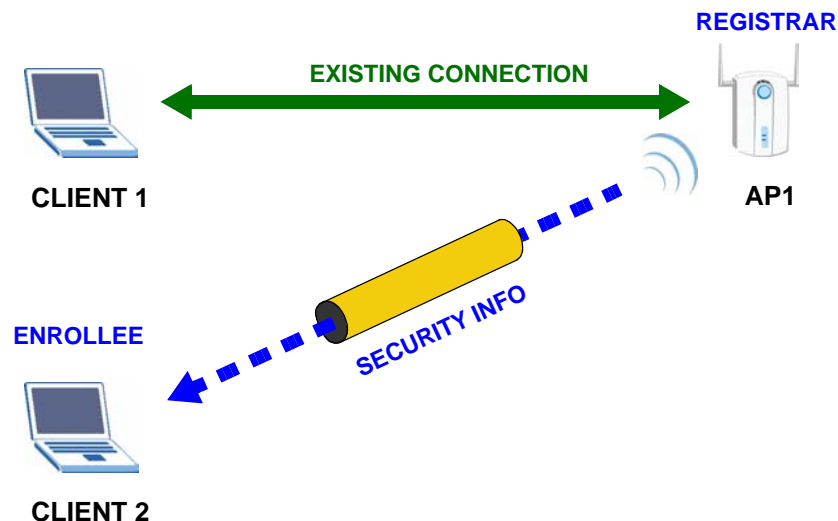
In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access

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

Figure 83 WPS: Example Network Step 3

18.10.4.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).

- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

18.10.5 WPS External Registrar

You can have an external WPS registrar (for example a computer running Windows Vista) give wireless settings to the ZyXEL Device or wireless clients.

Use an Ethernet cable to connect the Windows Vista computer directly to one of the ZyXEL Device's Ethernet ports. In Windows Vista, double-click the ZyXEL AP network connection icon and enter the PIN from the ZyXEL Device or a wireless client in the Windows Connect Now (WCN) screens.

PART III
Diagnostics and Management

Diagnostics

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

19.1 Diagnostics

Click **Diagnostics** to open the screen shown next. Use this screen to test the ZyXEL Devices connections. The ENET connections appear as four separate connections when you enable virtual ports (see), otherwise they appear as a single connection. If you are using single line mode, **DSL2** must be connected and working to pass the ADSL synchronization test. If you are not using single line mode, the ADSL synchronization test can be passed if either DSL line is connected and working.

Figure 84   Diagnostics

Settings

This chapter describes how to manage your ZyXEL Device's configuration.

20.1 Backup Configuration Using the Web Configurator

Click **Management > Settings > Backup** to open the following screen. Use this screen to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Figure 85   Management > Settings > Backup

Settings - Backup

Backup DSL router configurations. You may save your router configurations to a file on your PC.
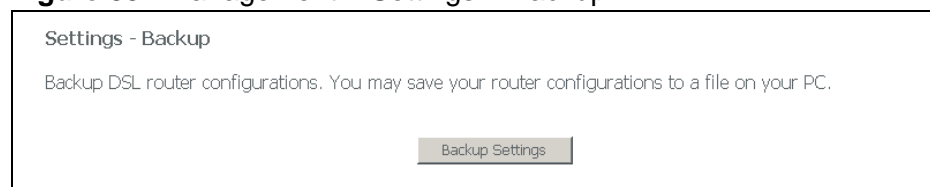
Backup Settings

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

20.2 Restore Configuration Using the Web Configurator

Click **Management > Settings > Update** to open the following screen. Use this screen to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

Figure 86   Management > Settings > Update

Tools -- Update Settings

Update DSL router settings. You may update your router settings using your saved files.

Settings File Name: [   ] [Browse...]

[Update Settings]

Table 62

Settings File Name	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.
Update Settings	Click this to begin the upload process.

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

You must then wait before logging into the ZyXEL Device again. The ZyXEL Device automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 87   Temporarily Disconnected

Local Area Connection
Network cable unplugged

10:44

You may need to change the IP address of your computer to be in the same subnet as that of the ZyXEL Device's IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

20.3 Restoring Factory Defaults

Click **Management > Settings > Restore Default** to open the following screen.

Figure 88   Management > Settings > Restore Default

Tools -- Restore Default Settings

Restore DSL router settings to the factory defaults.

Restore Default Settings

Click **Restore Default Settings** to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device.

You may need to change the IP address of your computer to be in the same subnet as that of the default ZyXEL Device IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

Logs

This chapter contains information about configuring general log settings and viewing the ZyXEL Device's logs. Refer to the appendix for example log message explanations.

21.1 Logs Overview

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

21.2 System Log

Click **Management > System Log** to open the following screen. Click **View System Log** screen to see the logs, or **Configure System Log** to configure the logging settings.

Figure 89   Management > System Log
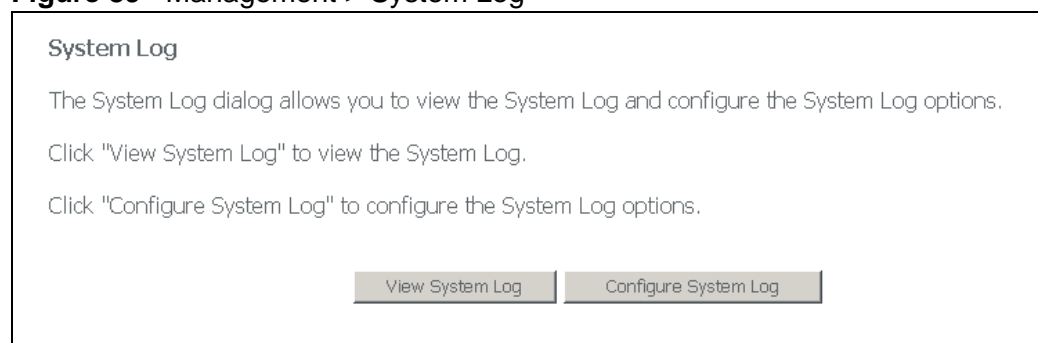
21.3 Viewing the System Log

Click **Management > System Log** > **View System Log** to view the ZyXEL
Device's system logs.

Figure 90   Management > System Log > View System Log

Date/Time	Facility	Severity	Message
Jan 1 00:00:21	syslog	emerg	P-663HN-51 started: BusyBox v1.00 (2009.07.15-06:05+0000)
Jan 1 00:00:21	user	crit	kernel: eth0 Link UP.
Jan 1 00:01:52	user	crit	kernel: eth1 Link UP.
Jan 1 00:02:33	user	crit	kernel: Virtual device wl0 asks to queue packet!

The following table describes the fields in this screen.

Table 63   Management > System Log > View System Log

LABEL	DESCRIPTION
Date/Time	This field displays when the log was recorded.
Facility	This is the log's category.
Severity	This is the event's degree of seriousness.
Message	This field states the reason for the log.
Refresh	Click **Refresh** to renew the log screen.
Close	Click this to close the window.

21.4 Configuring Log Settings

Click **Management > System Log** > **Configure System Log** to display the following screen. Use this screen to configure the level of events to log and where to send logs.

Figure 91   Management > System Log > Configure System Log

The following table describes the fields in this screen.

Table 64   Management > System Log > Configure System Log

LABEL	DESCRIPTION
Log	This controls whether or not the ZyXEL Device logs events.
Log Level	Select the lowest level of events that you want the ZyXEL Device to log. The ZyXEL Device logs all events with that severity level or higher.
Display Level	Select the lowest level of events that you want the ZyXEL Device to display. The ZyXEL Device displays events with that severity level or higher.
Mode	Select **Local** to only record events in the ZyXEL Device's memory. Select **Remote** to send events to a remote syslog server. Select **Both** to record events in the ZyXEL Device's memory and send them to a remote syslog server.
Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Server UDP Port	Enter the UDP port number the ZyXEL Device is to use when sending syslog events to the syslog server.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

22.1 SNMP Overview

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of TCP/IP protocol suite. A manager station can monitor the ZyXEL Device through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 92   SNMP Management Model
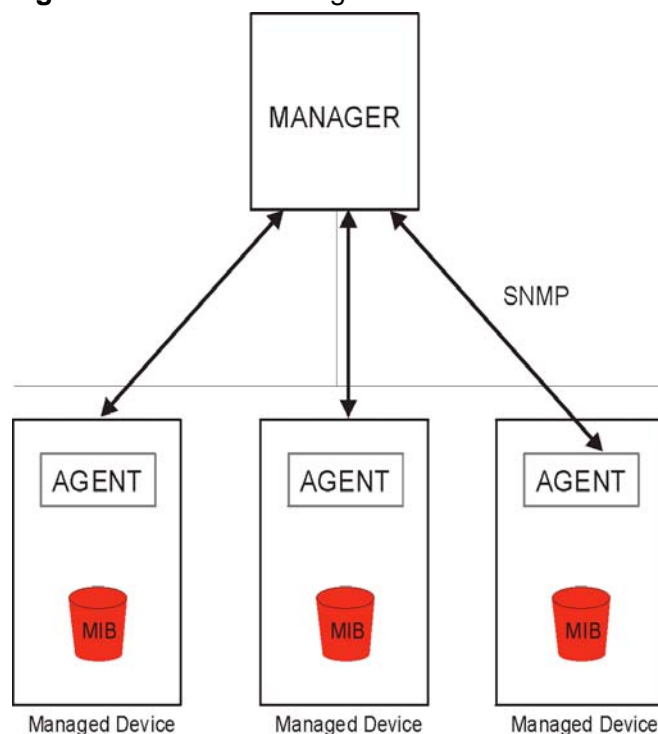
An SNMP managed network consists of two main components: agents and a manager.

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

through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

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

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

Table 65   SNMP Commands

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

22.1.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance. The ZyXEL Device supports the following MIBs:

• ADSL mib

• AT mib

• ATM mib

• ICMP mib

• IP mib

• SNMP mib

• SYSOR mib

• TCP mib

• UDP mib

The ZyXEL Device uses these MIBs to provide read-only information. You cannot use SNMP to configure the ZyXEL Device.

22.2 SNMP Screen

To open this screen, click **Advanced Application**, **Access Control**, **SNMP**.

Figure 93   SNMP

The following table describes the labels in this screen.

Table 66   SNMP

LABEL	DESCRIPTION
SNMP Agent	Enable the SNMP agent to turn on SNMP on the ZyXEL Device.
Read Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
System Name	Specify the name the ZyXEL Device uses for SNMP.
System Location	Specify where the ZyXEL Device is.
System Contact	Specify the name of the person administering the ZyXEL Device.
Trap Manager IP	Enter the IP address of a station to send your SNMP traps to. The ZyXEL Device sends a coldStart trap when the power is turned on.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.
Port	Enter the port number upon which the station listens for SNMP traps.

TR-069 Client

23.1 TR-069 Client Screen

TR-069 is a protocol that defines how your ZyXEL Device can be managed via a management server such as ZyXEL's Vantage CNM Access.

An administrator can use an Auto Configuration Server (ACS) to remotely set up the ZyXEL device, modify settings, perform firmware upgrades as well as monitor and diagnose the ZyXEL device. All you have to do is enable the device to be managed by an ACS and specify the ACS IP address or domain name and username and password.

Use this screen to configure your ZyXEL Device's settings for CPE WAN Management Protocol (CWMP).

Click **Management > TR-069 Client**. The following screen appears.

Figure 94   Management > TR-069 Client

The following table describes the fields in this screen.

Table 67 Management > TR-069 Client

LABEL	DESCRIPTION
Inform	Select whether to **Enable** or **Disable** CPE WAN Management Protocol (CWMP) operation.
Inform Interval	The interval between the device's attempt to connect to the Auto Configuration Server (ACS) to send information and check for configuration updates.
ACS URL	Enter the address of the ACS.
ACS User Name	Enter the username for the ACS.
ACS Password	Enter the password for the ACS.
Display SOAP messages on serial console	Select whether to **Enable** or **Disable** text-based messages from the ACS to be displayed by the ZyXEL Device. These messages are used for debugging.
Connection Request Authentication	Select this if you want the ZyXEL Device to periodically send messages to the ACS to keep the connection alive. This is needed in case the ACS changes gateway configuration.
Connection Request User Name	Enter the username for the ACS for reauthentication in case the connection is interrupted.
Connection Request Password	Enter the password for the ACS for reauthentication in case the connection is interrupted.
Save/Apply	Click this to save the changes.
GetRPCMethod	Click this to get a list of commands accepted by the ACS.

Time

This chapter covers how to set the time in the ZyXEL Device.

24.1 Time Setup

Click **Management** > **Internet Time** to open the following screen. Use this screen to configure how the ZyXEL Device synchronizes its internal clock with a time server on the Internet.

Figure 95   Management > Internet Time

Time settings

This page allows you to the modem's time configuration.

☑ Automatically synchronize with Internet time servers

| First NTP time server: | clock.fmt.he.net | |
| Second NTP time server: | None | |

Time zone offset: (GMT-12:00) International Date Line West

Save/Apply

The following table describes the labels in this screen.

Table 68   Management > Internet Time

LABEL	DESCRIPTION
Automatically synchronize with Internet time servers	Select this radio button to have the ZyXEL Device get the time and date from the NTP time server you specify. See RFC 1305 for details on NTP.
First NTP time server	Enter the IP address or URL of the time server that the ZyXEL Device should use to update time and date settings.
Second NTP time server	Enter the IP address or URL of the time server that the ZyXEL Device should use to update time and date settings if it cannot get a response from the first time server.

Table 68 Management > Internet Time (continued)

LABEL	DESCRIPTION
Time Zone	Choose the time zone of your location. This sets the time difference between your time zone and Greenwich Mean Time (GMT).
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

Access Control

This chapter describes how to configure access control.

25.1 Access Control Screen

Use the access control screens to enable or disable service access to the ZyXEL Device.

25.2 Service Access Control Screen

To open this screen, click **Management > Access Control** > **Services**.

Figure 96   Management > Access Control > Services

The following table describes the labels in this screen.

Table 69 Management > Access Control > Services

LABEL	DESCRIPTION
Services	Services you may use to access the ZyXEL Device are listed here.
LAN	Select the **Enable** check boxes for the corresponding services that you want to allow to access the ZyXEL Device from the LAN.
WAN	Select the **Enable** check boxes for the corresponding services that you want to allow to access the ZyXEL Device from the WAN.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

25.3 IP Addresses

This screen lists the IP addresses of trusted computers that may manage the ZyXEL Device. To open this screen, click **Management > Access Control** > **IP Addresses**.

Figure 97   Management > Access Control > IP Addresses

The following table describes the labels in this screen.

Table 70   Management > Access Control > IP Addresses

LABEL	DESCRIPTION
Access Control Mode	Enable this to have the ZyXEL Device check the source IP address of incoming local management sessions.
IP Address	This is the IP address of a trusted computer from which you can manage the ZyXEL Device.

Table 70 Management > Access Control > IP Addresses (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new trusted IP address.

25.4 Adding IP Addresses

Use this screen to add IP addresses of trusted computers that may manage the ZyXEL Device. To open this screen, click **Management > Access Control** > **IP Addresses > Add**.

Figure 98 Management > Access Control > IP Addresses > Add

The following table describes the labels in this screen.

Table 71 Management > Access Control > IP Addresses > Add

LABEL	DESCRIPTION
IP Address	Specify the IP address of a trusted computer from which you want to manage the ZyXEL Device.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

25.5 Passwords

Click **Management > Access Control** > **Passwords** to open the following screen. Use this screen to configure the ZyXEL Device's passwords.

Note: The "support" user name and password for ISP technician login only works through the DSL connection.

Figure 99 Management > Access Control > Passwords

The following table describes the labels in this screen.

Table 72 Management > Access Control > Passwords

LABEL	DESCRIPTION
Username	Select the user name for which you want to configure the password.
	The **admin** or **user** account can only access the ZyXEL Device from the LAN.
	The **support** account can only access the ZyXEL Device from the WAN.
	Only the **admin** or **support** account can use Telnet to log into the ZyXEL Device.
Old Password	Type the existing password.
New Password	Type the new password. Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Confirm Password	Type the new password again to make sure it is entered properly.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

25.6 Authentication

Click **Management > Access Control** > **Authentication** to open the following screen. Use this screen to set whether or not users must enter a user name and password to access the ZyXEL Device's system information summary page.

Figure 100   Management > Access Control > Authentication

The following table describes the labels in this screen.

Table 73   Management > Access Control > Authentication

LABEL	DESCRIPTION
Login authentication on web home page	Select this to require users to enter the ZyXEL Device's user account's user name and password in order to access the ZyXEL Device's system information summary page. Clear this to allow users to access the ZyXEL Device's system information summary page without entering the ZyXEL Device's user account's user name and password.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

Update Software

This chapter covers upgrading the ZyXEL Device's firmware.

26.1 Uploading Firmware

The software embedded in the ZyXEL Device is called "firmware". Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "ZyXEL Device.bin". The upload process described here may take up to two minutes. After a successful upload, the system will reboot.

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

Click **Management > Update Software** to open the following screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

Figure 101   Management > Update Software

Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name: [   ] [Browse...]

[Update Software]

The following table describes the labels in this screen.

Table 74 Management > Update Software

LABEL	DESCRIPTION
Software File name	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.
Update Software	Click **Upload** to begin the upload process. This process may take up to two minutes.

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

After you upload firmware, wait before logging into the ZyXEL Device again. The ZyXEL Device automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 102 Network Temporarily Disconnected

After the ZyXEL Device finishes restarting, log in again and check your new firmware version in the **Status** screen.
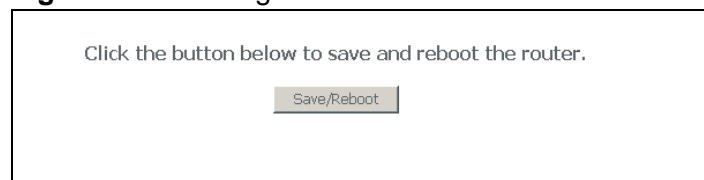
Save/Reboot and Logout

This chapter covers the save and reboot screen.

27.1 Save/Reboot

Click **Management > Save/Reboot** to open the following screen. Click **Save/Reboot** to save all of your ZyXEL Device's settings and reboot the without turning the power off.

Figure 103   Management > Save/Reboot

27.2 Logout

Click **Management > Logout** to exit the web configurator.

PART IV
Troubleshooting and Specifications

201

28

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*
- *ZyXEL Device Access and Login*
- *Internet Access*

28.1 Power, Hardware Connections, and LEDs

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

1   Make sure the ZyXEL Device is turned on.

2   Make sure you are using the power adaptor or cord included with the ZyXEL Device.

3   Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.

4   Turn the ZyXEL Device off and on.

5   If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1   Make sure you understand the normal behavior of the LED. See Section 1.5 on page 25.

2 Check the hardware connections. See Section 1.4 on page 23.

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

4 Turn the ZyXEL Device off and on.

5 If the problem continues, contact the vendor.

28.2 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

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 ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 29.

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 2.3 on page 29.

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 6.2.1 on page 76), use the new IP address.

- • If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.4 on page 23 and Section 1.5 on page 25.

3 Make sure your Internet browser does not block pop-up windows. See Appendix C on page 201.

4 Make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)

- • If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 6.2.1 on page 76. Your ZyXEL Device is a DHCP server by default.

- • If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device. See Section 6.2.1 on page 76.

5 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 2.3 on page 29.

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

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

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

2 Turn the ZyXEL Device off and on.

3 If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 29.

28.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.4 on page 23 and Section 1.5 on page 25.

2 If your ISP gave you Internet connection information, make sure you entered it correctly in the **Network** > **WAN** > **Internet Connection** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 Disconnect all the cables from your device, and follow the directions in Section 1.4 on page 23 again.

4 If the problem continues, contact your ISP.

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

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.4 on page 23 and Section 1.5 on page 25.

2 Reboot the ZyXEL Device.

3 Turn the ZyXEL Device off and on.

4 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 25. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Reboot the ZyXEL Device.

3 Turn the ZyXEL Device off and on.

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

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

Table 75 Device Specifications

Dimensions (W x D x H)	255 x 165 x 63 mm
Power Specification	12 VDC 1.5 A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X (auto-crossover) 10/100 Mbps RJ-45 Ethernet ports
Reset Button	The reset button is built into the rear panel. Use this button to restore the ZyXEL Device to its factory default settings. Press for 10 seconds to restore to factory default settings.
WPS/WLAN button	Press this button for five seconds and release it. Then press the WPS button on another wireless device within 2 minutes to set up a security-enabled wireless connection. Press this button for 1 to 4 seconds and release it to turn the wireless LAN on or off.
Antenna	ZyXEL DeviceThe ZyXEL Device is equipped with one external 2dBi (2.4GHz) antenna and on internal 2dBi (2.4GHz) antenna to provide clear radio transmission and reception on the wireless network.
Operating Temperature	0° C ~ 40° C
Storage Temperature	-30° ~ 60° C
Operating Humidity	20%~85% (non-condensing)
Storage Humidity	10%~95% (non-condensing)

Table 76 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Admin User Name	admin
User User Name	user
Support User Name	support
Default Password	1234

Table 76 Firmware Specifications

FEATURE	DESCRIPTION
ADSL Standards	Multi-Mode standard (ANSI T1.413,Issue 2; G.dmt(G.992.1); G.lite(G992.2)).
	ADSL2 G.dmt.bis (G.992.3)
	ADSL2 G.lite.bis (G.992.4)
	ADSL2+ (G.992.5)
	Reach-Extended ADSL (RE ADSL)
	SRA (Seamless Rate Adaptation)
	Auto-negotiating rate adaptation
	ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5)
	Multi-protocol over AAL5 (RFC2684/1483)
	PPP over ATM AAL5 (RFC 2364)
	PPP over Ethernet (RFC 2516)
	MAC encapsulated routing (ENET encapsulation)
	VC-based and LLC-based multiplexing
	Up to 8 PVCs (Permanent Virtual Circuits)
	OAM F4/F5 end-to-end loopback, AIS, and RDI OAM cells
	ATM-based Multi-Pair Bonding (G.998.1) support
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol.
	Transparent bridging for unsupported network layer protocols.
	DHCP Server/Client/Relay
	RIP I / RIP II
	ICMP
	ATM QoS
	SNMP v1 and v2c with MIB II support (RFC 1213)
	IP Multicasting IGMP v1 and v2
	IGMP Proxy
	UPnP
Management	Use the embedded web configurator to easily configure the rich range of features on the ZyXEL Device.
	SNMP manageable
	Syslog
	Built-in diagnostic tools for ADSL circuitry and LAN ports

Table 76 Firmware Specifications

FEATURE	DESCRIPTION
Wireless Functionality	Allows IEEE 802.11n, IEEE 802.11g and/or IEEE 802.11b wireless clients to connect to the ZyXEL Device wirelessly. Enable wireless security (WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The ZyXEL Device 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. The ZyXEL Device can use wireless bridging to establish up to four wireless links with other APs.
Firewall	Block traffic originating from the Internet from accessing the LAN. Protects against DoS and DDoS attacks, including SYNC flooding, IP Smurf, Ping of Death, Fraggle, Teardrop, and Land attacks.
NAT	Virtual Server (Port Forwarding) Port Triggering DMZ Host IP
Other Features	Dynamic DNS Static Routes
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide 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 your public IP address(es) to multiple private IP addresses for the computers on your network.
Virtual Server	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device 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.

Table 76 Firmware Specifications

FEATURE	DESCRIPTION
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. These dates and times are then used in logs.
Syslog	The ZyXEL Device can send syslogs to an external syslog server.
PPPoE	PPPoE mimics a dial-up Internet access connection.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
Firewall	You can configure firewall on the ZyXEL Device 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.
Access Control	This allows you to decide whether a service (HTTP traffic for example) from a computer on the LAN can access the ZyXEL Device.

Table 77 Standards Supported

| STANDARD	DESCRIPTION
RFC 1483/2684 (MPOA)	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2364 (PPPoA)	PPP over AAL5
RFC 2516 (PPPoE)	PPP over Ethernet
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard
ITU G.992.1 (G.dmt)	ITU standard for ADSL using discrete multitone modulation
ITU G.992.2 (G. lite)	ITU standard for ADSL using discrete multitone modulation
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.3 (G.lite.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits.
ITU G.998.1 (G.bond ATM)	ATM-based Multi-Pair Bonding
RFC 1112 (IGMP v1)	Internet Group Management Protocol, Version 1
RFC 2236 (IGMP v2)	Internet Group Management Protocol, Version 2
RFC 867	Daytime Protocol

Table 77 Standards Supported

STANDARD	DESCRIPTION
RFC 868	Time Protocol
RFC 1305	Network Time Protocol (Version 3) Specification, Implementation
RFC 1334 (PAP)	PPP Authentication Protocols
RFC 1994 (CHAP)	PPP Challenge Handshake Authentication Protocol
RFC 1332 (IPCP)	The PPP Internet Protocol Control Protocol
RFC 1058 (RIP-1)	Routing Information Protocol
RFC 1723 (RIP-2)	RIP Version 2 - Carrying Additional Information
RFC 1631 (NAT)	IP Network Address Translator
RFC 1661 (PPP)	The Point-to-Point Protocol
RFC 1157 (SNMPv1)	Simple Network Management Protocol, Version 1
RFC 1441 (SNMPv2)	Simple Network Management Protocol, Version 2
RFC 2408 (ISAKMP)	Internet Security Association and Key Management Protocol

29.1 DSL Connector Pin Assignments

The ZyXEL Device's RJ-11 DSL connector handles both the DSL 1 and DSL 2 connections.

• Pins 3 and 4 are for DSL 1.

• Pins 2 and 5 are for DSL 2.

Figure 104   DSL Connector Pin Assignments
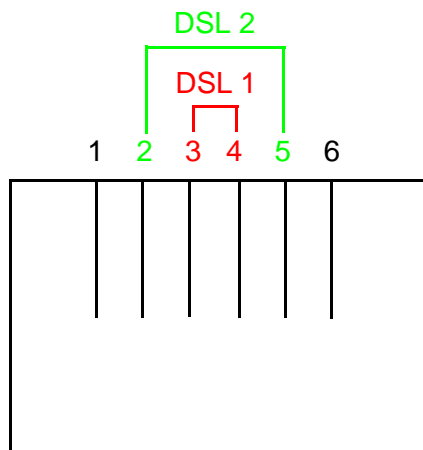
29.2 Power Adaptor Specifications

Table 78   North American Plug Standards

AC POWER ADAPTOR MODEL	12V 1.5 A Switching Power Adapter
INPUT POWER	100-240 VAC, 50/60 HZ, 0.5 A
OUTPUT POWER	12 VDC, 1.5 A
POWER CONSUMPTION	18 W MAX.
SAFETY STANDARDS	UL, CUL (UL 60950-1 FIRST EDITION CSA C22.2 NO. 60950-1-03 1ST.)

PART V
Appendices and Index

A

Setting Up Your Computer's IP Address

Note: Your specific ZyXEL device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

- *Windows XP/NT/2000* on page 215
- *Windows Vista* on page 219
- *Mac OS X: 10.3 and 10.4* on page 223
- *Mac OS X: 10.5* on page 227
- *Linux: Ubuntu 8 (GNOME)* on page 230
- *Linux: openSUSE 10.3 (KDE)* on page 235

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

Figure 105 Windows XP: Start Menu
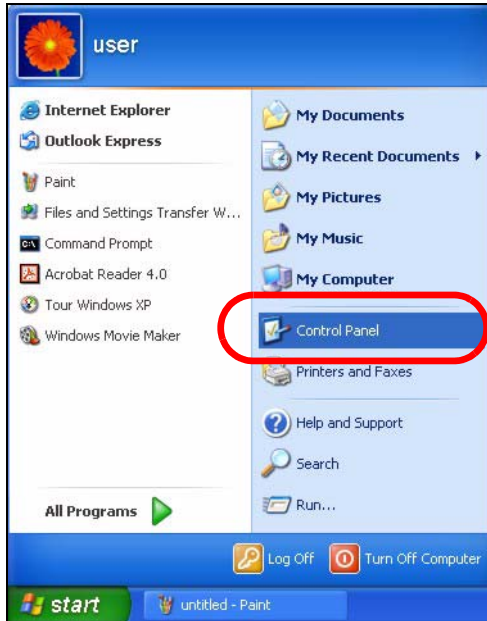
2 In the **Control Panel**, click the **Network Connections** icon.

Figure 106 Windows XP: Control Panel

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

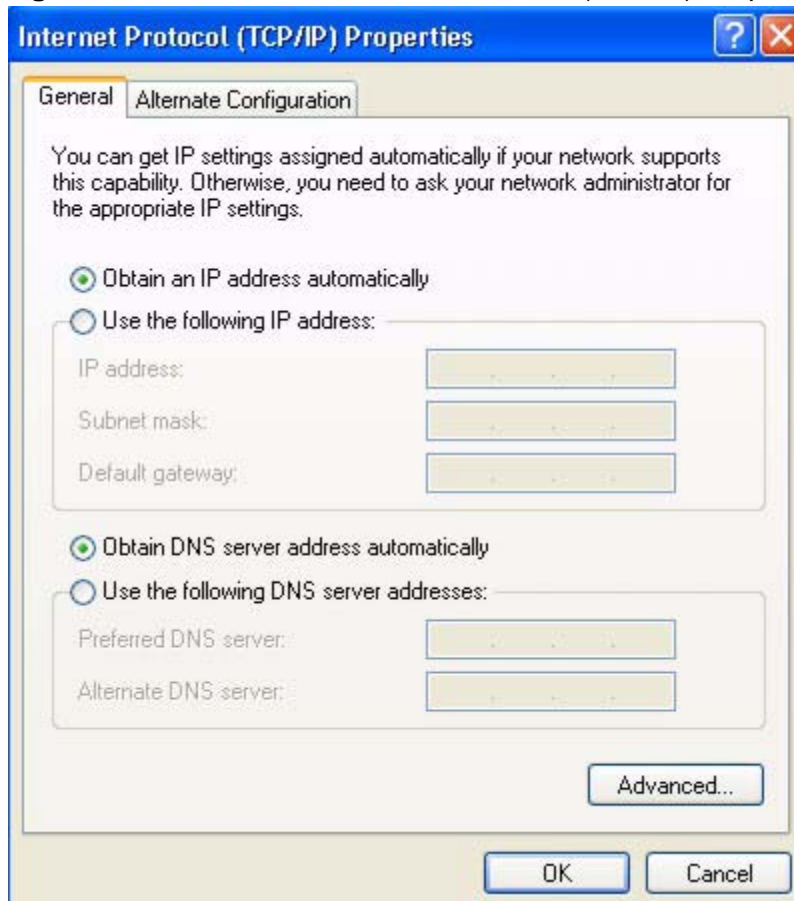**Figure 107** Windows XP: Control Panel > Network Connections > Properties
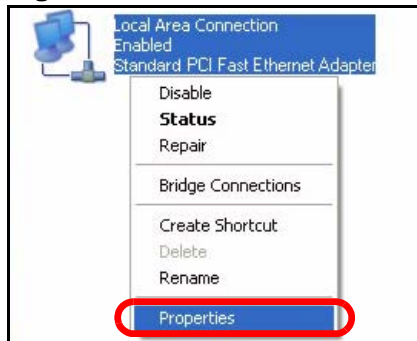
4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 108 Windows XP: Local Area Connection Properties
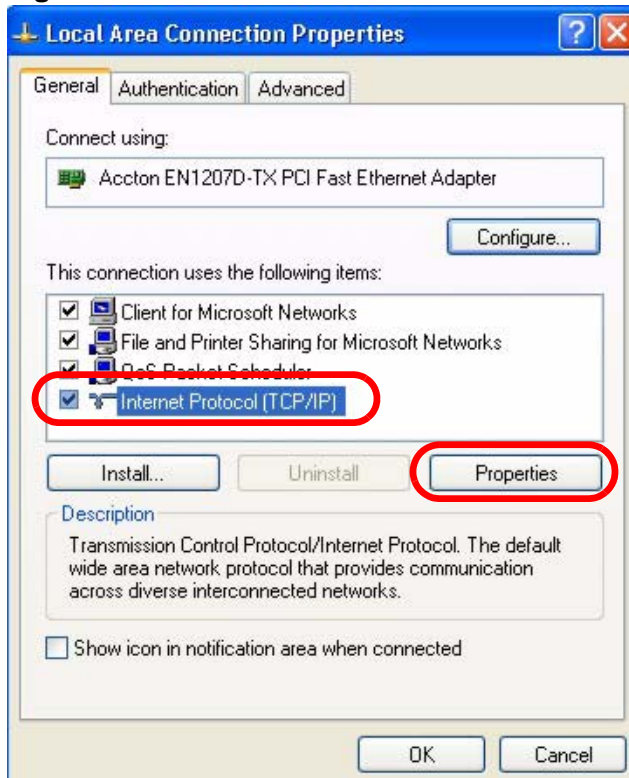
5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 109 Windows XP: Internet Protocol (TCP/IP) Properties

6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

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

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

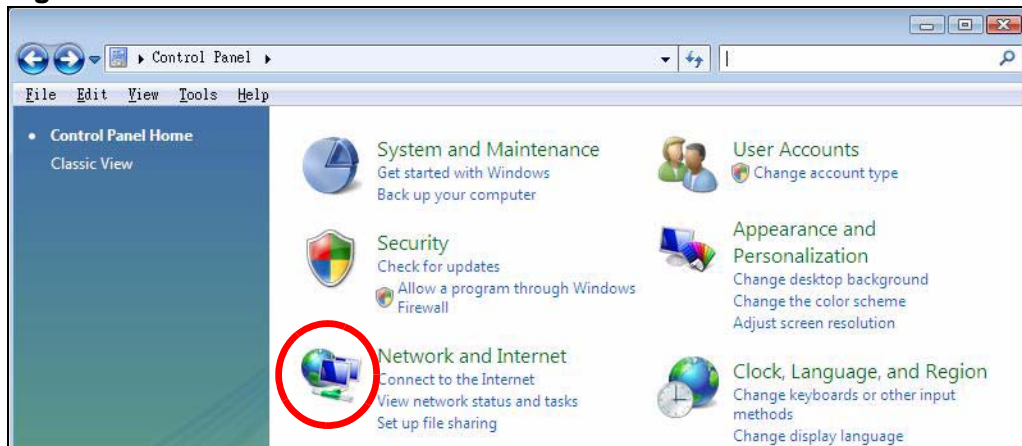This section shows screens from Windows Vista Professional.

1 Click **Start** > **Control Panel**.

Figure 110 Windows Vista: Start Menu
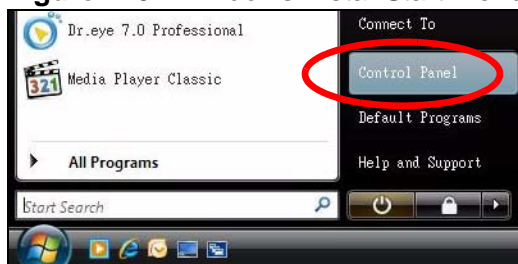
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 111 Windows Vista: Control Panel

3 Click the **Network and Sharing Center** icon.

Figure 112 Windows Vista: Network And Internet

4 Click **Manage network connections**.

Figure 113 Windows Vista: Network and Sharing Center
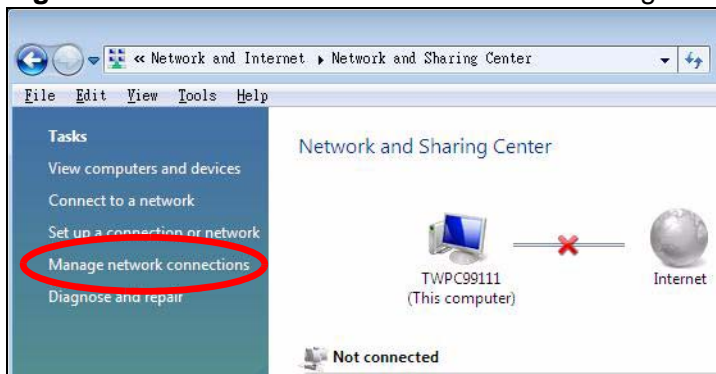
**5** Right-click **Local Area Connection** and then select **Properties**.

Figure 114 Windows Vista: Network and Sharing Center
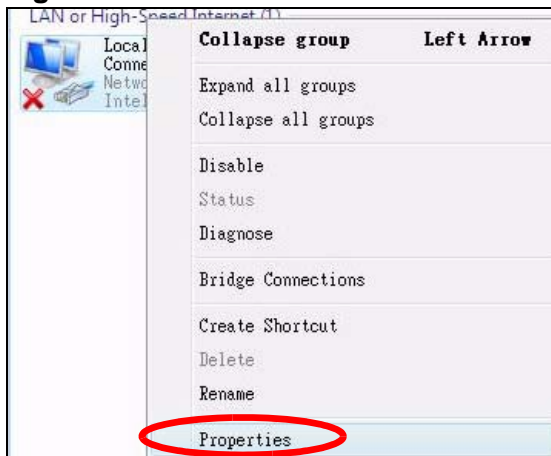
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 115 Windows Vista: Local Area Connection Properties
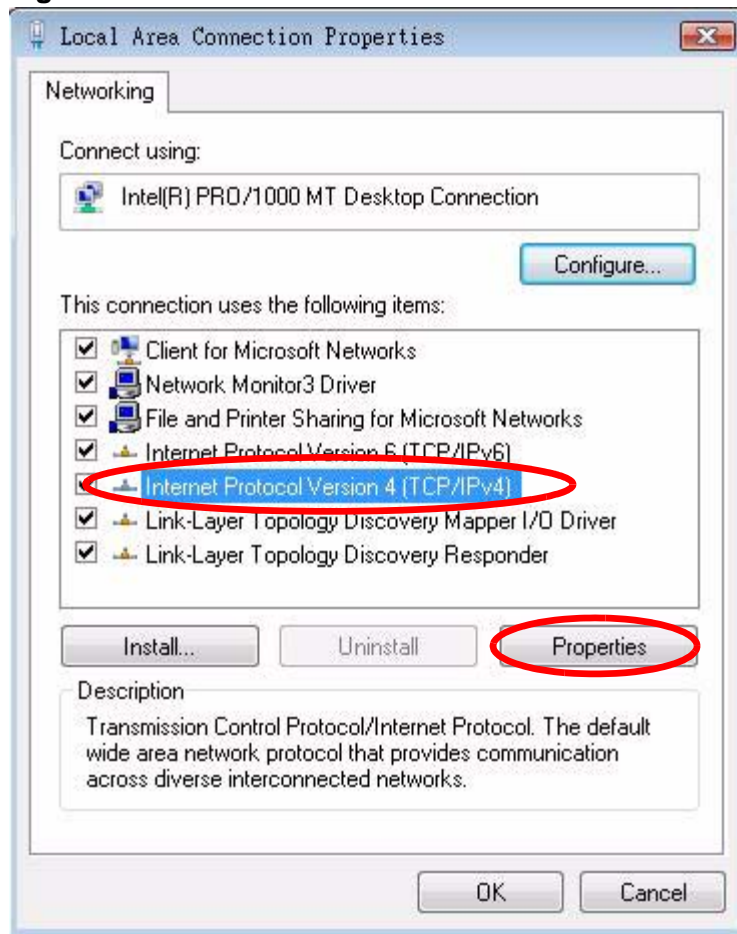
7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 116 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties
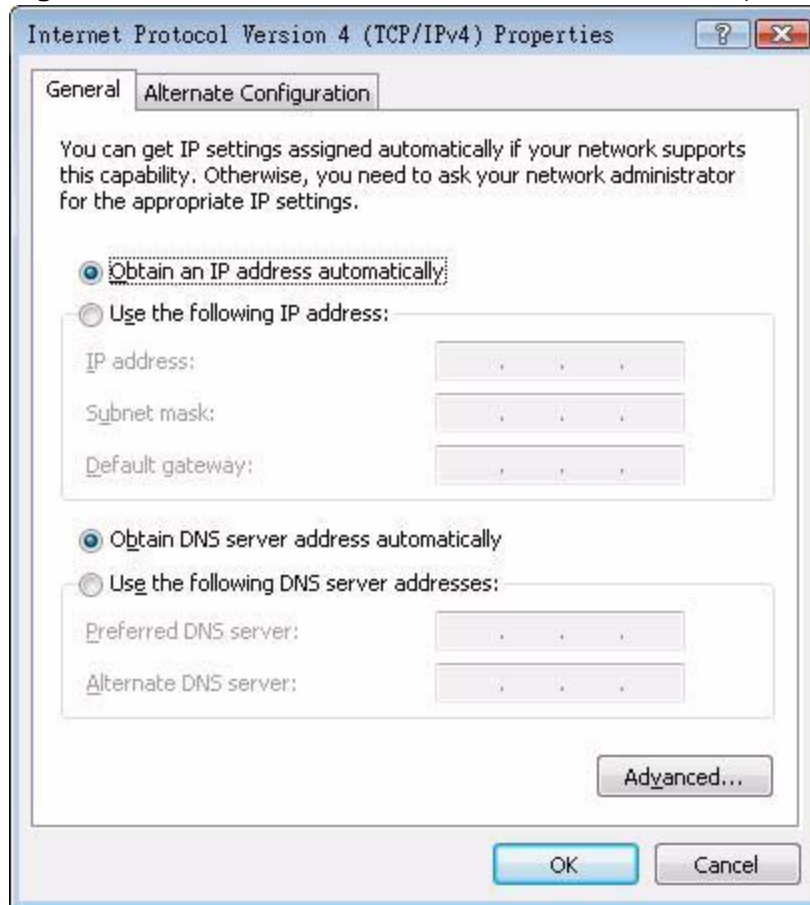
8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

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

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

**2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

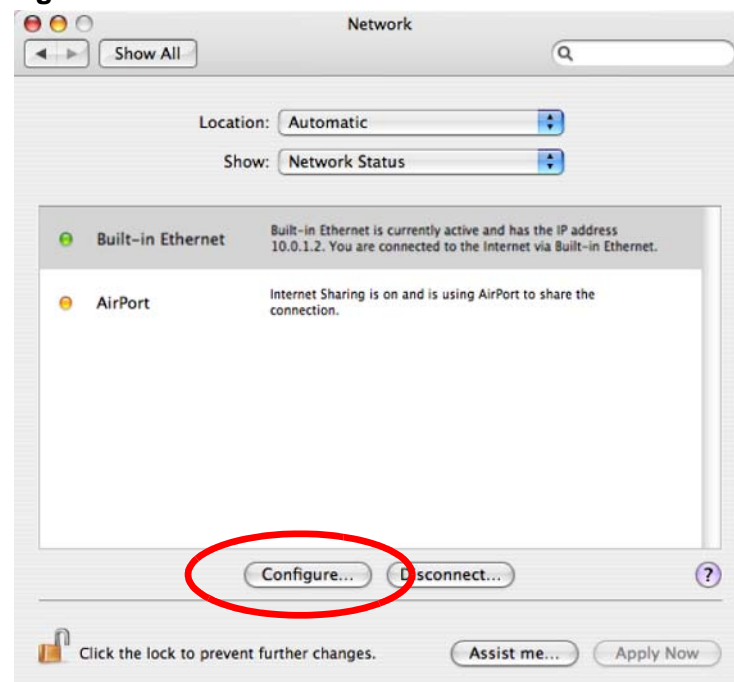**1** Click **Apple** > **System Preferences**.

Figure 117 Mac OS X 10.4: Apple Menu
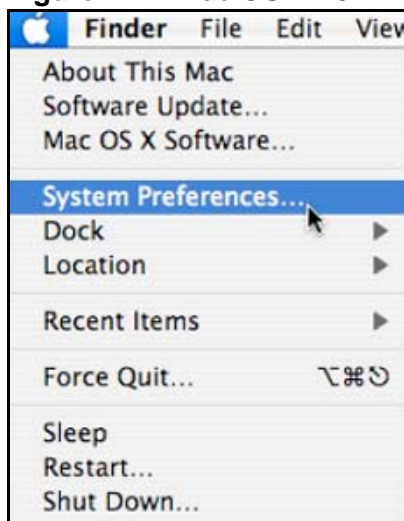
2 In the **System Preferences** window, click the **Network** icon.

Figure 118 Mac OS X 10.4: System Preferences

3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

Figure 119 Mac OS X 10.4: Network Preferences

4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.
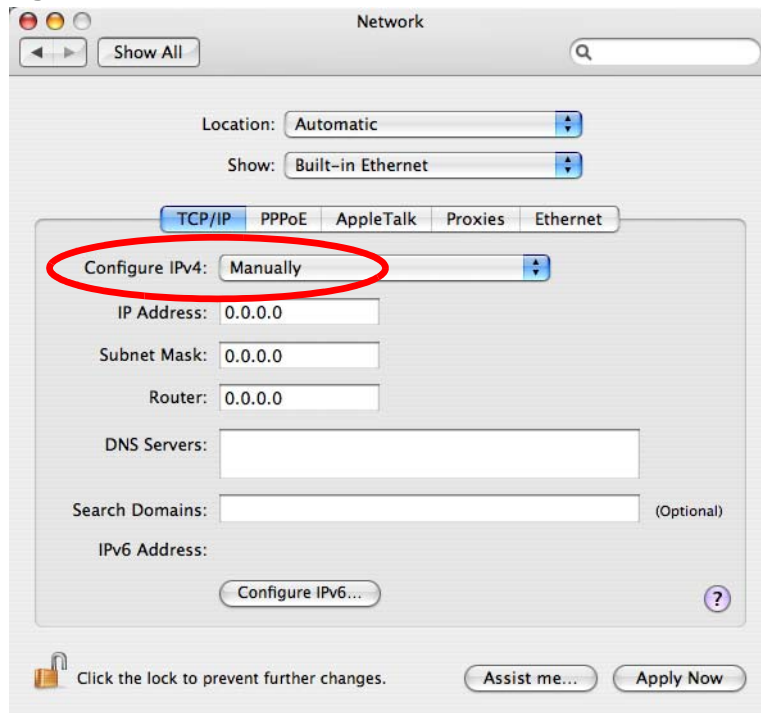
Figure 120 Mac OS X 10.4: Network Preferences > TCP/IP Tab.
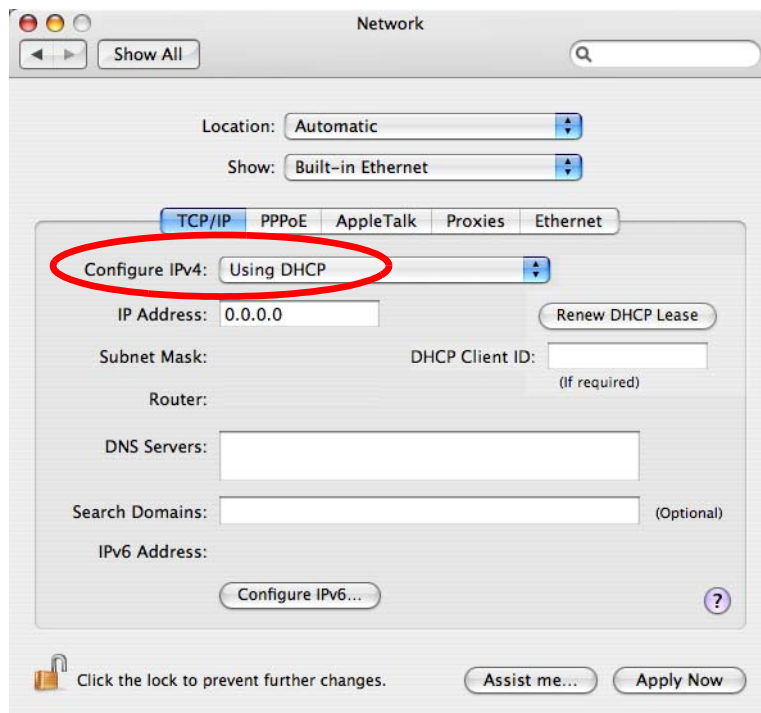
5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.

• In the **Router** field, type the IP address of your device.

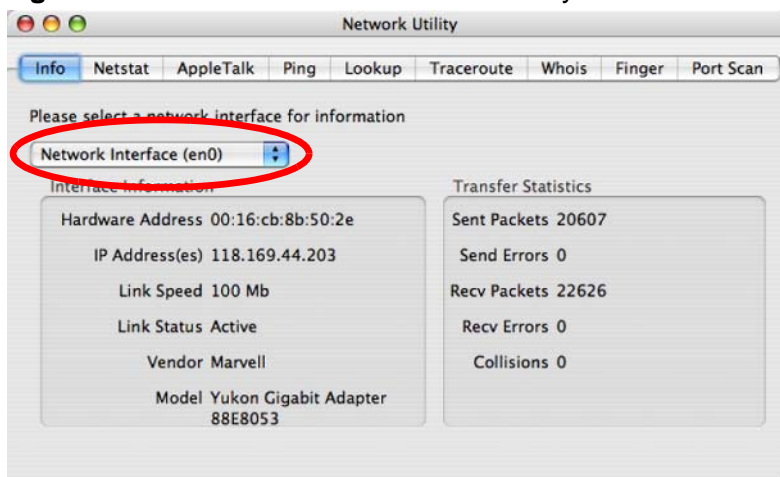**Figure 121**   Mac OS X 10.4: Network Preferences > Ethernet

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

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

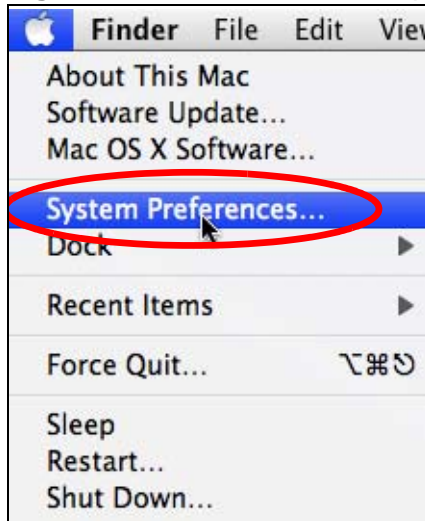**Figure 122**   Mac OS X 10.4: Network Utility

Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

1 Click **Apple** > **System Preferences**.

Figure 123 Mac OS X 10.5: Apple Menu
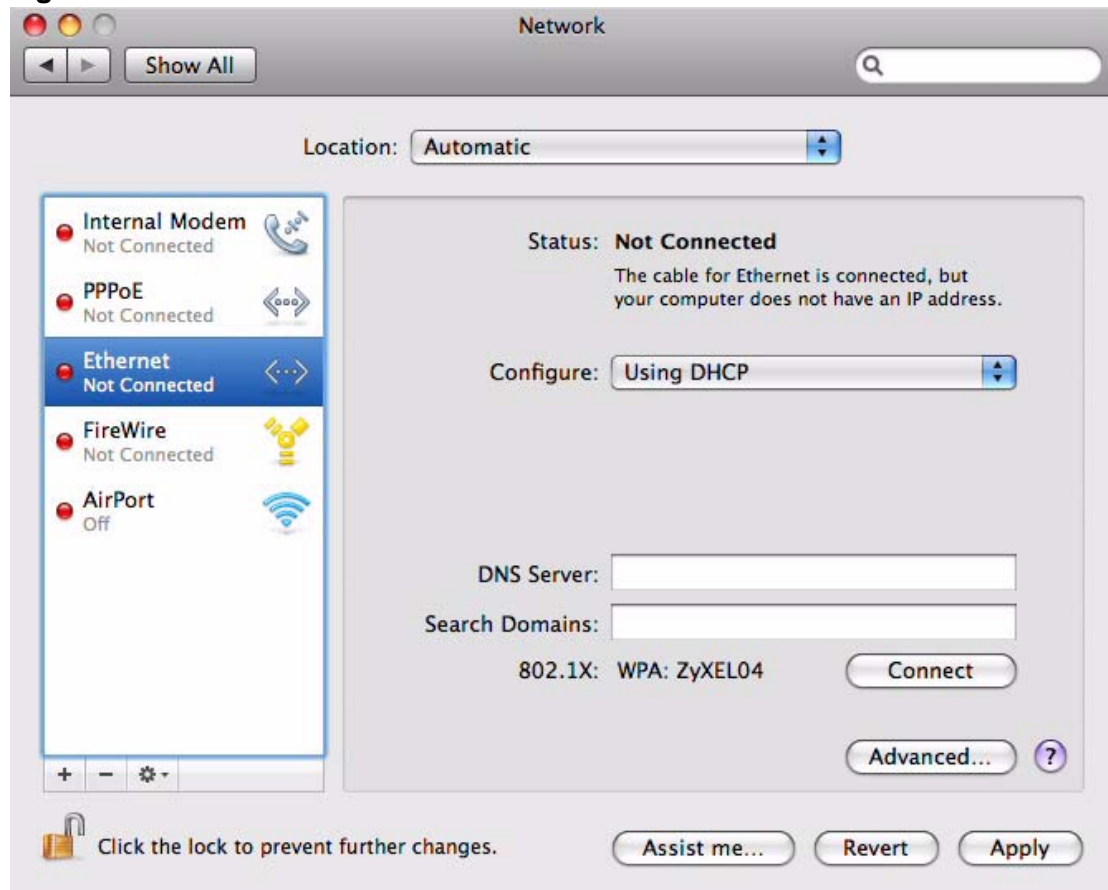

2 In **System Preferences**, click the **Network** icon.

Figure 124 Mac OS X 10.5: Systems Preferences

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

Figure 125 Mac OS X 10.5: Network Preferences > Ethernet

4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.

- In the **Router** field, enter the IP address of your ZyXEL Device.

Figure 126 Mac OS X 10.5: Network Preferences > Ethernet
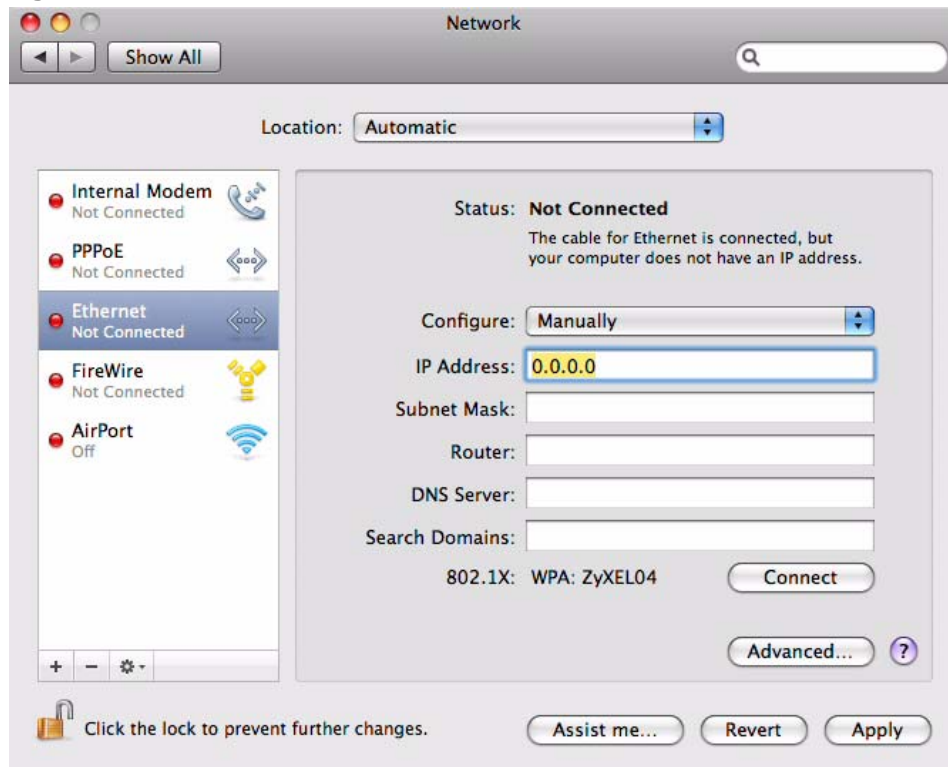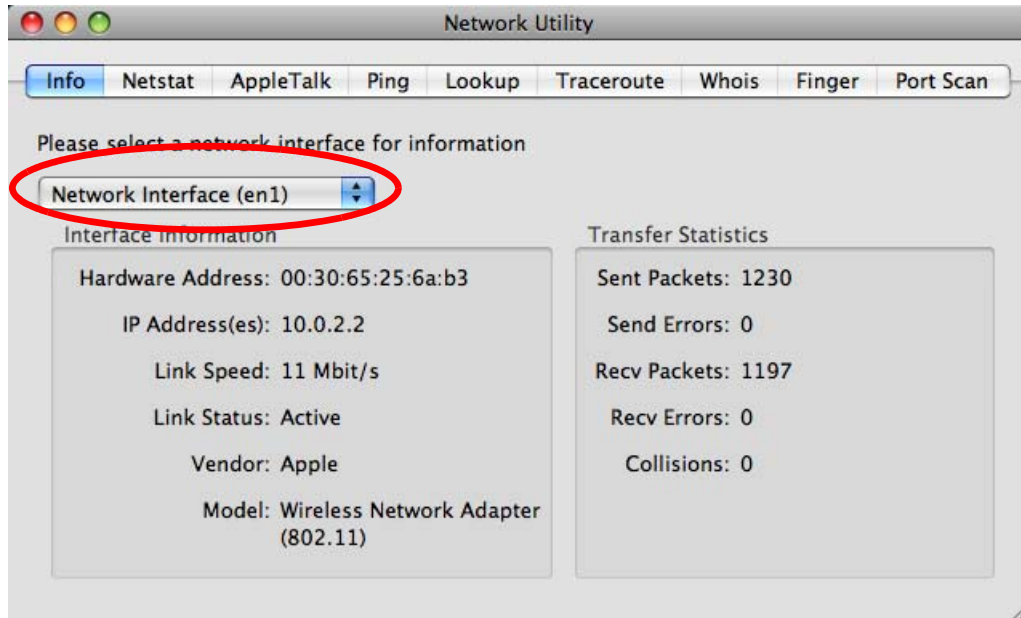

6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 127 Mac OS X 10.5: Network Utility


Linux: Ubuntu 8 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

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

Follow the steps below to configure your computer IP address in GNOME:

1 Click **System** > **Administration** > **Network**.

Figure 128   Ubuntu 8: System > Administration Menu
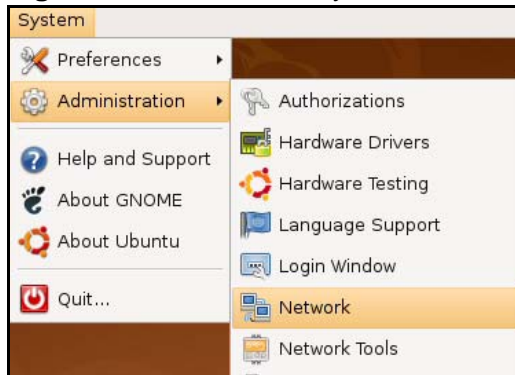
2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 129   Ubuntu 8: Network Settings > Connections
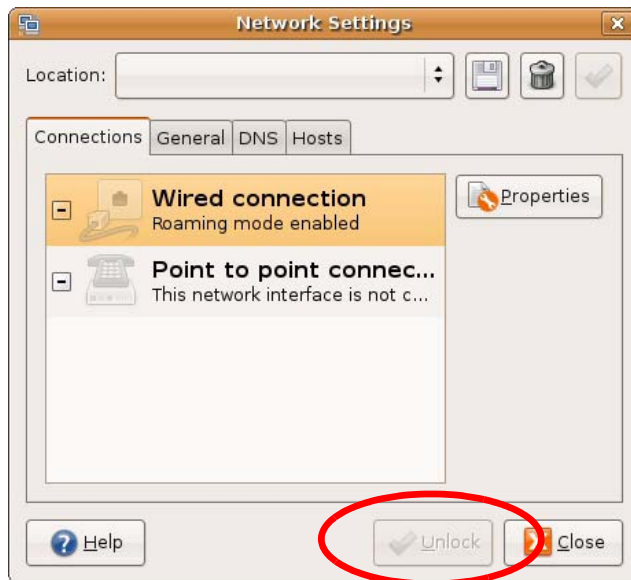
3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 130 Ubuntu 8: Administrator Account Authentication

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 131 Ubuntu 8: Network Settings > Connections

5   The **Properties** dialog box opens.

Figure 132   Ubuntu 8: Network Settings > Properties

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6   Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

**Figure 133** Ubuntu 8: Network Settings > DNS

8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices**

tab. The **Interface Statistics** column shows data if your connection is working properly.

**Figure 134** Ubuntu 8: Network Tools
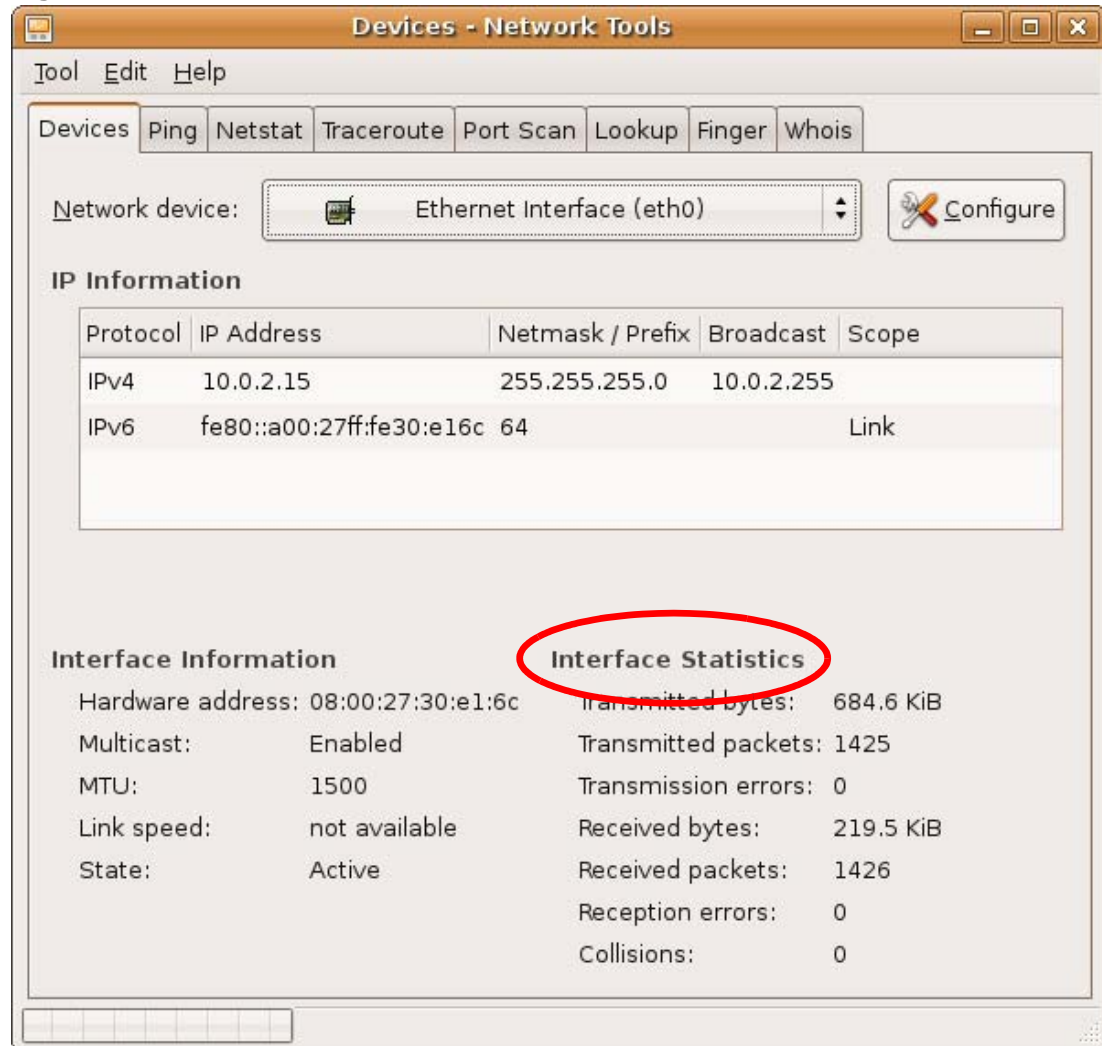
Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

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

Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu** > **Computer** > **Administrator Settings (YaST)**.

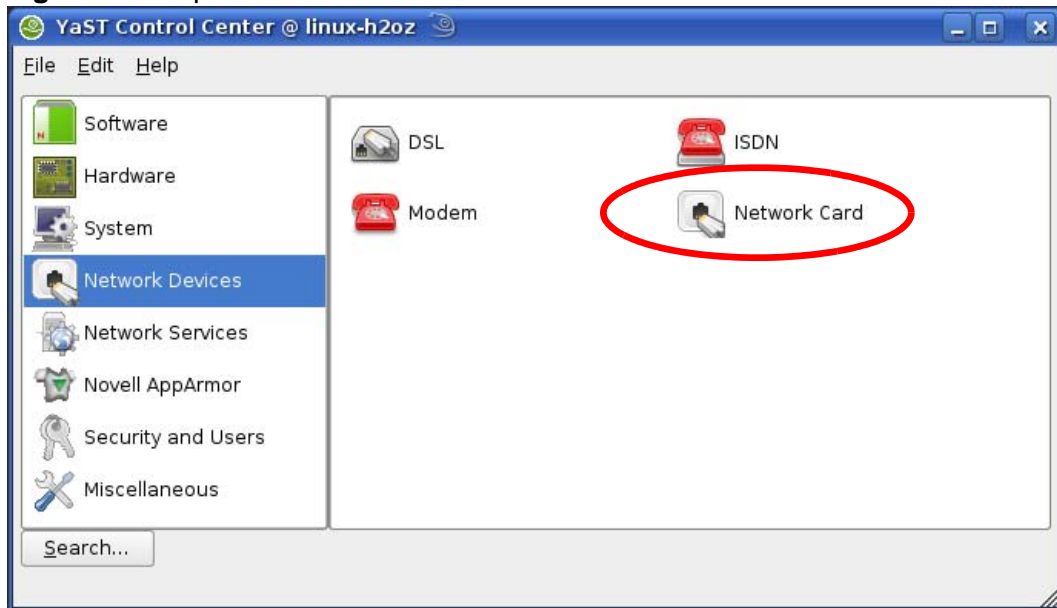**Figure 135** openSUSE 10.3: K Menu > Computer Menu
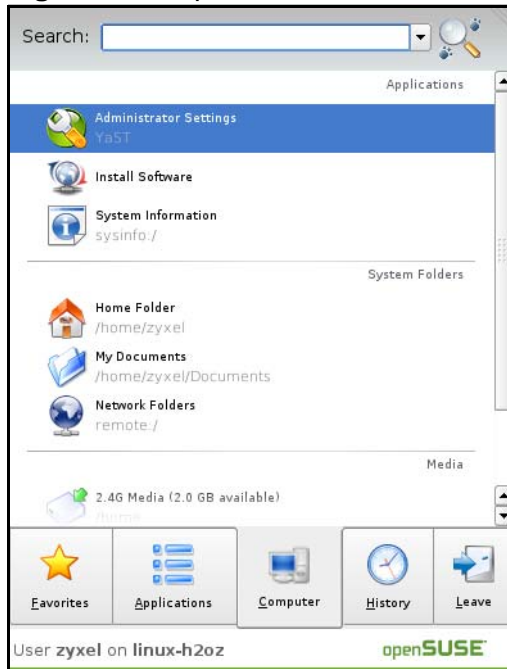
2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 136 openSUSE 10.3: K Menu > Computer Menu

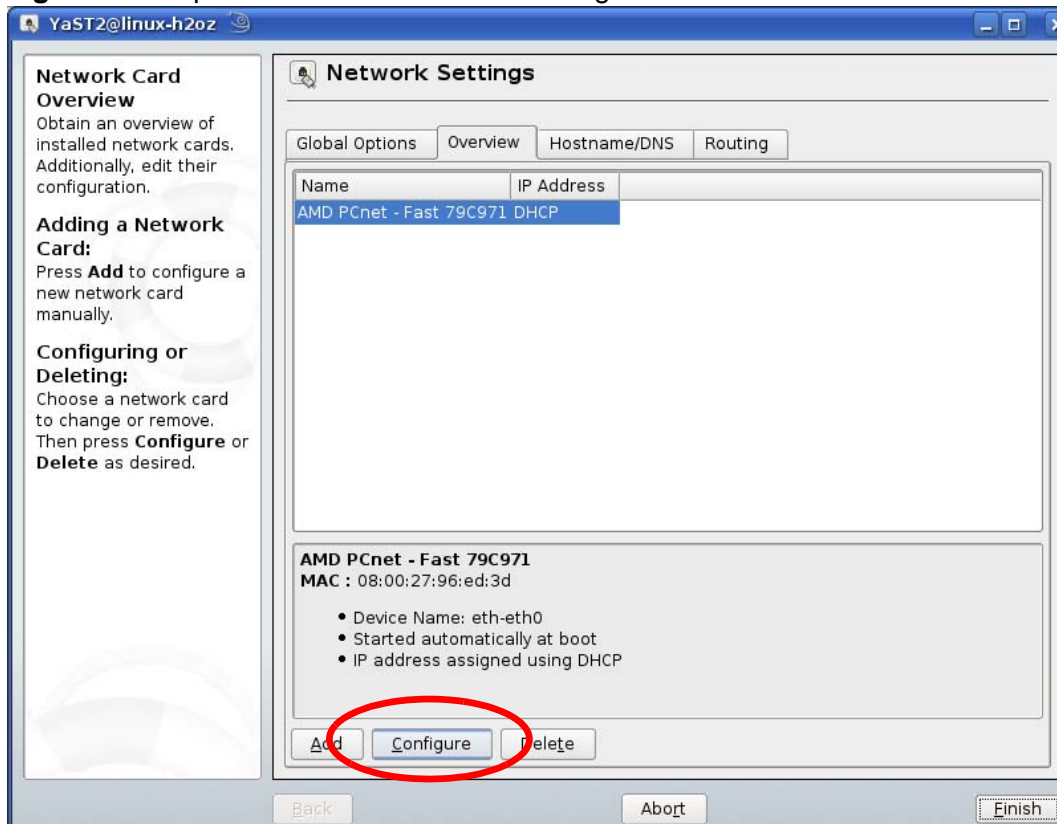**3** When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.
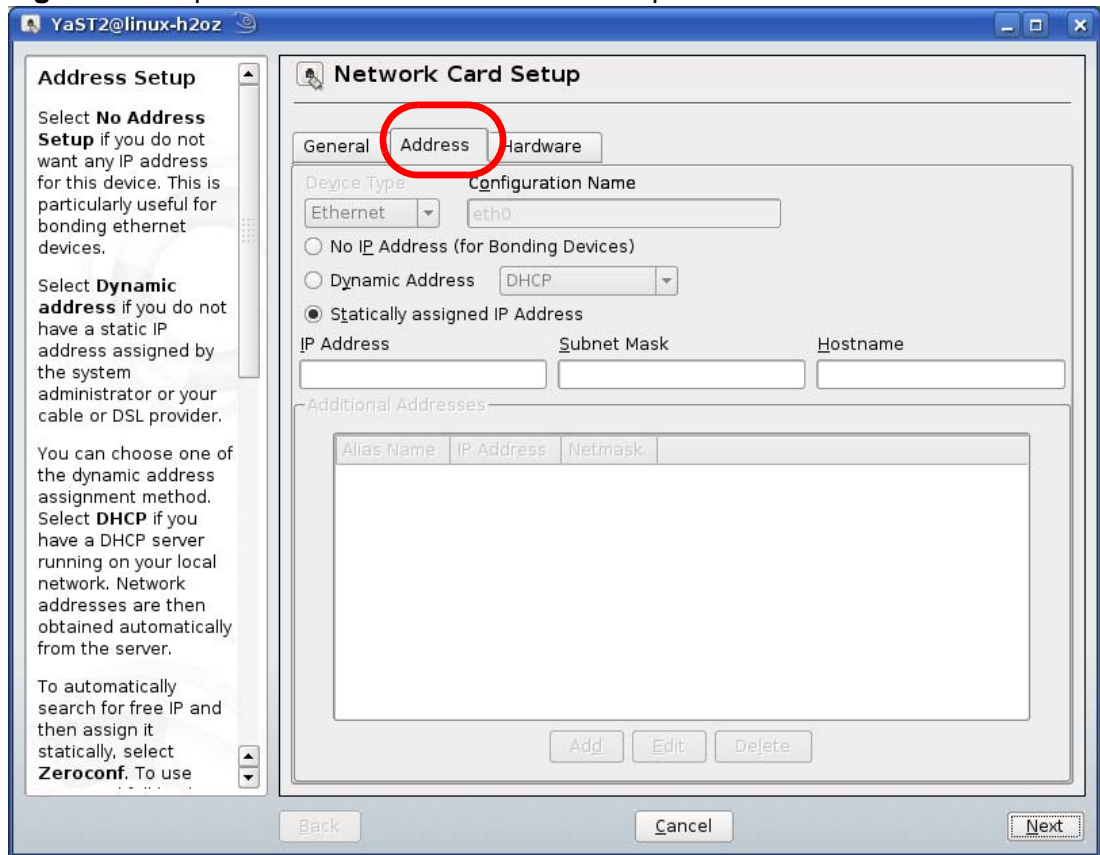
Figure 137 openSUSE 10.3: YaST Control Center

4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 138 openSUSE 10.3: Network Settings

5   When the **Network Card Setup** window opens, click the **Address** tab

Figure 139   openSUSE 10.3: Network Card Setup

6   Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7   Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 140 openSUSE 10.3: Network Settings
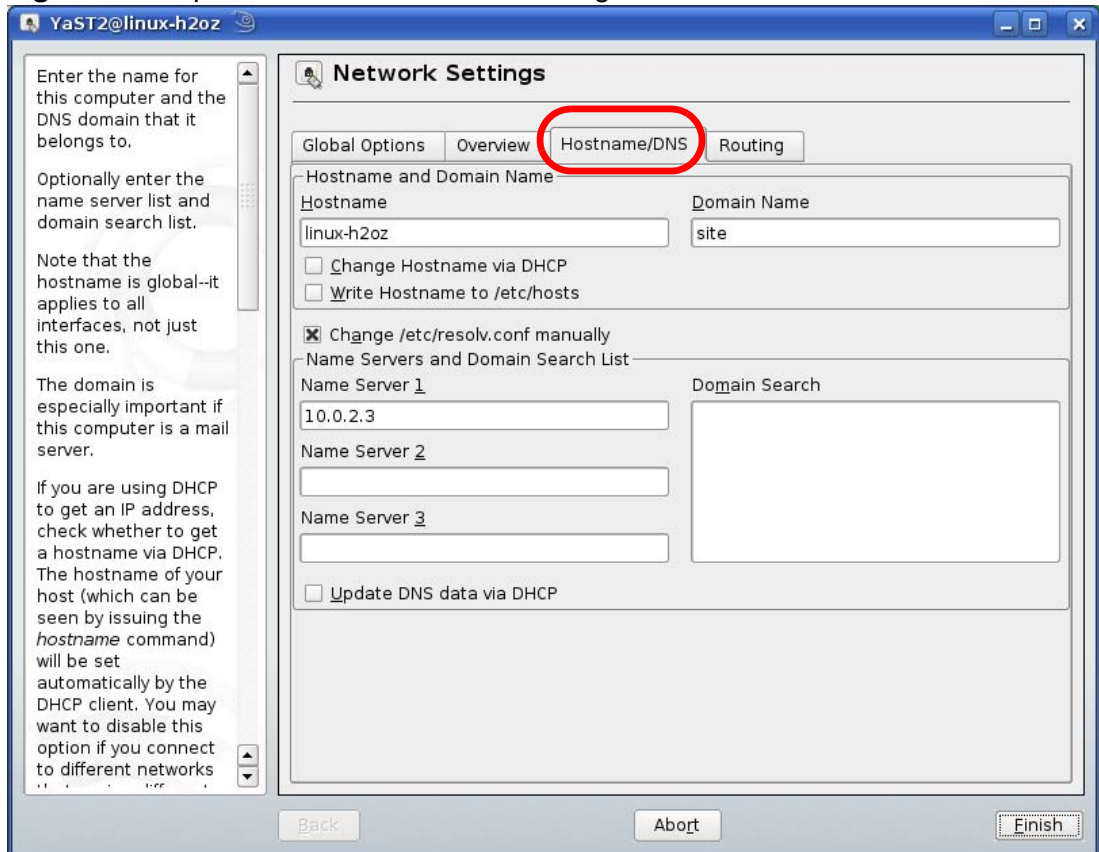
9 Click **Finish** to save your settings and close the window.

Verifying Settings

Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 141 openSUSE 10.3: KNetwork Manager
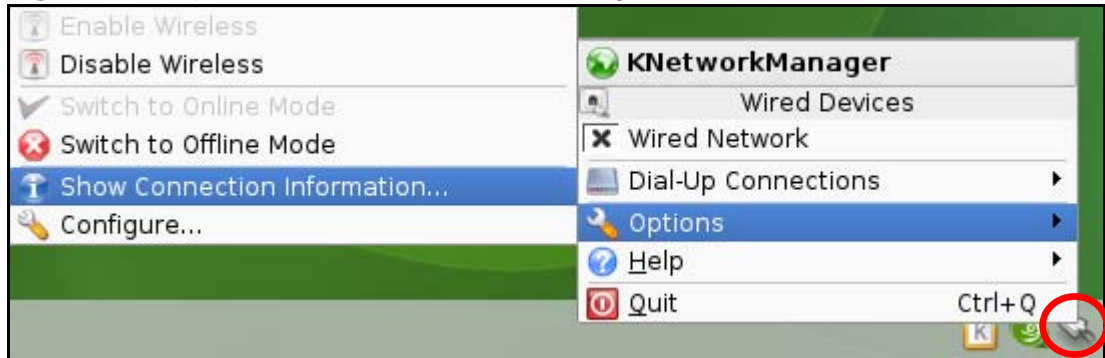
When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 142 openSUSE: Connection Status - KNetwork Manager

B

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.
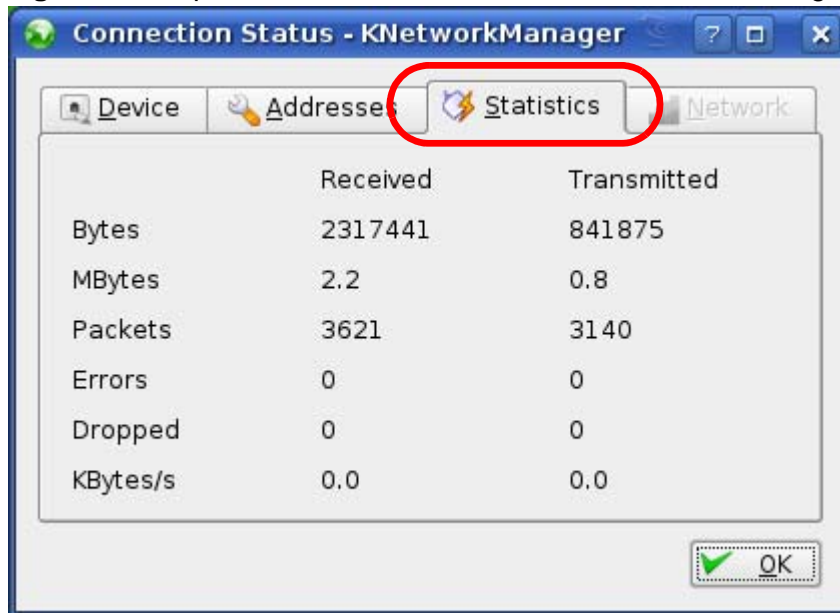
Internet Explorer Pop-up Blockers

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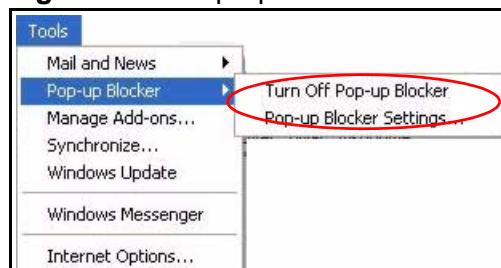
You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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 144 Internet Options: Privacy
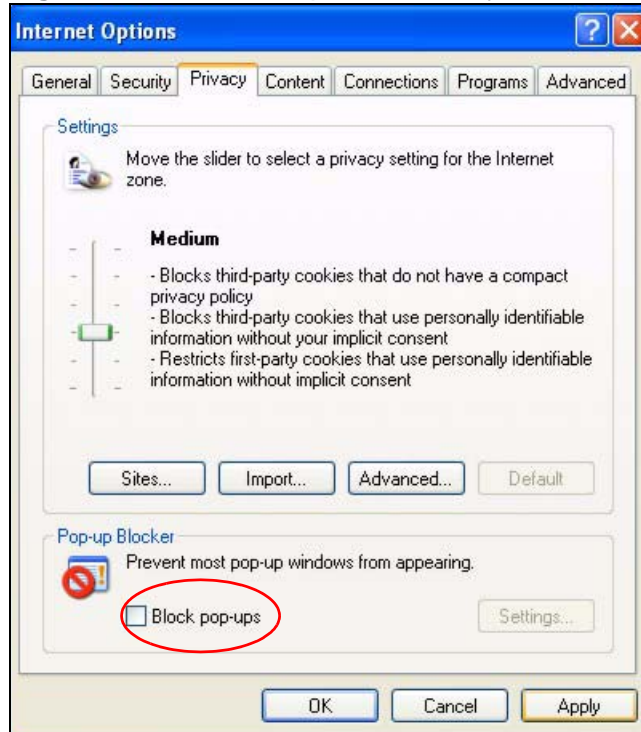
3 Click **Apply** to save this setting.

Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 145 Internet Options: Privacy
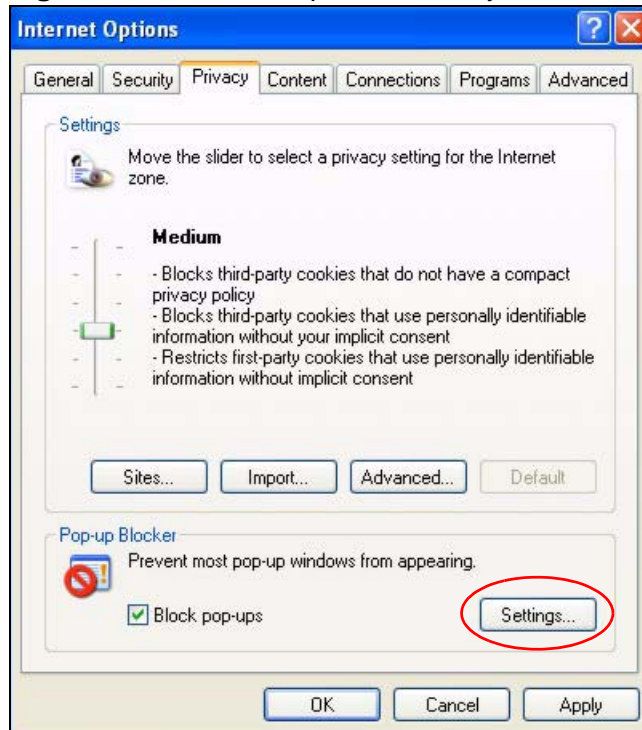
3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

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

Figure 146 Pop-up Blocker Settings
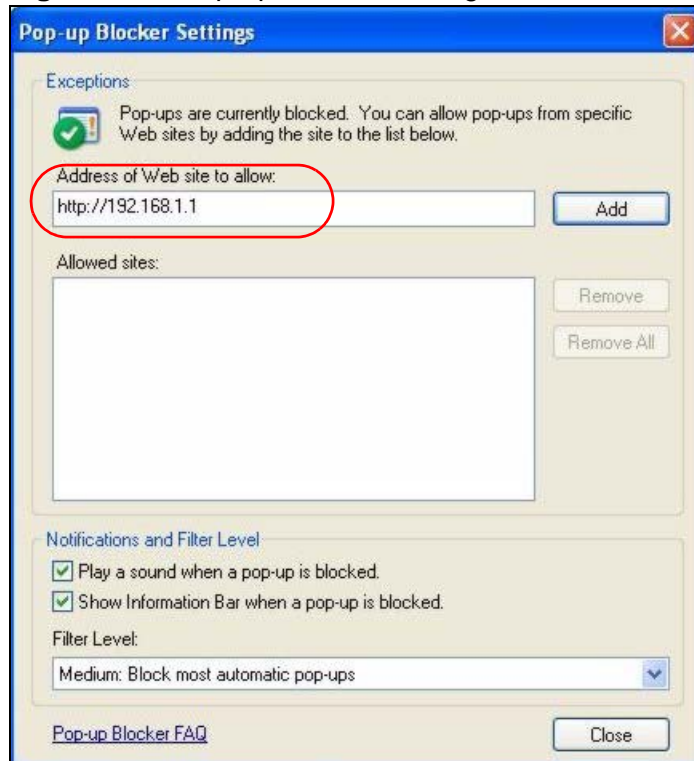
5 Click **Close** to return to the **Privacy** screen.

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

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

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

Figure 147 Internet Options: Security
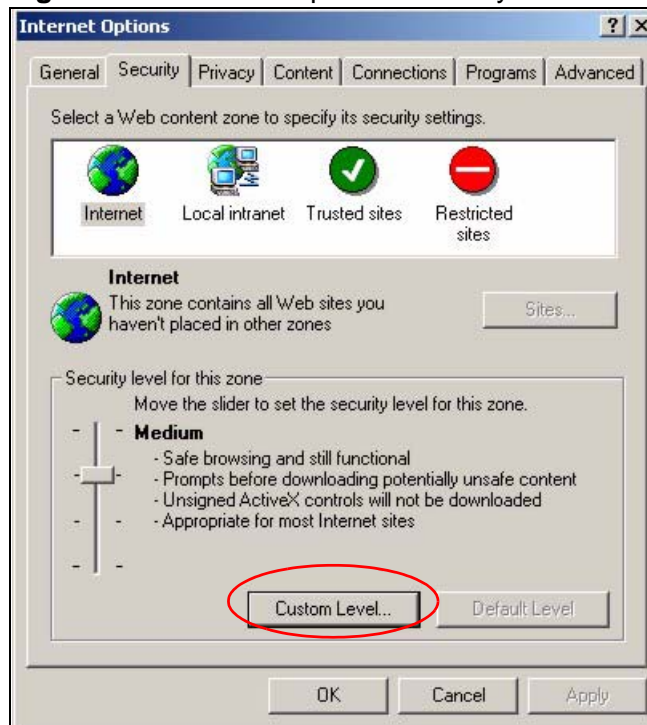
2 Click the **Custom Level...** button.

3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 148 Security Settings - Java Scripting
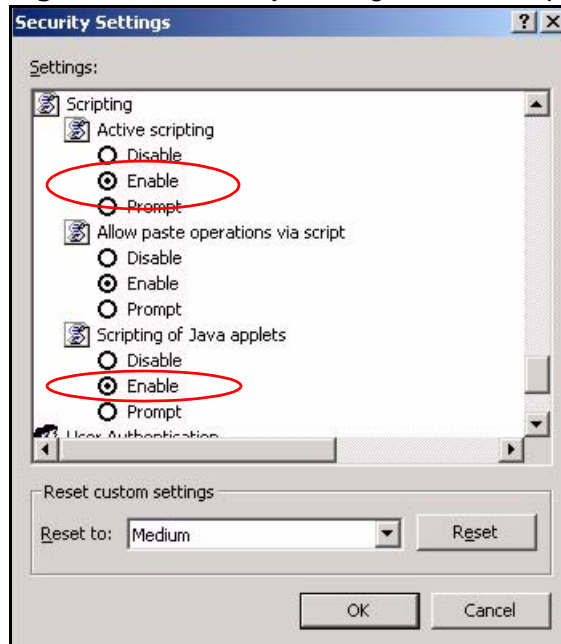
Java Permissions

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

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

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 149 Security Settings - Java
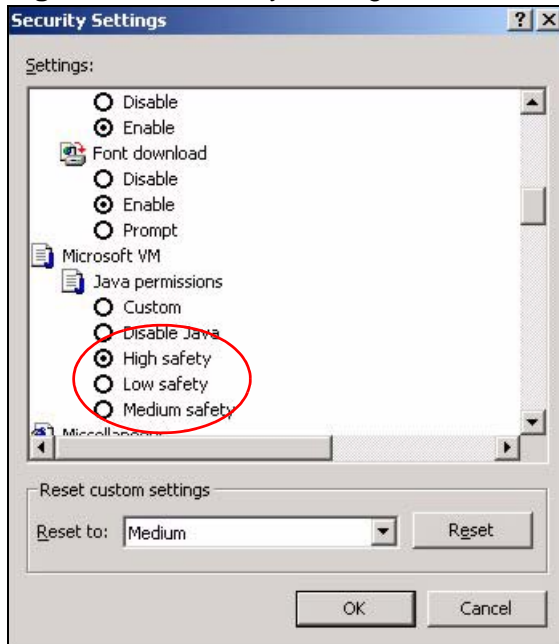
JAVA (Sun)

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

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 150 Java (Sun)
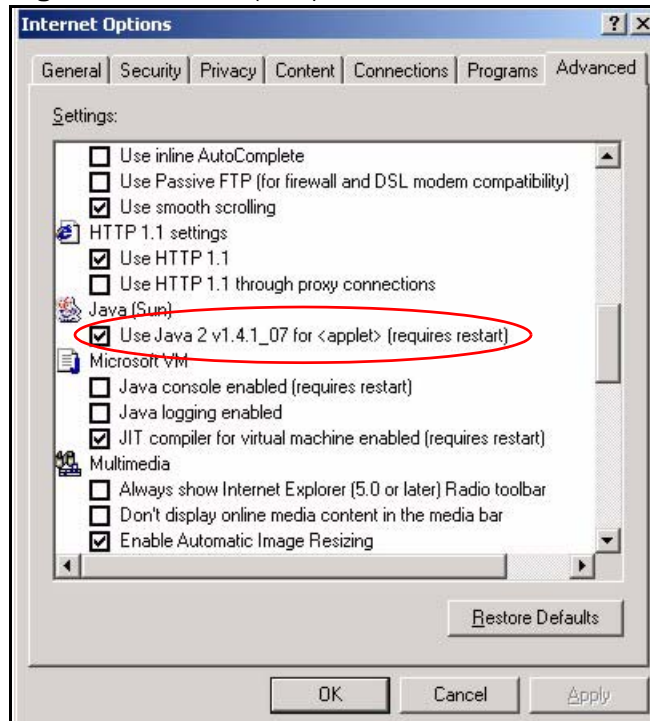
Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 151 Mozilla Firefox: Tools > Options
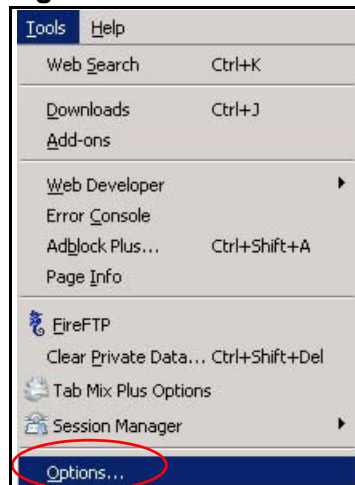
Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 152   Mozilla Firefox Content Security
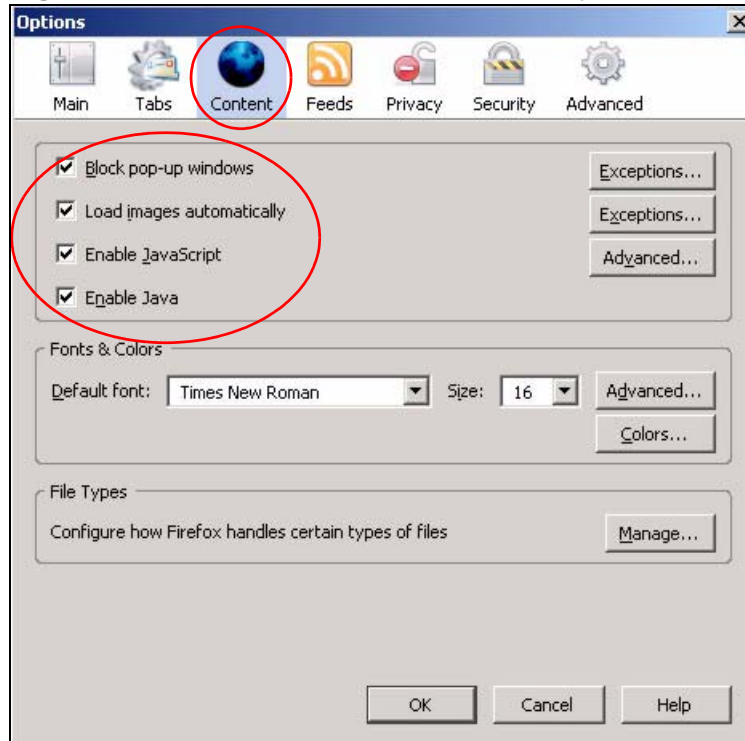
IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

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

Introduction to IP Addresses

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

Structure

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

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

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

Figure 153 Network Number and Host ID
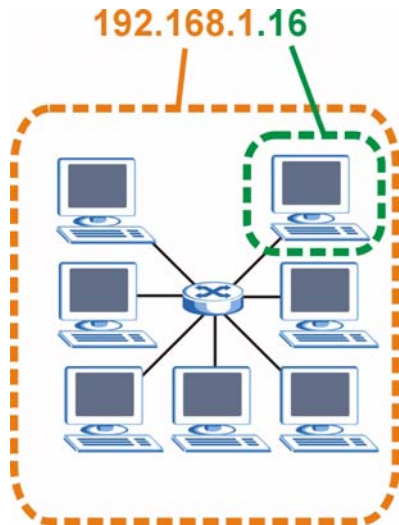
How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

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 79 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 80   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 81   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 82   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 154 Subnetting Example: Before Subnetting
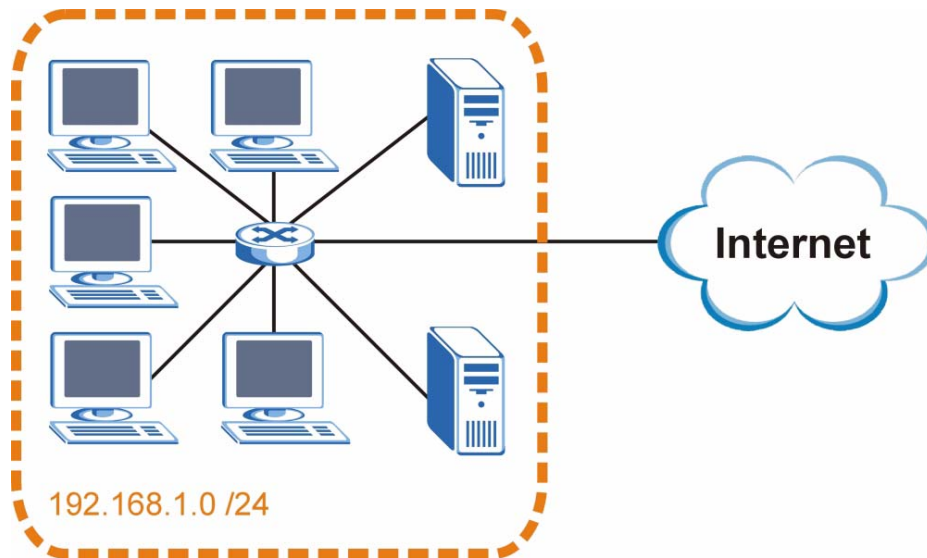
You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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**.
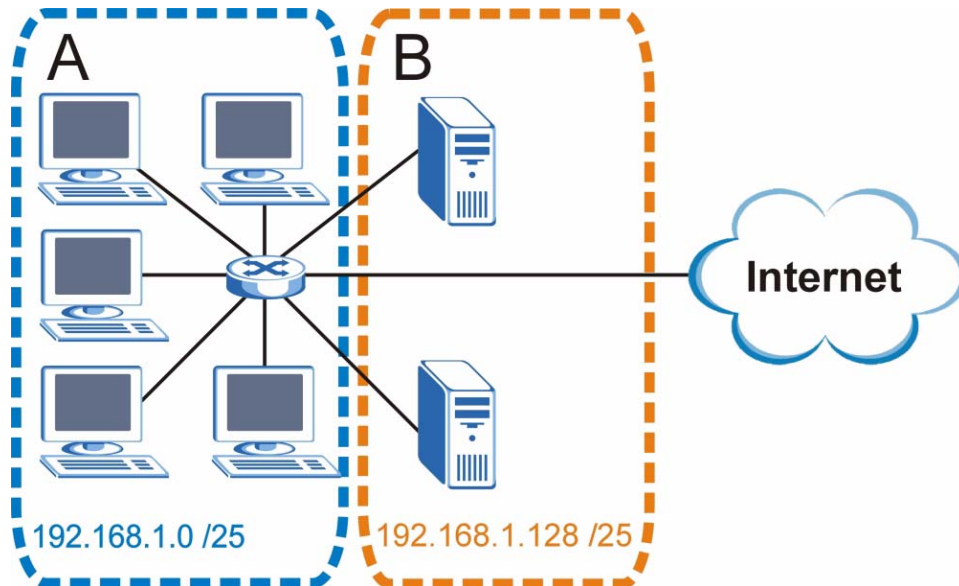
Figure 155   Subnetting Example: After Subnetting

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 83 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 84 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 85 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 86 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 86   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 87   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 88   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 89 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 ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP

address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

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

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

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

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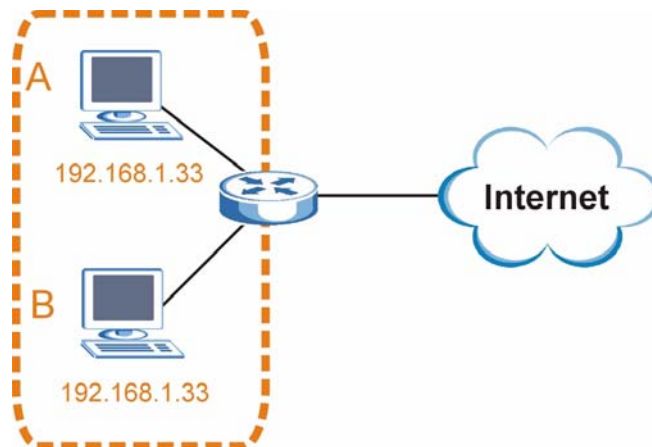
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP

address to computer **A** or setting computer **A** to obtain an IP address automatically.

Figure 156 Conflicting Computer IP Addresses Example

Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

**Figure 157** Conflicting Computer IP Addresses Example
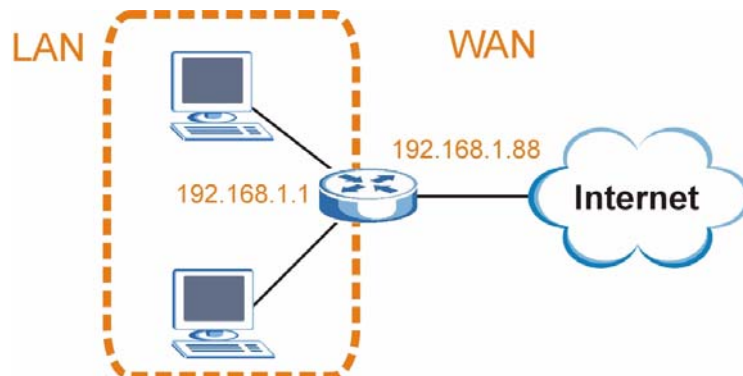
Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address.

The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 158 Conflicting Computer and Router IP Addresses Example

D
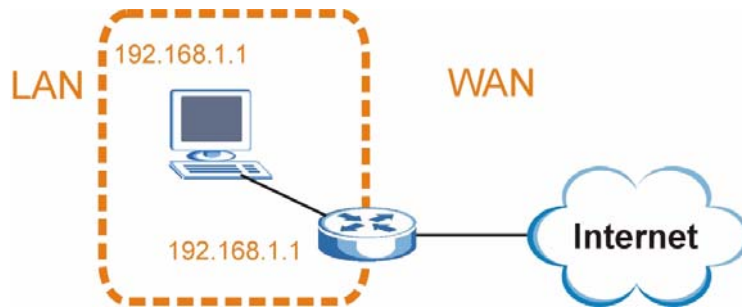
Wireless LANs

Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 159   Peer-to-Peer Communication in an Ad-hoc Network
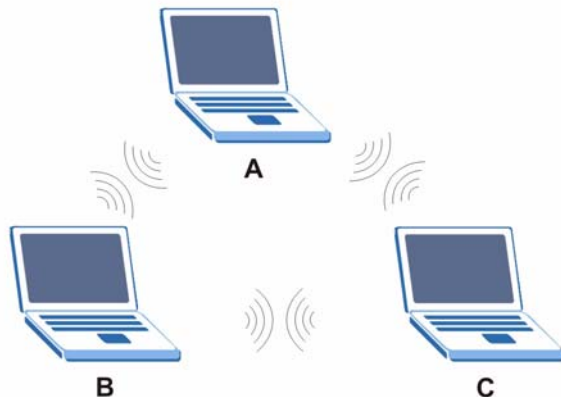

BSS

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

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate

with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 160 Basic Service Set
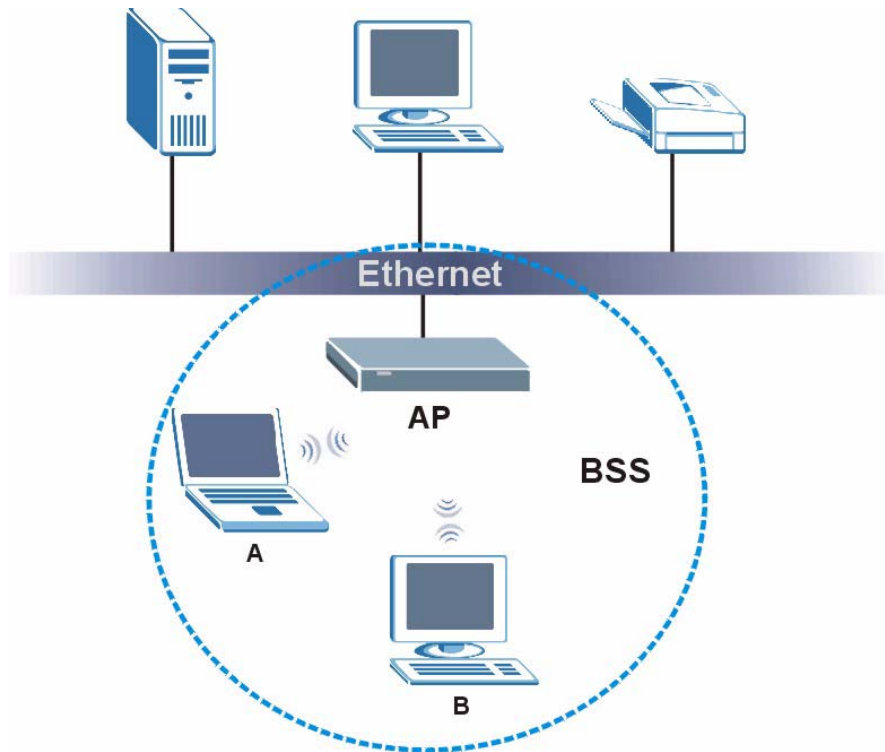
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 161   Infrastructure WLAN
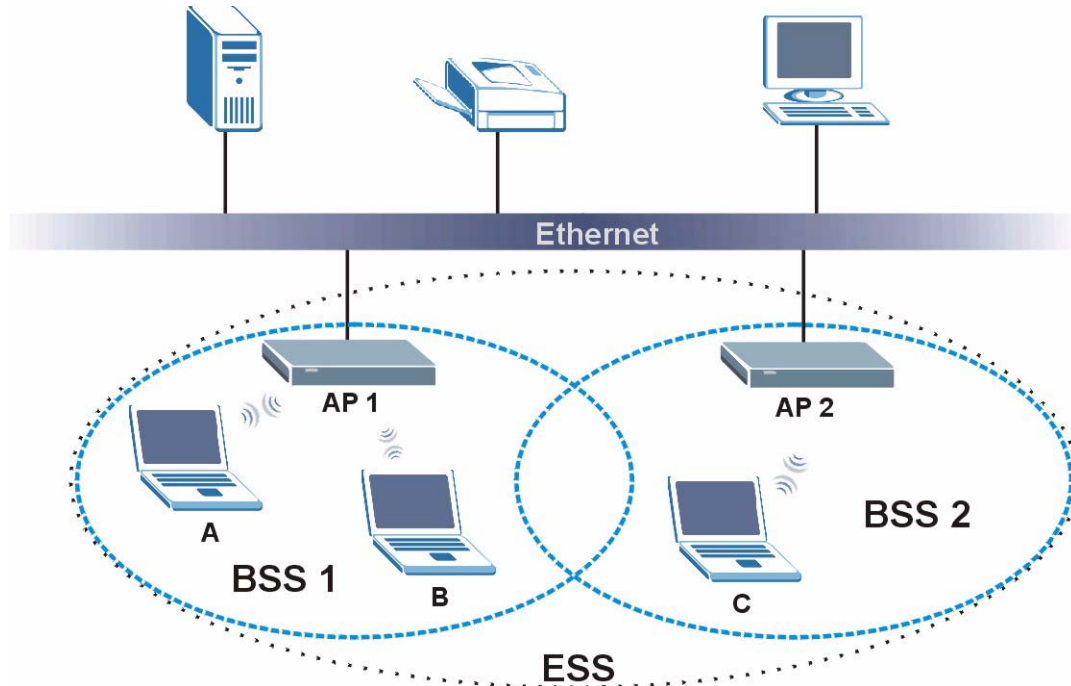
Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or

wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 162 RTS/CTS
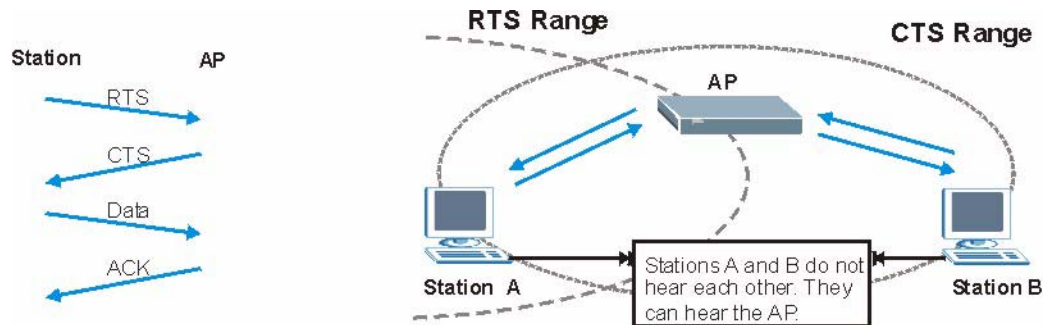
When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

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

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

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

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

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

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

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has

several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 90 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Table 91 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
	WPA2
Most Secure	

Note: You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 92 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption

keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1 The AP passes the wireless client's authentication request to the RADIUS server.

2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 163 WPA(2) with RADIUS Application Example
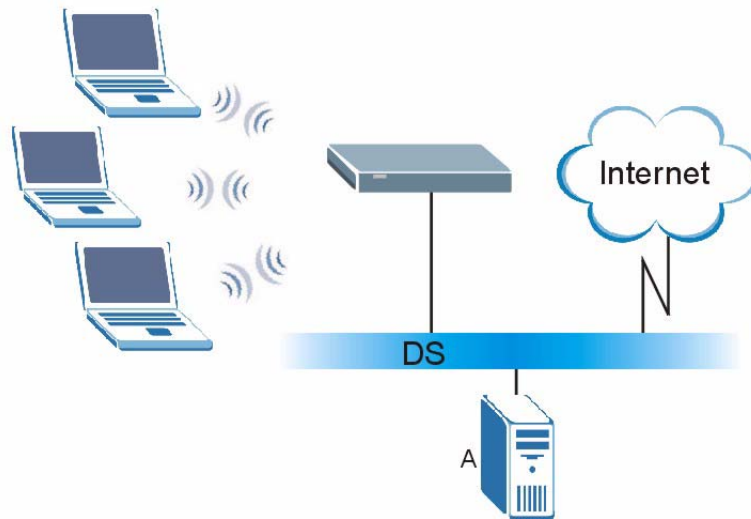
WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 164 WPA(2)-PSK Authentication
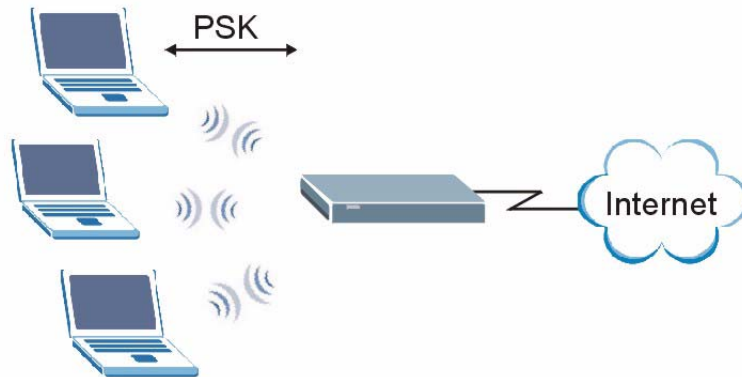
Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 93 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.

- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

E

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 94   Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.

Table 94 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).

Table 94 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

281

Table 94 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

F

Open Software Announcements

End-User License Agreement for "P-663HN-51"

Note: WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL on its Open Source web site (ftp://opensource.zyxel.com) (collectively the "Open-Sourced Components") You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the online electronic documentation for the Software (ftp://opensource.zyxel.com), and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO

NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

12.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The

exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

Note: Some components of the P-663HN-51 incorporate source code covered under the GPL License, LGPL License, BSD License, and BSD like License. To obtain the source code covered under those Licenses, please check ftp://opensource.zyxel.com to get it.

G

Legal Information

Copyright

Copyright © 2009 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the ZyXEL Device is subject to the terms and conditions of any related service providers.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

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 ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index