NBG-510S

802.11g Wireless Remote Access Broadband Gateway

User's Guide

Version 1.00
7/2007
Edition 1

DEFAULT LOGIN	
IP Address	**http://192.168.1.1**
User Name	**admin**
Password	**1234**

ZyXEL

www.zyxel.com

About This Guide

Intended Audience

This manual is intended for home and small business network administrators who want to install and configure the ZyXEL Device. This guide assumes that the administrators who are familiar with basic network configuration.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for initial secure remote access to the LAN.
- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.
- Supporting Disk

  Refer to the included CD for support documents.
- ZyXEL Web Site

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

User Guide Feedback

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

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

E-mail: techwriters@zyxel.com.tw

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.

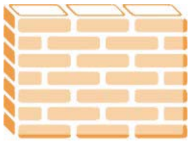
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NBG-510S 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, **Network** > **WAN** > **Internet Connection** means you first click **Network** in the navigation panel, then the **WAN** sub menu and finally the **Internet Connection** 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.

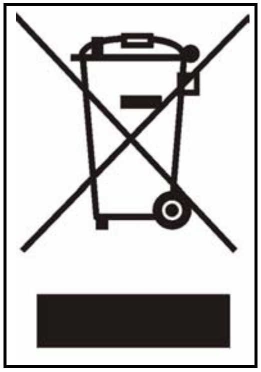
ZyXEL Device 	Computer 	Notebook computer
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router
Broadband modem or router 		

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do NOT remove the plug and plug into a wall outlet by itself; always attach the plug to the power supply first before insert into the wall
- 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.
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

This product is recyclable. Dispose of it properly.



Contents Overview

Table of Contents

List of Figures

List of Tables

PART I
Introduction

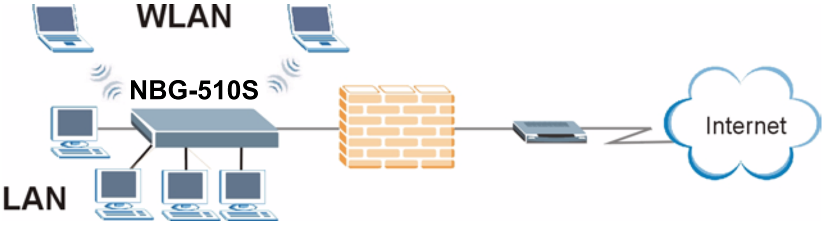
Introducing the ZyXEL Device

This chapter introduces the main applications of the ZyXEL Device.

1.1 Overview

The NBG-510S Wireless SSL Remote Access Gateway provides wireless connectivity, shared Internet access, and firewall protection. It also provides easy, secure remote user access for file sharing and management of home network computers.

Figure 1 Secure Wired and Wireless Internet Access Through Broadband Modem or Router

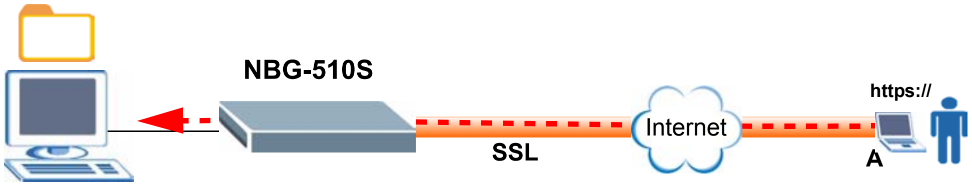


- The ZyXEL Device is easy to install and configure.
- Directly connect computers or Ethernet devices to the four-port LAN switch.
- The wireless LAN feature (WLAN) supports IEEE 802.11b and IEEE 802.1g devices as well as Super G wireless technology for enhanced wireless data throughput speeds.
- NAT and DHCP server features let you share high-speed Internet access through a broadband modem or router.
- Strong firewall protection secures your network from attacks.

1.1.1 Remote User Access Secured by SSL

The secure remote access portal (user portal) makes it easy to give remote users secure access to shared files on your home computers. The secure remote access uses SSL (the Secure Socket Layer protocol), so no security software installation is required. Remote users can use Internet Explorer or other standard web browsers. Here remote user **A** uses a web browser to go to the secure remote access portal and securely access a shared file on a computer behind the ZyXEL Device.

Figure 2 SSL-protected File Sharing for Remote Users



The secure remote access portal also allows secure remote desktop connections for managing computers on your network. The secure remote access screens (user portal) includes the screens the remote users log into and use for secure file sharing and remote computer management.

1.2 Good Habits for Managing the ZyXEL Device

Use the web configurator for everyday management of the ZyXEL Device with a (supported) web browser.

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 is 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.

2

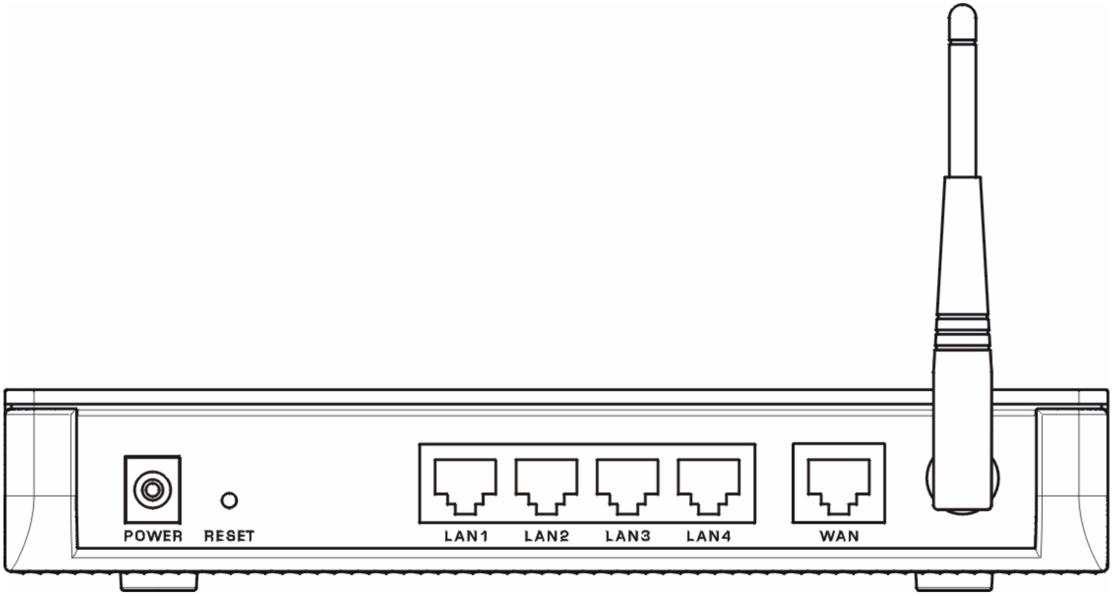
Hardware Connection

This chapter describes the port connections and LEDs.

2.1 Ports and Connectors

This section describes the ports and connectors on the ZyXEL Device. Refer to the Quick Start Guide for information on connecting the ZyXEL Device for initial setup and basic configuration.

Figure 3 Rear Panel



The following table describes the port connections.

Table 1 Rear Panel

LABEL	DESCRIPTION
POWER	Use the included power adaptor to connect the **POWER** socket to an appropriate power source. See Appendix A on page 171 for the power adaptor's specifications.
RESET	Use this button to reset the ZyXEL Device to the factory default settings. See Section 3.6 on page 38 for details.
LAN 1~4	Use Ethernet cables to connect these 10/100 Mbps Ethernet ports to computers, servers or Ethernet devices on your network.
WAN	Use an Ethernet cable to connect this Ethernet port to a broadband modem or router.

2.2 LEDs

The following table describes the LEDs (lights) on the ZyXEL Device.

Figure 4 LEDs

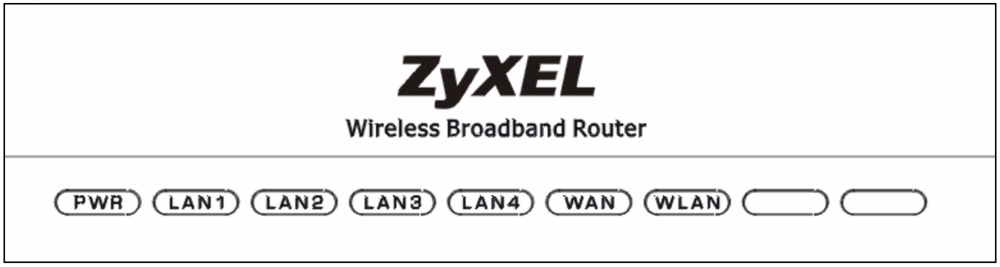


Table 2 LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The ZyXEL Device is receiving power.
		Off	The ZyXEL Device is not receiving power.
LAN/WAN	Yellow	On	This port has a successful 100 Mbps connection.
		Blinking	This port has a successful 100 Mbps connection and is sending/receiving data.
	Green	On	This port has a successful 10 Mbps connection.
		Blinking	This port has a successful 10 Mbps connection and is sending/receiving data.
		Off	This port does not have a successful Ethernet connection.
WLAN	Green	On	The ZyXEL Device's wireless LAN connection is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The ZyXEL Device is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.

3

The Web Configurator

This chapter introduces the web configurator and shows you how to log in as an administrator.

3.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyXEL Device setup and management via Internet browser. The recommended screen resolution is 1024 by 768 pixels. Use one of the following web browsers:

- Internet Explorer 5 (administrator login only), 6.0, or 7.0
- Netscape Navigator 7.2
- Mozilla 1.7.13,
- FireFox 1.5.0.9 or 2.0.

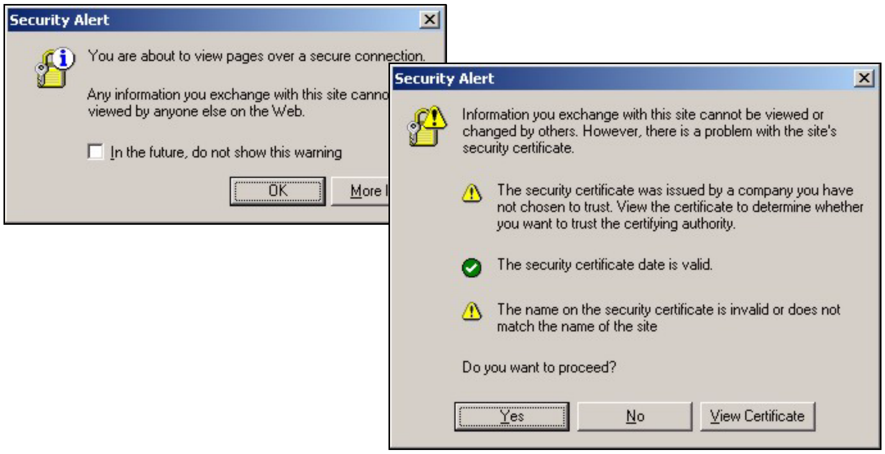
In order to use the web configurator you need to allow:

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

3.2 Logging into the ZyXEL Device

1 Make sure you have properly connected the ZyXEL Device to your network. See the Quick Start Guide.
2 Open your web browser, and go to http://192.168.1.1 (the default LAN IP address).
3 A security alert and/or certificate screen displays. Click **OK** and/or **Yes** to continue.

Figure 5 Login: Security Message



Security Alert

You are about to view pages over a secure connection.

Any information you exchange with this site canno viewed by anyone else on the Web.

□ In the future, do not show this warning

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

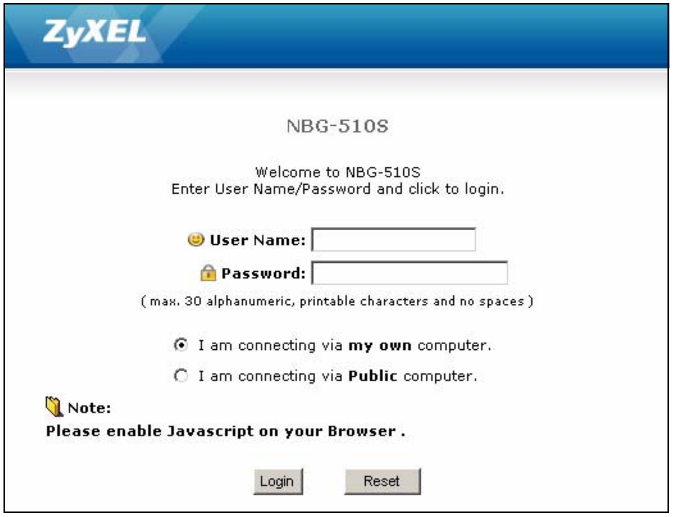
⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

4 The **Login** screen appears. For administrator access, type the administrator user name (default: “**admin**”) and password (default: “**1234**”). For secure remote user access (using the user portal), type your remote user account’s user name and password (see Chapter 25 on page 155 for more on using the secure remote user screens).

- If you are using a computer that is also used by others, select **I am connecting via public computer**. Your web browser cache will be automatically cleaned once you terminate the connection. This prevents anyone from obtaining information from the browser cache.
- If you are using your computer to access the ZyXEL Device, select **I am connecting via my own computer**. Your web browser cache will not be cleaned after you log out.

Figure 6 Login: Enter Account Information



NBG-510S

Welcome to NBG-510S
Enter User Name/Password and click to login.

User Name:

Password:

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

● I am connecting via **my own** computer.

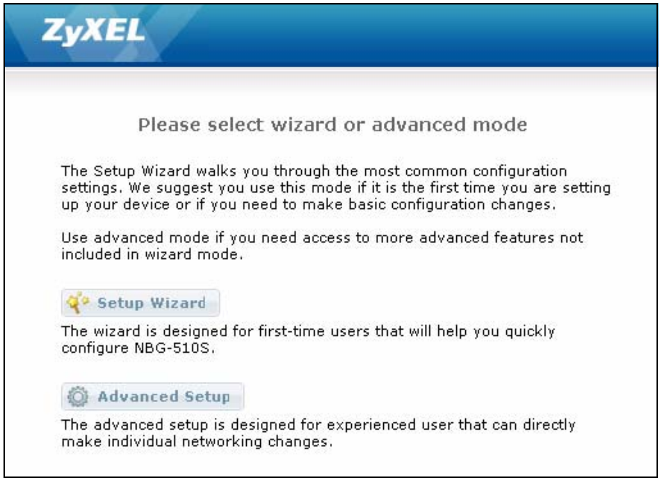
○ I am connecting via **Public** computer.

Note:
Please enable Javascript on your Browser .

5 The initial screen displays as shown.

- Click **Setup Wizard** to configure the ZyXEL Device using the wizard screens and proceed to Chapter 5 on page 41.
- Click **Advanced Setup** to access the main screen (see Figure 10 on page 34) and configure the ZyXEL Device using the advanced configuration screens.

Figure 7 Login: Initial Screen



Please select wizard or advanced mode

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

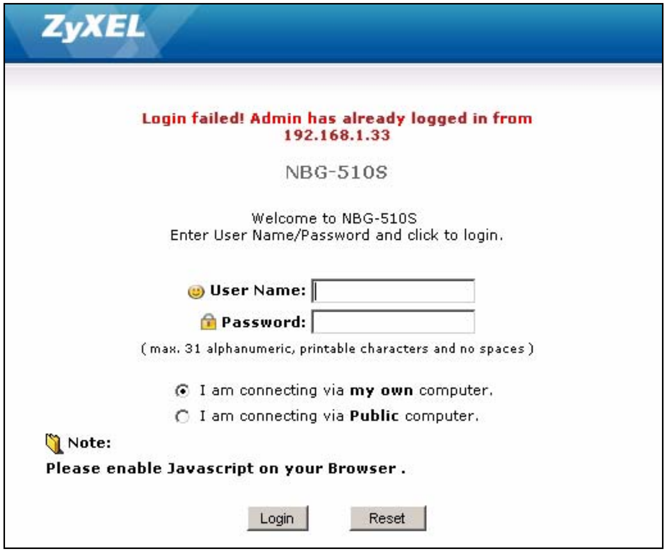
Use advanced mode if you need access to more advanced features not included in wizard mode.

The wizard is designed for first-time users that will help you quickly configure NBG-510S.

The advanced setup is designed for experienced user that can directly make individual networking changes.

If another person is currently logged in using the administrator account, you are not able to log in and a message displays in the screen as shown next.

Figure 8 Login: Admin Already Logged In



Login failed! Admin has already logged in from 192.168.1.33

NBG-510S

Welcome to NBG-510S
Enter User Name/Password and click to login.

User Name:

Password:

(max. 31 alphanumeric, printable characters and no spaces)

● I am connecting via **my own** computer.
○ I am connecting via **Public** computer.

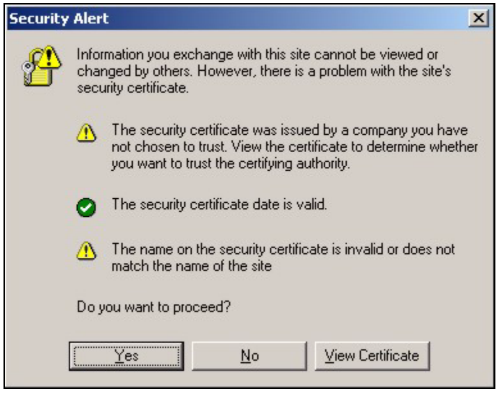
Note:
Please enable Javascript on your Browser .

6 Another certificate screen displays. Click **Yes** to continue.

- The ZyXEL Device automatically forwards administrator sessions to its HTTPS server on TCP port 8443.
- The ZyXEL Device automatically forwards secure remote access sessions to its HTTPS server on TCP port 443.

If the ZyXEL Device is behind a firewall or NAT router, make sure you configure port forwarding or a firewall rule to allow traffic to the ZyXEL Device on TCP port 8443 for administration connections and TCP port 443 for secure remote access connections.

Figure 9 Login Screen: Security Message for Administrator Login



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

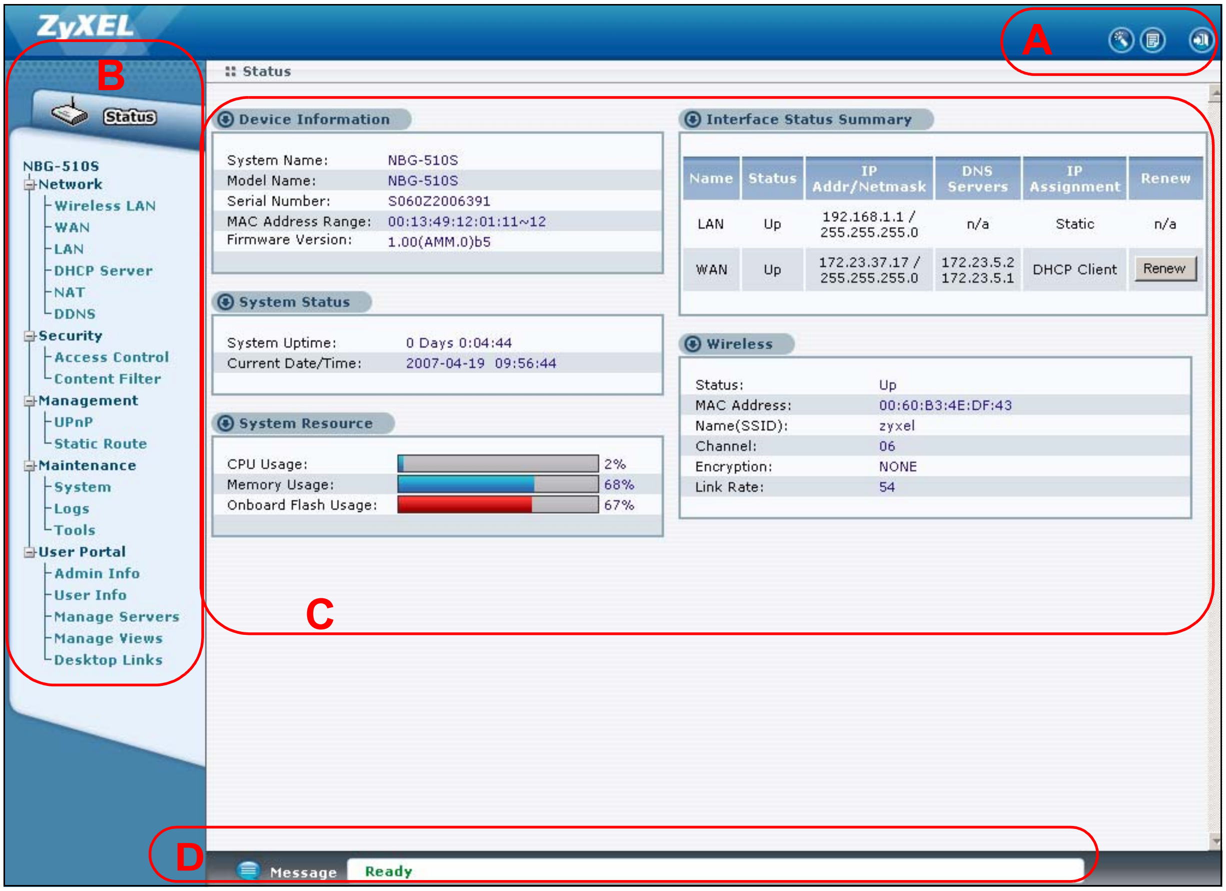
Do you want to proceed?

7 The main screen displays.

3.3 Web Configurator Main Screen

The **Status** screen is the main screen and it is the first screen that displays every time you access the web configurator as an administrator.

Figure 10 Main Screen



Device Information

System Name:	NBG-510S
Model Name:	NBG-510S
Serial Number:	S060Z2006391
MAC Address Range:	00:13:49:12:01:11~12
Firmware Version:	1.00(AMM.0)b5

System Status

System Uptime:	0 Days 0:04:44
Current Date/Time:	2007-04-19 09:56:44

System Resource

CPU Usage:	2%
Memory Usage:	68%
Onboard Flash Usage:	67%

Interface Status Summary

Name	Status	IP Addr/Netmask	DNS Servers	IP Assignment	Renew
LAN	Up	192.168.1.1 / 255.255.255.0	n/a	Static	n/a
WAN	Up	172.23.37.17 / 255.255.255.0	172.23.5.2 172.23.5.1	DHCP Client	Renew

Wireless

Status:	Up
MAC Address:	00:60:B3:4E:DF:43
Name(SSID):	zyxel
Channel:	06
Encryption:	NONE
Link Rate:	54

Message Ready

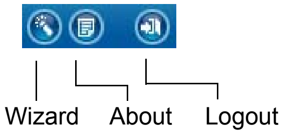
The main screen is divided into these parts:

- **A** - title bar

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

3.3.1 Title Bar

The title bar provides some icons in the upper right corner.



The icons provide the following functions.

Table 3 Title Bar: Web Configurator Icons

ICON	DESCRIPTION
Wizard	Click this icon to open one of the web configurator wizard.
About	Click this icon to display basic information about the ZyXEL Device.
Logout	Click this icon to log out of the web configurator.

3.3.2 Navigation Panel

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

Table 4 Menu Summary

LINK	TAB	FUNCTION
Status		See the ZyXEL Device's general device information, system status, system resource usage, interface status, and wireless status.
Network		
Wireless LAN		Configure the wireless LAN card for wireless clients to connect to.
WAN	Internet Connection	Configure the WAN interface for Internet access.
	Advanced	Configure the WAN interface's multicast setting.
LAN		Configure the LAN interface to connect to the local network.
DHCP Server	General	Turn the DHCP server function on or off and configure the IP address pool.
	Client List	See the list of DHCP clients using the ZyXEL Device and the IP addresses assigned to them.
NAT	Port Forwarding	Allow users on the WAN to access local servers.
	Port Triggering	Allow computers on the LAN to dynamically take turns using services that use a range of ports.
DDNS		Dynamic DNS let you use a domain name with a dynamic WAN IP address.
Security		
Access Control	Access Control	Use firewall rules to allow or block applications. Use QoS to give higher priority to traffic from specific applications (like voice).
	Schedules	Configure schedules for applying firewall rules.
Content Filter		Block certain web features and URL keywords.

Table 4 Menu Summary (continued)

LINK	TAB	FUNCTION
Management		
UPnP		UPnP provides simple peer-to-peer network connectivity between devices.
Static Route		Use static routes to tell the ZyXEL Device about networks beyond the directly connected ones.
Maintenance		
System	General	Configure the ZyXEL Device's administrative settings.
	Time Setting	Configure the ZyXEL Device's time and date settings.
Logs		View log entries.
Tools	Firmware	Upload firmware to your ZyXEL Device
	Configuration	Backup and restore the ZyXEL Device configuration or reset the factory defaults.
	Restart	Reboot the ZyXEL Device.
	Box Access	Select which services can access the ZyXEL Device from the WAN.
	Diagnostic Tools	Check connectivity to a website or computer on the Internet, check the Internet connection's behavior, and resolve a domain name's IP address.
User Portal		The secure remote user portal lets remote users securely access LAN resources. Remote access to LAN computers is made secure through SSL or HTTPS. Configure permissions for authorized remote users to access specific network resources. In addition to accessing folders and files, remote users can be authorized to use remote desktop connections to remotely control LAN computers.
Admin Info		Configure the portal administrator's details.
User Info	User Info	Create and manage secure remote portal user accounts.
	Copy User Views	Copy a portal user's collection of accessible resources (view) to another user.
Manage Servers		Edit the list of LAN resources that secure remote portal users can access.
Manage Views		Edit each secure remote portal user's collection of accessible files and folders.
Desktop Links		Configure secure remote portal user access for using remote desktop connections to remotely control LAN computers. The remote users may use VNC (Virtual Network Computing) or RDP (Remote Desktop) protocol.

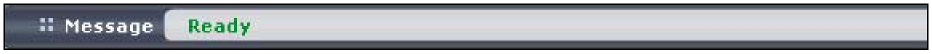
3.3.3 Main Window

The main window shows the screen you select in the menu. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See Chapter 4 on page 39 for more information about the **Status** screen.

3.3.4 Status Bar

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

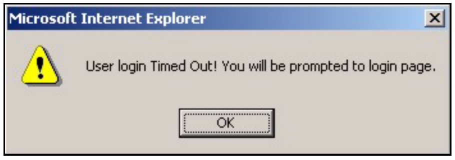


Ready

3.4 Login Timeout

By default, the web configurator automatically logs you out after 5 minutes (300 seconds) of inactivity. When this happens, a warning screen displays and you will be redirected to the login screen. Simply log into the web configurator again to continue your management tasks.

Figure 11 Timeout Message



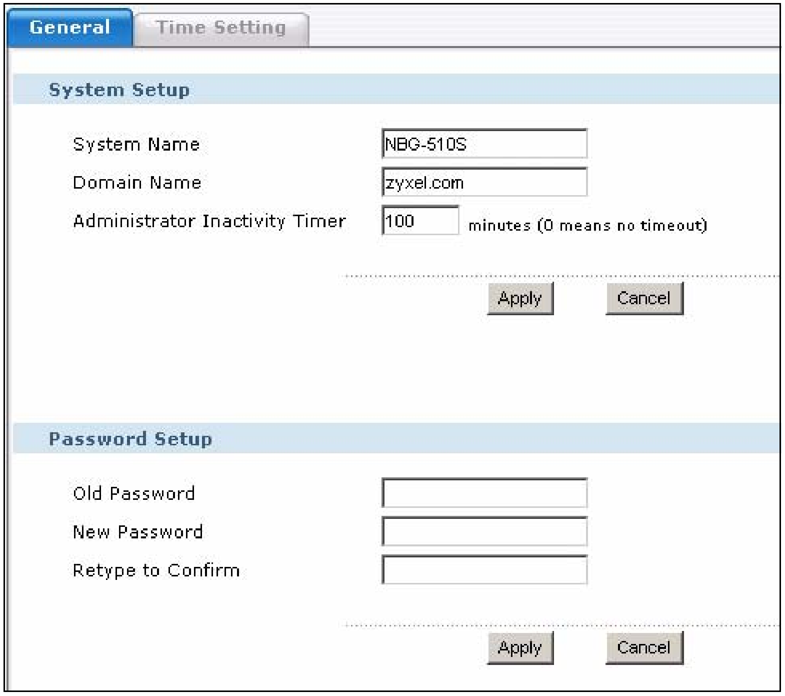
User login Timed Out! You will be prompted to login page.

3.4.1 Changing Login Timeout

To change the default login timeout period click **Maintenance > General** to display the following screen. In the **Administrator Inactivity Timer** field, specify a time (in minutes). Click **Apply** to save the changes. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).

You can also use this screen to change the administrator login password (refer to Section 3.5 on page 37).

Figure 12 Maintenance: Password



System Setup

System Name: NBG-510S

Domain Name: zyxel.com

Administrator Inactivity Timer: 100 minutes (0 means no timeout)

Password Setup

Old Password

New Password

Retype to Confirm

3.5 Changing Password

It is highly recommended that you change the default administrator login password in the Change Password screen after the first successful login. Click **Maintenance > General** to display the configuration screen (see Figure 12 on page 37).

In the **Old Password** field, enter the current password. Enter the new password (up to 31 printable ASCII characters with no spaces allowed) in the **New Password** and the **Re-type to Confirm** fields. Click **OK** to save the changes.

3.6 Device Reset

You can reset the ZyXEL Device using the **RESET** button. You need to reset your ZyXEL Device to the factory default settings if

- you have changed the default administrator login password and have now forgotten it.

or

- you want to start configuring the ZyXEL Device again from the default settings.

Resetting your device back to the defaults erases all your custom settings.

Follow the steps below to reset the ZyXEL Device using the **RESET** button panel.

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

2 Use a pointed object to press the **RESET** button in for five seconds and release it. The device restarts with the factory default settings (the default LAN IP address is **192.168.1.1** and the administrator login password is **1234**).

3 Wait until the device finished rebooting before accessing the web configurator again.

4

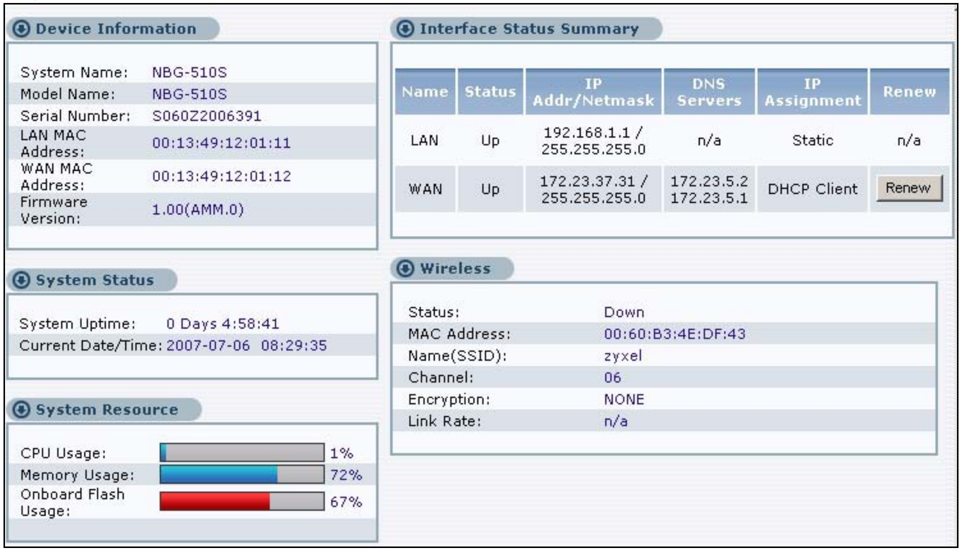
Status

This chapter explains the **Status** screen, which is the screen you see when you first log in to the ZyXEL Device.

4.1 Status Screen

Use the **Status** screen to look at the ZyXEL Device’s general device information, system status, system resource usage, licensed service status, and interface status. To access this screen, click **Status** in the navigation panel.

Figure 13 Status



Device Information

System Name:	NBG-510S
Model Name:	NBG-510S
Serial Number:	S060Z2006391
LAN MAC Address:	00:13:49:12:01:11
WAN MAC Address:	00:13:49:12:01:12
Firmware Version:	1.00(AMM.0)

System Status

System Uptime:	0 Days 4:58:41
Current Date/Time:	2007-07-06 08:29:35

System Resource

CPU Usage:	1%
Memory Usage:	72%
Onboard Flash Usage:	67%

Interface Status Summary

Name	Status	IP Addr/Netmask	DNS Servers	IP Assignment	Renew
LAN	Up	192.168.1.1 / 255.255.255.0	n/a	Static	n/a
WAN	Up	172.23.37.31 / 255.255.255.0	172.23.5.2 172.23.5.1	DHCP Client	Renew

Wireless

Status:	Down
MAC Address:	00:60:B3:4E:DF:43
Name(SSID):	zyxel
Channel:	06
Encryption:	NONE
Link Rate:	n/a

The following table describes the labels in this screen.

Table 5 Status

LABEL	DESCRIPTION
Device Information	
System Name	This field displays the name used to identify the ZyXEL Device on any network.
Model Name	This field displays the model name of this ZyXEL Device.
Serial Number	This field displays the serial number of this ZyXEL Device.
LAN MAC Address	This field displays the MAC address assigned to the LAN interface.

Table 5 Status (continued)

LABEL	DESCRIPTION
WAN MAC Address	This field displays the MAC address assigned to the WAN interface. If you configured the WAN interface’s MAC address (see , the configured MAC address displays here instead of the factory default.
Firmware Version	This field displays the version number of the firmware the ZyXEL Device is currently using.
System Status	
System Uptime	This field displays how long the ZyXEL Device has been running since it last restarted or was turned on.
Current Date/ Time	This field displays the current date and time in the ZyXEL Device. The format is yyyy-mm-dd hh:mm:ss.
System Resource	
CPU Usage	This field displays what percentage of the ZyXEL Device’s processing capability is currently being used.
Memory Usage	This field displays what percentage of the ZyXEL Device’s RAM is currently being used.
Onboard Flash Usage	This field displays what percentage of the ZyXEL Device’s onboard flash memory is currently being used.
Interface Status Summary	
Name	This field displays the name of each Ethernet interface.
Status	This field displays the current connection status of each interface.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. **Unavailable** displays if the interface did not receive an IP address and subnet mask via DHCP or the ZyXEL Device could not connect to ISP.
IP Assignment	This field displays how the interface gets its IP address. **Static** - This interface has a static IP address. **DHCP Client** - This interface gets its IP address from a DHCP server. **PPPOE** - This interface gets its IP address from a PPPoE server. **PPTP** - This interface gets its IP address from a PPTP server.
Renew	Click **Renew** to update the IP address for the interface. This field displays **n/a** if the interface has a static IP address.
Wireless	
Status	**Up** displays when the WLAN is enabled. **Down** displays when the WLAN is disabled.
MAC Address	This field displays the ZyXEL Device’s MAC address for wireless LAN connections.
Name (SSID)	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN.
Channel	This is the channel number used by the ZyXEL Device now.
Encryption	This field displays what type of encryption the ZyXEL Device is using for wireless LAN connections.
Link Rate	This displays the maximum transmission rate in Mb/s.

5

Setup Wizard

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

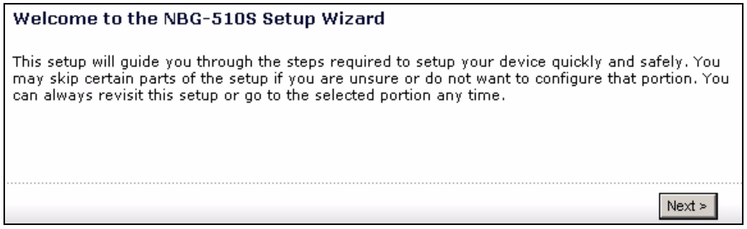
5.1 Wizard Setup Overview

Use the setup wizard screens to configure your Internet access settings.

Follow the steps to configure the wizard screens. Click **Next >** in each wizard screen to continue.

1 To display the setup wizard, click **Setup Wizard** in the initial main screen.

Figure 14 Wizard Welcome Screen

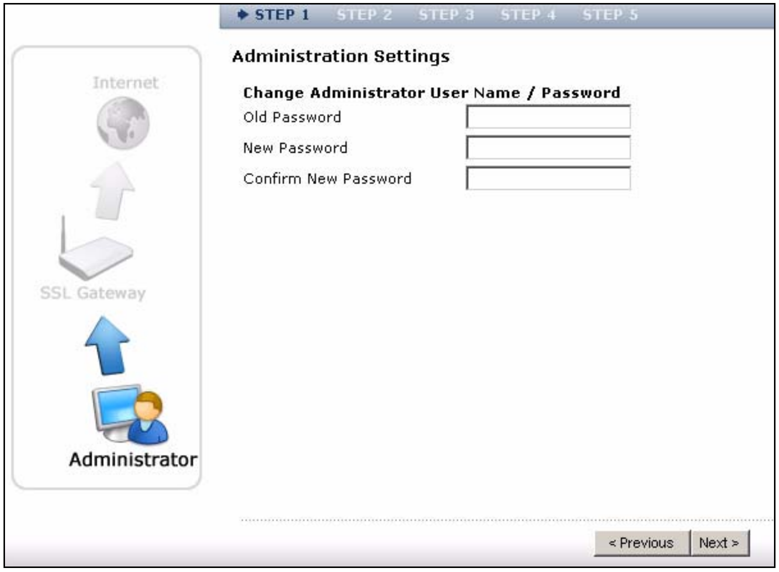


Welcome to the NBG-510S Setup Wizard

This setup will guide you through the steps required to setup your device quickly and safely. You may skip certain parts of the setup if you are unsure or do not want to configure that portion. You can always revisit this setup or go to the selected portion any time.

2 Create a new administrator password. Enter a unique password (up to 31 printable ASCII characters with no spaces allowed).

Figure 15 Wizard: Administration Settings



Administration Settings

Change Administrator User Name / Password

Old Password

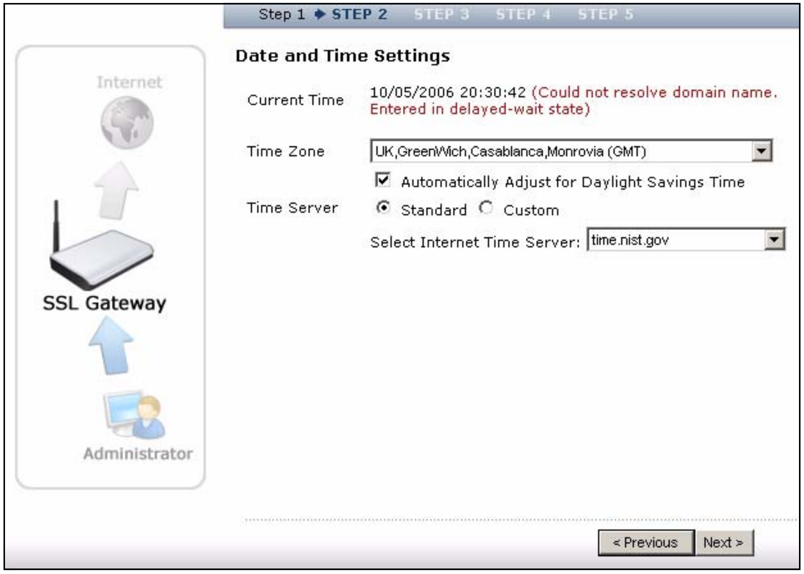
New Password

Confirm New Password

You cannot use the admin account to access network resources.

3 Select the ZyXEL Device's time zone and whether or not you use Daylight Saving Time. You can select a time server from the list or select **Custom** and enter another time server.

Figure 16 Wizard: Date and Time Settings



Date and Time Settings

Current Time 10/05/2006 20:30:42 (Could not resolve domain name. Entered in delayed-wait state)

Time Zone UK,GreenWich,Casablanca,Monrovia (GMT)

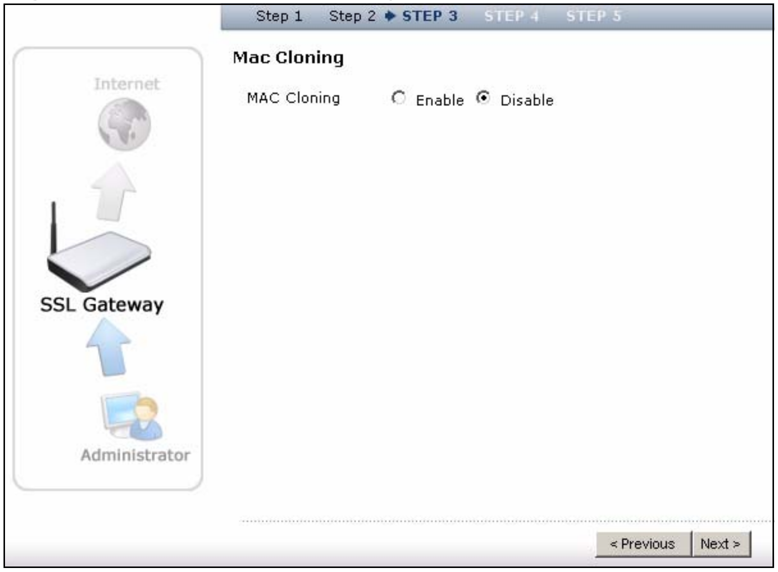
☑ Automatically Adjust for Daylight Savings Time

Time Server ● Standard ○ Custom

Select Internet Time Server: time.nist.gov

4 If the Internet Service Provider (ISP) uses your computer's hardware (MAC) address in authenticating your Internet access, enable MAC cloning and enter your computer's MAC address to have the ZyXEL Device use your computer's MAC address.

Figure 17 Wizard: MAC Cloning

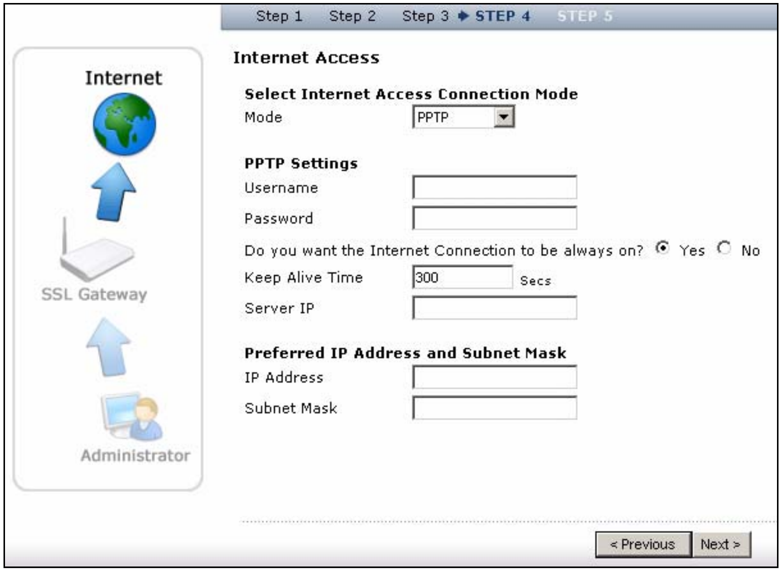


Mac Cloning

MAC Cloning ○ Enable ● Disable

5 Use **DHCP client** if your ISP did not give you any Internet access settings. Otherwise select the mode that your ISP uses and enter the Internet access settings exactly as the ISP provided them.

Figure 18 Wizard: Internet Access



Internet Access

Select Internet Access Connection Mode

Mode	PPTP

PPTP Settings

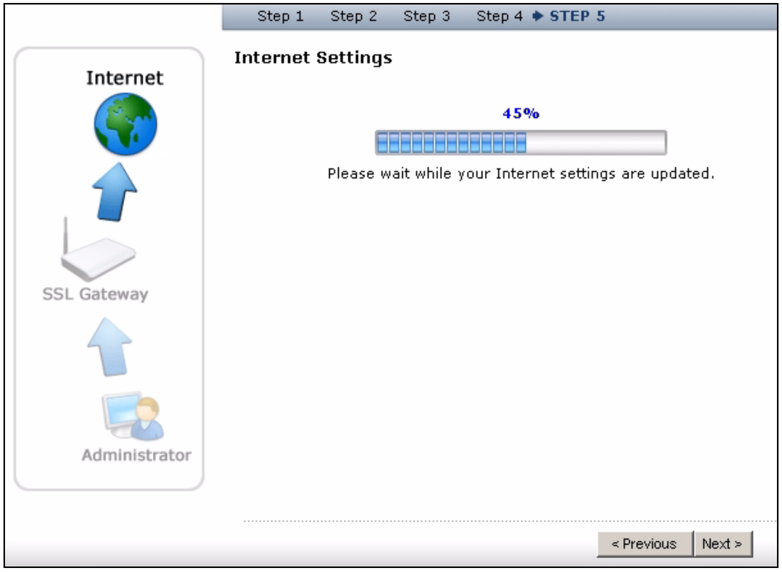
Username	
Password	
Do you want the Internet Connection to be always on?	● Yes ○ No
Keep Alive Time	300 Secs
Server IP	

Preferred IP Address and Subnet Mask

IP Address	
Subnet Mask	

6 Wait while the ZyXEL Device applies your Internet access settings. Then click **Next**.

Figure 19 Wizard: Applying Internet Settings

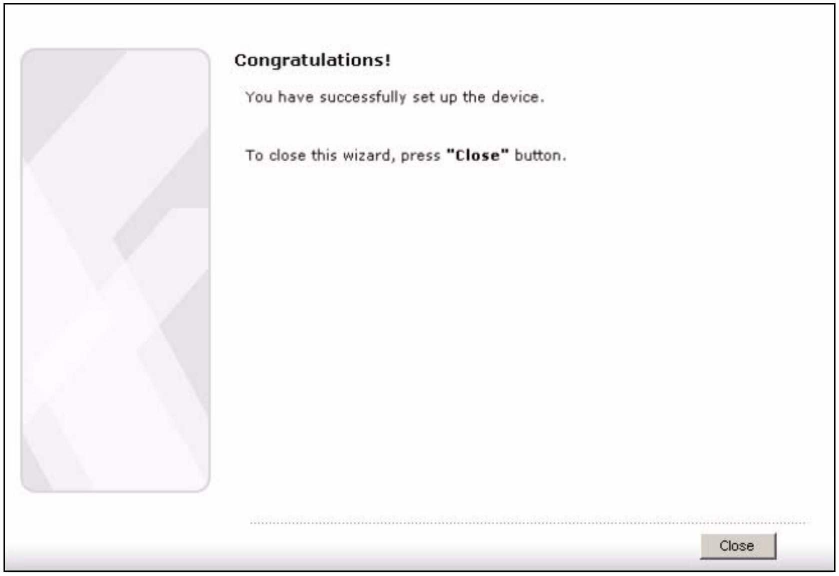


Internet Settings

Please wait while your Internet settings are updated.

7 Click **Close** in the final wizard screen.

Figure 20 Wizard: Applying Internet Settings



Congratulations!

You have successfully set up the device.

To close this wizard, press **"Close"** button.

6

Tutorials

6.1 Secure Remote Access Configuration Overview

Here is a brief summary of how to configure secure remote access (user portal) screens to allow remote users to securely access and upload shared files on the computers on your network. See the Quick Start Guide for an example.

6.1.1 Configure Secure Remote Access

This example is for a Windows computer.

1. Use Windows Explorer to share out the computer folders that the remote users can access.
2. Open your Internet browser (Internet Explorer for example) and log into the ZyXEL Device (see Section 3.2 on page 31 for details). Use the **User Portal** > **User Info** screens (Chapter 20 on page 135) to create user names and passwords for the remote users.
3. Use the **User Portal** > **Manage Views** screens (Chapter 23 on page 143) to configure what files each remote user can access on the LAN.
   - Configure folder categories and references to allow a remote user upload files.
   - You can configure categories and references for the guest account.
   - **User Portal** > **User Info** > **Copy User Views** can help speed up the process if you are configuring multiple accounts with similar views.

6.1.2 Test Secure Remote Access

1. Open another browser window (Internet Explorer for example) and log into the ZyXEL Device using a secure remote access account’s username and password (see Chapter 25 on page 155).
2. You see a screen with folders of the files you can access. Browse through the screens and make sure you can view and download files. Use the **Folders** screens to upload files.

6.2 Secure Remote Desktop Connections

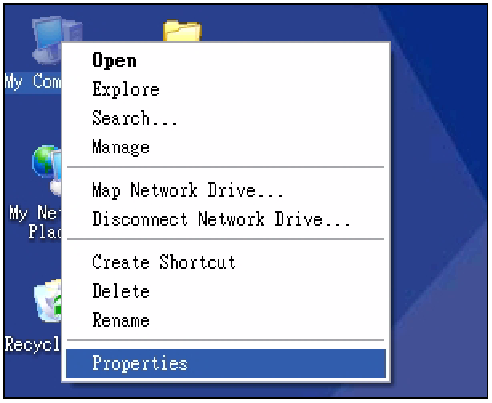
This example shows how to use Windows Remote Desktop Connection software (included in Windows XP) with the secure remote access portal for secure remote desktop connections for managing a computer on your network.

6.2.1 Configure the Computer to be Managed

Here is how to configure Windows Remote Desktop Connection on the LAN computer that you want to manage (a Windows XP computer in this example).

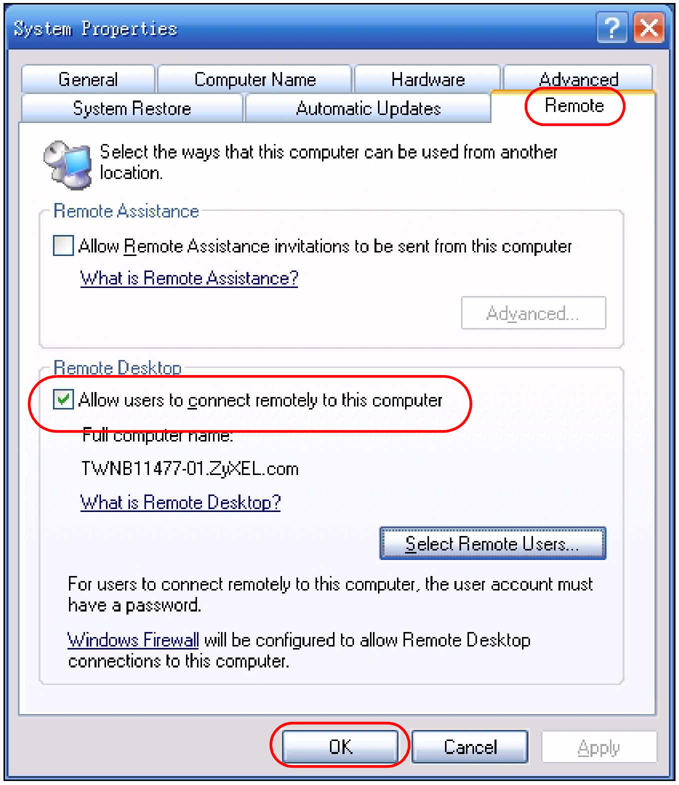
1 From your computer desktop, right-click My Computer and select Properties.

Figure 21 My Computer



2 Click the **Remote** tab, select **Allow users to connect remotely to this computer**, and click **OK**. This allows any of the computer’s administrator user accounts to remotely control the computer. If you want to manage which accounts can remotely control the computer, click **Select Remote Users**.

Figure 22 My Computer > Properties > Remote



Select the ways that this computer can be used from another location.

Remote Assistance

□ Allow Remote Assistance invitations to be sent from this computer

What is Remote Assistance?

Remote Desktop

☑ Allow users to connect remotely to this computer

Full computer name:

TWNB11477-01.ZyXEL.com

What is Remote Desktop?

For users to connect remotely to this computer, the user account must have a password.

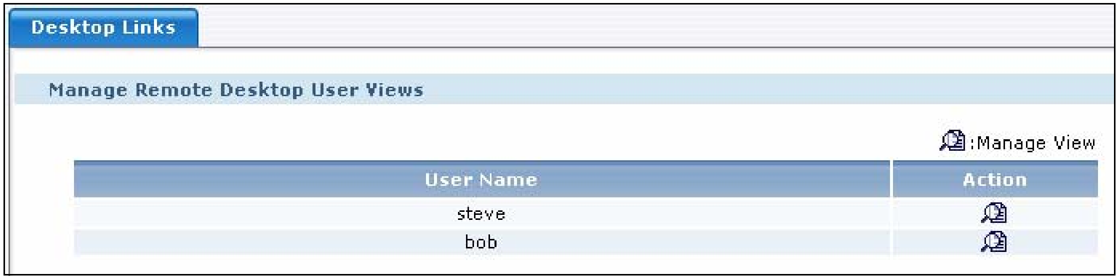
Windows Firewall will be configured to allow Remote Desktop connections to this computer.

6.2.2 Configure the ZyXEL Device

You configure policies for the LAN computers to be managed in the ZyXEL Device's **User Portal** > **Desktop Links** screens.

1 Log into the ZyXEL Device and click **User Portal > Desktop Links**. Click **Manage View** for the user you want to let control the LAN computer (**bob** in this example).

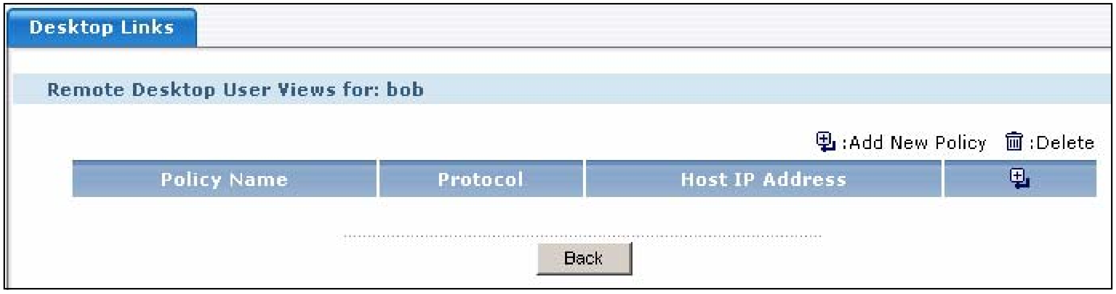
Figure 23 User Portal > Desktop Links



User Name	Action
steve	
bob	

2 Click the **Add New Policy** icon.

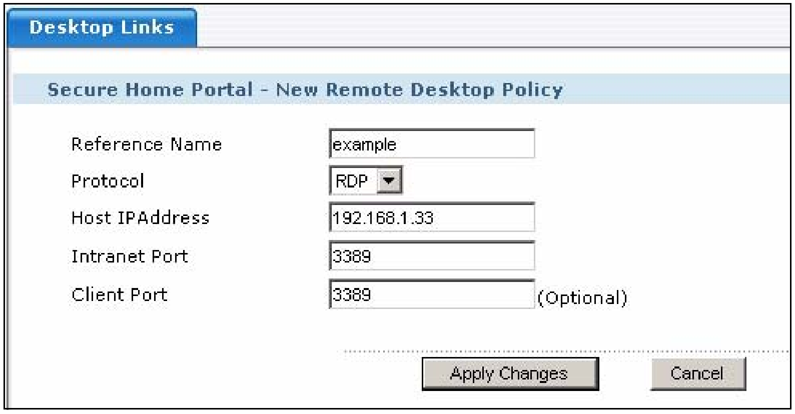
Figure 24 User Portal > Desktop Links > Manage View



Policy Name	Protocol	Host IP Address	

3 Configure the policy. The policy name (reference name) here is **example**. Windows Remote Desktop Connection uses RDP protocol. The computer is at LAN IP address 192.168.1.33. This example uses the default port settings (see Table 56 on page 153 for details about the port settings). Click **Apply Changes**.

Figure 25 User Portal > Desktop Links > Manage View > Add

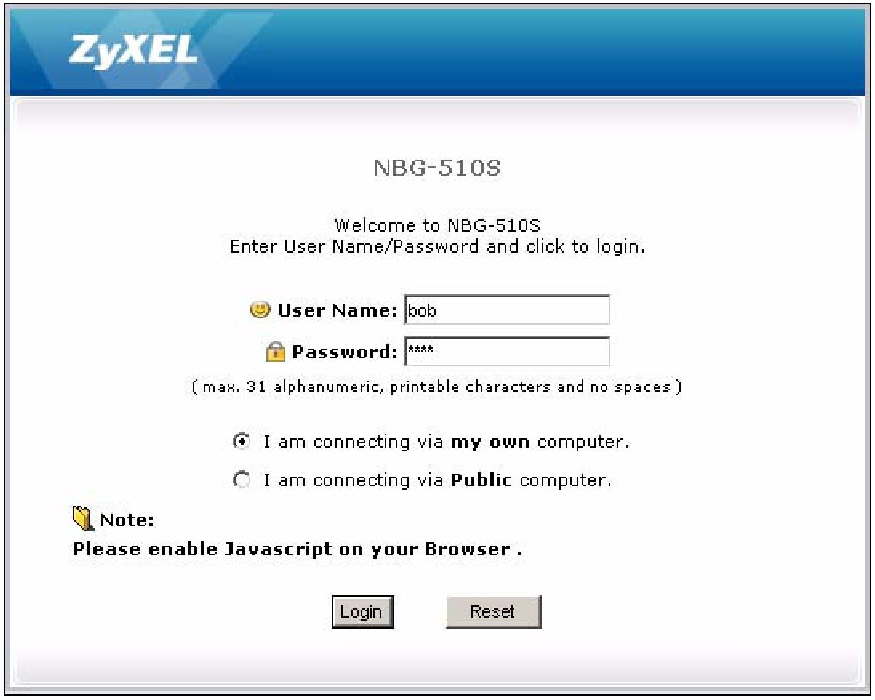


Reference Name	example
Protocol	RDP
Host IPAddress	192.168.1.33
Intranet Port	3389
Client Port	3389 (Optional)

6.2.3 Use the Secure Remote Desktop Connection

1 Open a browser window from a remote computer and log into the secure remote access screens using the bob account. Click **OK**, **Yes**, or **Run** in any security alert or certificate screens that display. See Section 25.2 on page 155 for more login details.

Figure 26 Secure Remote Access Login



NBG-510S

Welcome to NBG-510S
Enter User Name/Password and click to login.

User Name: bob

Password: ****

(max. 31 alphanumeric, printable characters and no spaces)

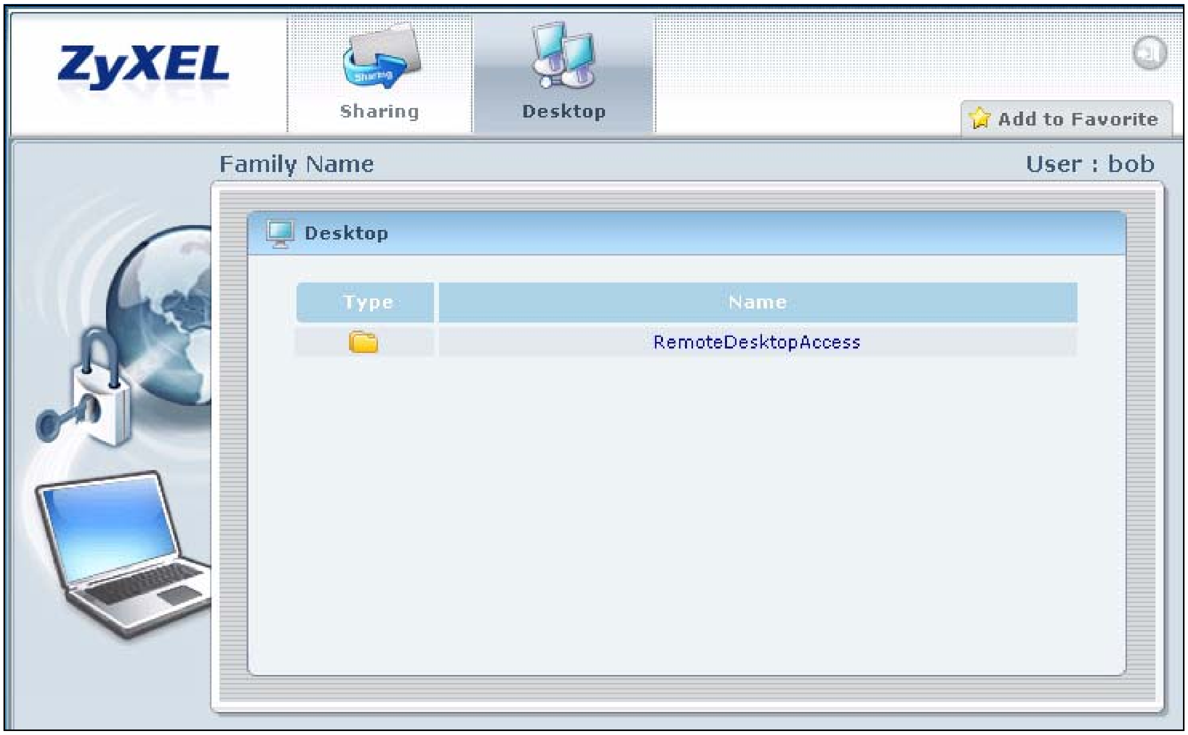
● I am connecting via **my own** computer.

○ I am connecting via **Public** computer.

Note:
Please enable Javascript on your Browser .

2 Click **Desktop** to open the following screen. Click **RemoteDesktopAccess** to open a screen with links for the LAN computers you can manage.

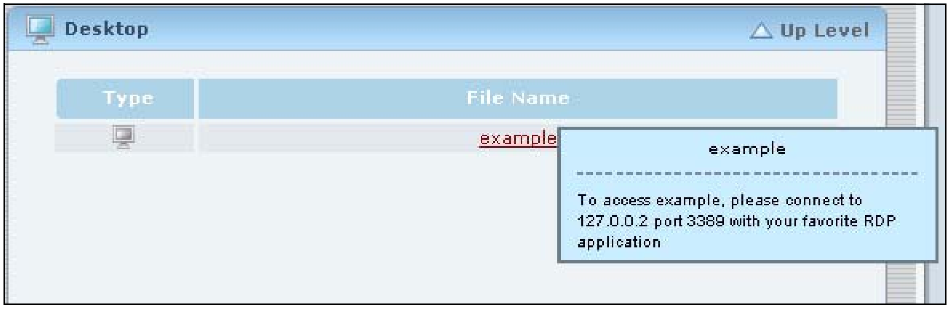
Figure 27 Desktop



Type	Name
🗀	RemoteDesktopAccess

3 Roll your mouse over the **(example**) link to display the loopback IP address and port number as shown next. The following steps show how to enter the loopback IP address and port number in the remote computer’s Windows Remote Desktop Connection software to use in communicating with the LAN computer you are managing.

Figure 28 Desktop Links



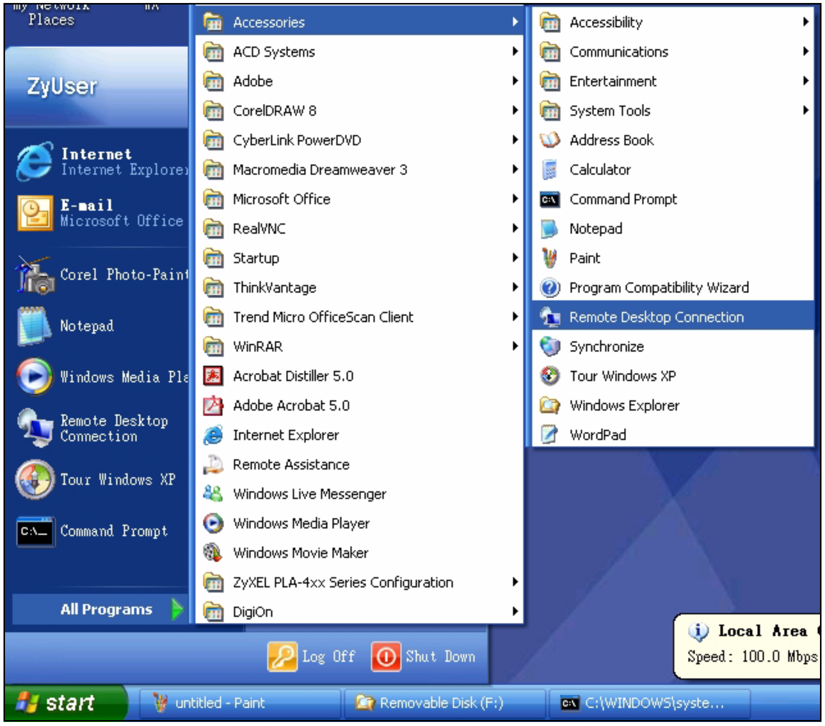
Type	File Name
🖥	example

example

To access example, please connect to 127.0.0.2 port 3389 with your favorite RDP application

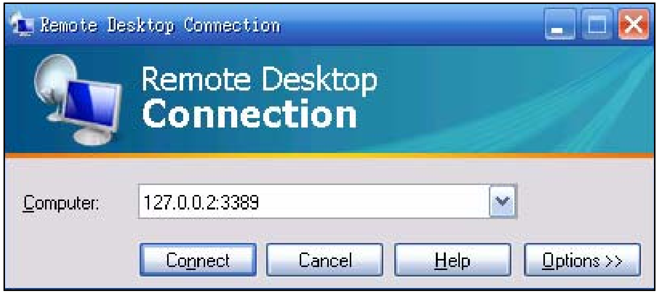
4 Stay logged into the ZyXEL Device’s secure remote access portal. In Windows, click **Start** > **Programs** > **Accessories** > **Remote Desktop Connection**.

Figure 29 Start > Programs > Accessories > Remote Desktop Connection



5 Enter the loopback IP address and port number from the desktop link (127.0.0.2 and 3389 in this example) separated by a colon, as shown here. Then click **OK**.

Figure 30 Entering the IP Address and Port Number



Computer: 127.0.0.2:3389

6 A login screen opens for the LAN computer. After you log in using one of the LAN computer's administrator accounts, you can manage the LAN computer.

- Stay logged into the ZyXEL Device's secure remote access portal.
- Make sure the remote computer is not running a remote desktop server on the same port number.

6.3 Wireless Tutorial

The following sections give examples of how to set up the ZyXEL Device and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through the ZyXEL Device wirelessly. See Chapter 7 on page 61 for more on the ZyXEL Device's wireless LAN configuration. See the **Quick Start Guide** for an example of configuring secure remote access.

6.4 Example Parameters

SSID	SSID_Example3
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
802.11 mode	IEEE 802.11b/g

In this chapter, the ZyXEL Device is also referred to as an access point (AP). A computer with a wireless network card or USB/PCI adapter is referred to here as a “wireless client”.

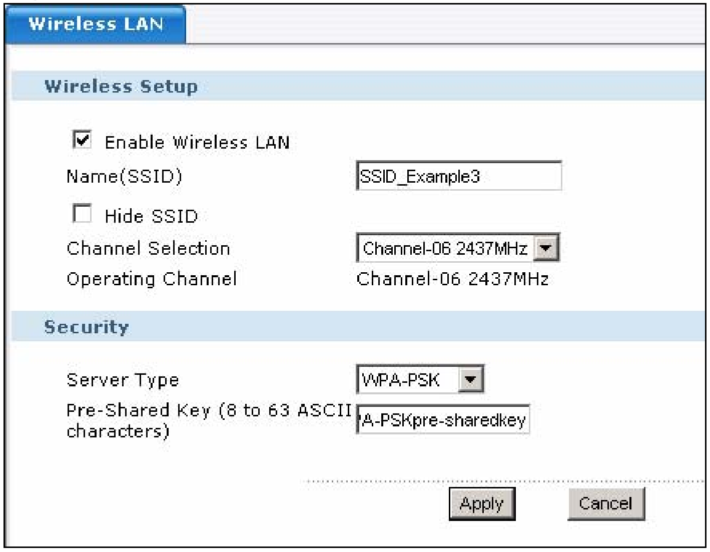
This chapter uses the M-302 utility screens as an example for the wireless client. The screens may vary for different models.

6.5 Configuring the ZyXEL Device

Follow the steps below to configure the wireless settings on your ZyXEL Device.

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

Figure 31 Network > Wireless LAN



Wireless Setup

☑ Enable Wireless LAN

Name(SSID) SSID_Example3

□ Hide SSID

Channel Selection Channel-06 2437MHz

Operating Channel Channel-06 2437MHz

Security

Server Type WPA-PSK

Pre-Shared Key (8 to 63 ASCII characters) 'A-PSKpre-sharedkey

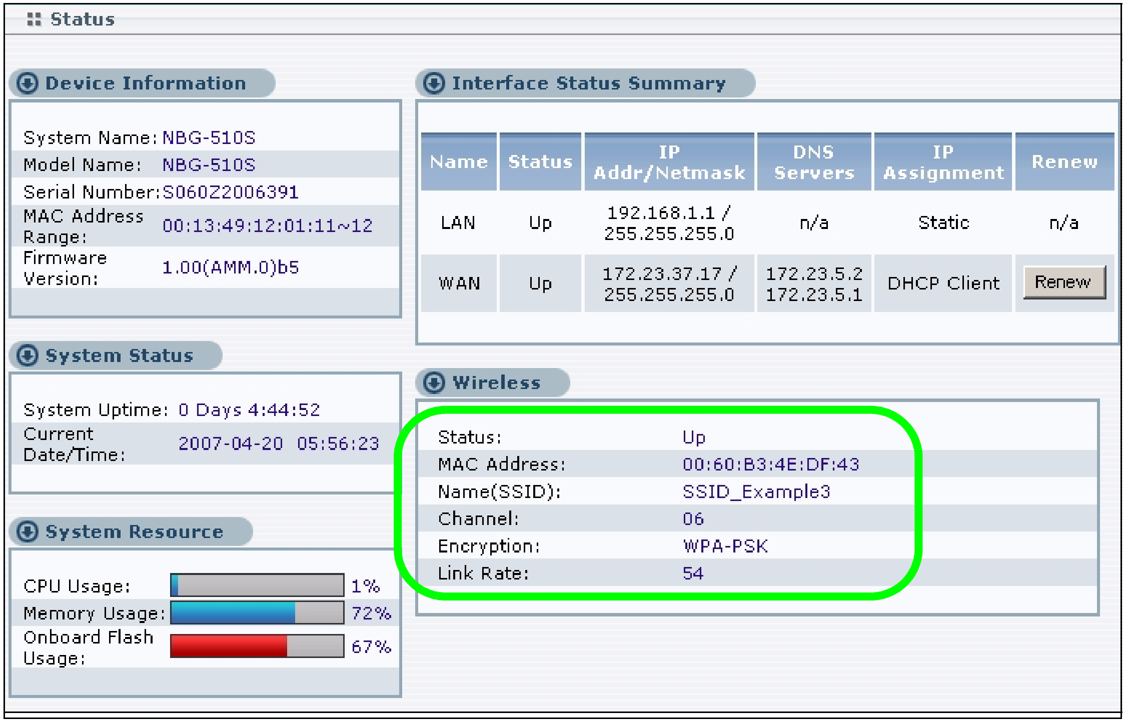
2 Make sure the **Enable Wireless LAN** check box is selected.

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

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

5 Open the **Status** screen. Under **Wireless**, verify that the wireless **Status** is **Up**, the **Name(SSID)** is **SSID_Example3**, and the **Encryption** is **WPA-PSK**.

Figure 32 Status: Wireless Settings Example



Status

Device Information

System Name: NBG-510S
Model Name: NBG-510S
Serial Number: S060Z2006391
MAC Address Range: 00:13:49:12:01:11~12
Firmware Version: 1.00(AMM.0)b5

Interface Status Summary

Name	Status	IP Addr/Netmask	DNS Servers	IP Assignment	Renew
LAN	Up	192.168.1.1 / 255.255.255.0	n/a	Static	n/a
WAN	Up	172.23.37.17 / 255.255.255.0	172.23.5.2 172.23.5.1	DHCP Client	Renew

System Status

System Uptime: 0 Days 4:44:52
Current Date/Time: 2007-04-20 05:56:23

Wireless

Status: Up
MAC Address: 00:60:B3:4E:DF:43
Name(SSID): SSID_Example3
Channel: 06
Encryption: WPA-PSK
Link Rate: 54

System Resource

CPU Usage: 1%
Memory Usage: 72%
Onboard Flash Usage: 67%

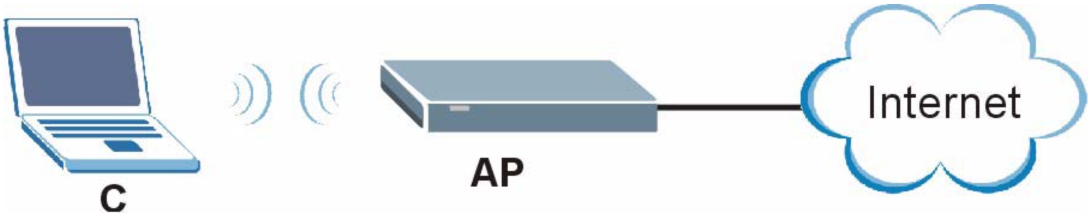
6 Now that you have configured the ZyXEL Device’s wireless settings, continue with the next section to configure wireless clients to connect to the ZyXEL Device.

6.6 Configuring the Wireless Client

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

6.6.1 Connecting to a Wireless LAN

The following sections show you how to join a ZyXEL wireless client (not included) to the wireless network. This example uses the ZyXEL utility that comes with a ZyXEL wireless client. In the following diagram, the wireless client is labelled **C** and the access point is labelled **AP**.



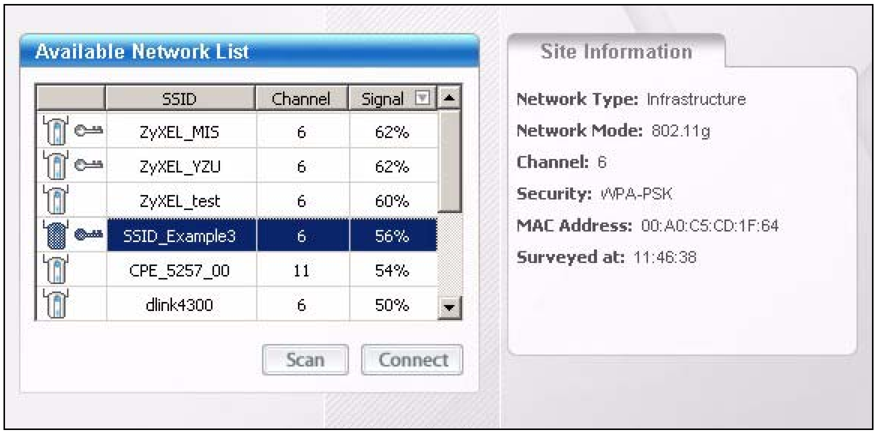
There are three ways to connect the client to an access point.

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

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

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

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



Available Network List

	SSID	Channel	Signal
	ZyXEL_MIS	6	62%
	ZyXEL_YZU	6	62%
	ZyXEL_test	6	60%
	SSID_Example3	6	56%
	CPE_5257_00	11	54%
	dlink4300	6	50%

Site Information

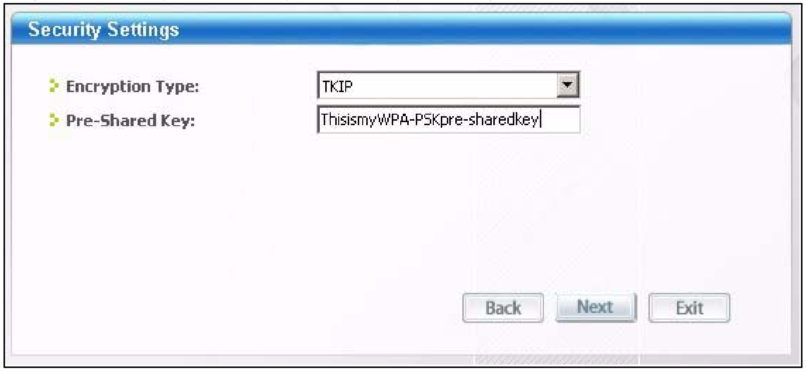
Network Type: Infrastructure
Network Mode: 802.11g
Channel: 6
Security: WPA-PSK
MAC Address: 00:A0:C5:CD:1F:64
Surveyed at: 11:46:38

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

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

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

Figure 33 ZyXEL Utility: Security Settings

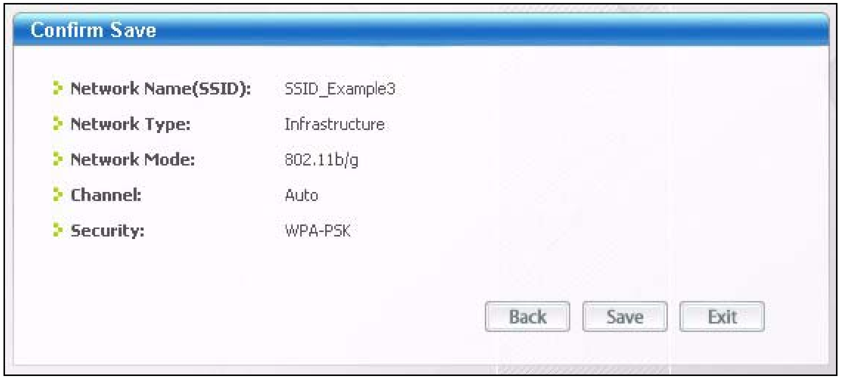


Security Settings

Encryption Type: TKIP
Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

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

Figure 34 ZyXEL Utility: Confirm Save

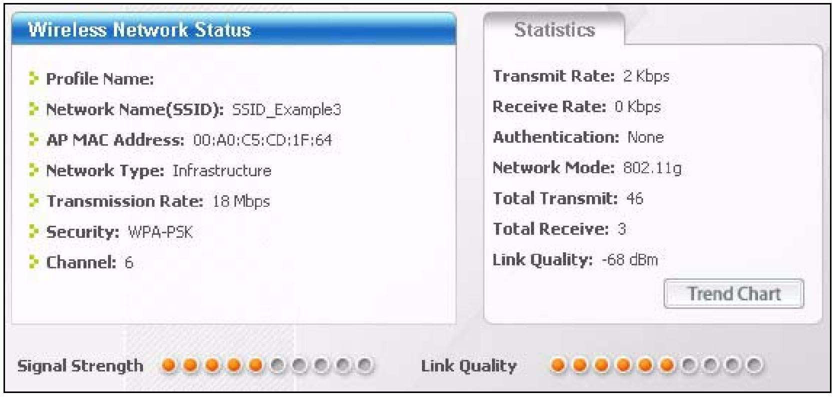


Confirm Save

- Network Name(SSID): SSID_Example3
- Network Type: Infrastructure
- Network Mode: 802.11b/g
- Channel: Auto
- Security: WPA-PSK

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

Figure 35 ZyXEL Utility: Link Info



Wireless Network Status

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

Statistics

Transmit Rate: 2 Kbps
Receive Rate: 0 Kbps
Authentication: None
Network Mode: 802.11g
Total Transmit: 46
Total Receive: 3
Link Quality: -68 dBm

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

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

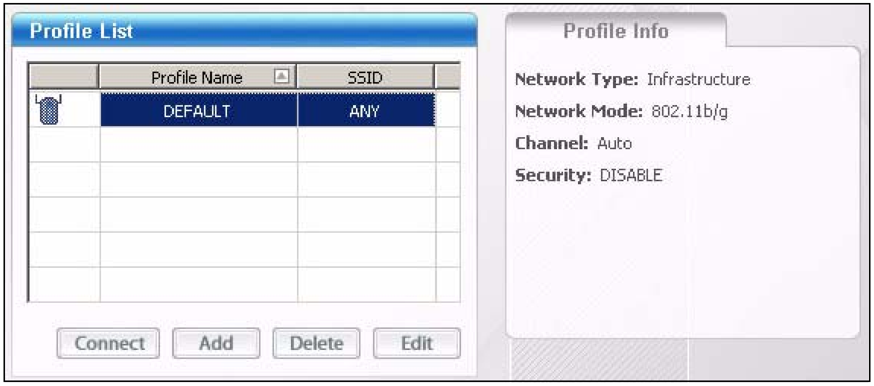
6.6.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the wireless client. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

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

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

Figure 36 ZyXEL Utility: Profile



Profile List

	Profile Name	SSID
	DEFAULT	ANY

Profile Info

Network Type: Infrastructure

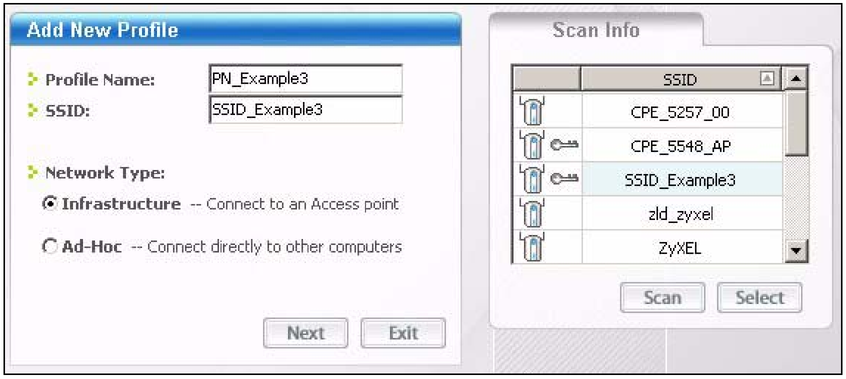
Network Mode: 802.11b/g

Channel: Auto

Security: DISABLE

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

Figure 37 ZyXEL Utility: Add New Profile



Add New Profile

Profile Name: PN_Example3

SSID: SSID_Example3

Network Type:

● Infrastructure -- Connect to an Access point

○ Ad-Hoc -- Connect directly to other computers

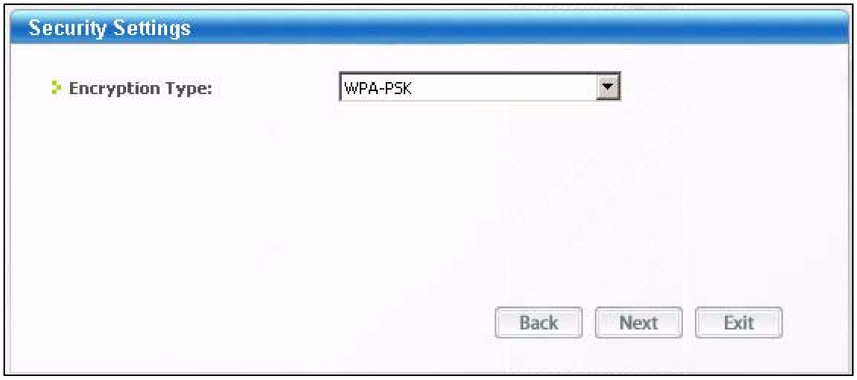
Scan Info

	SSID
	CPE_5257_00
	CPE_5548_AP
	SSID_Example3
	zld_zyxel
	ZyXEL

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

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

Figure 38 ZyXEL Utility: Profile Security

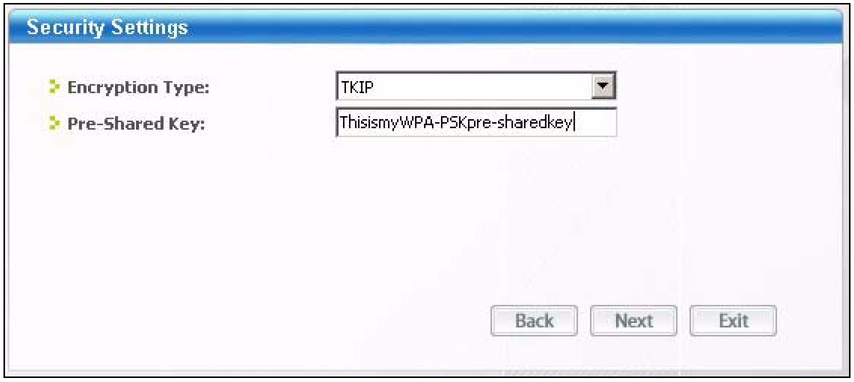


Security Settings

Encryption Type: WPA-PSK

5 This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.

Figure 39 ZyXEL Utility: Profile Encryption

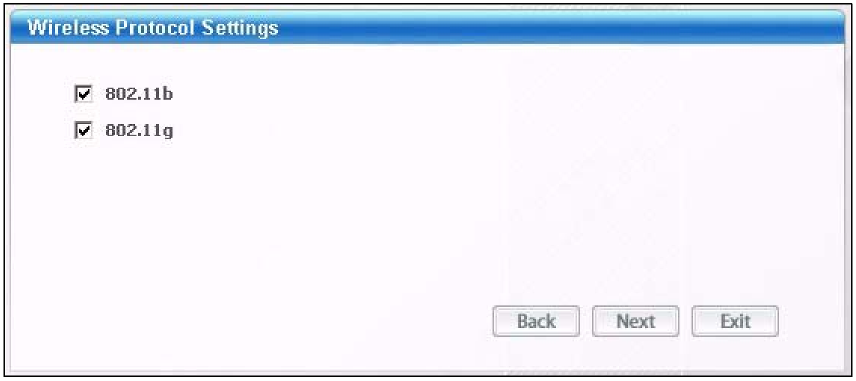


Security Settings

- Encryption Type: TKIP
- Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

6 In the next screen, leave both boxes checked.

Figure 40 Profile: Wireless Protocol Settings.



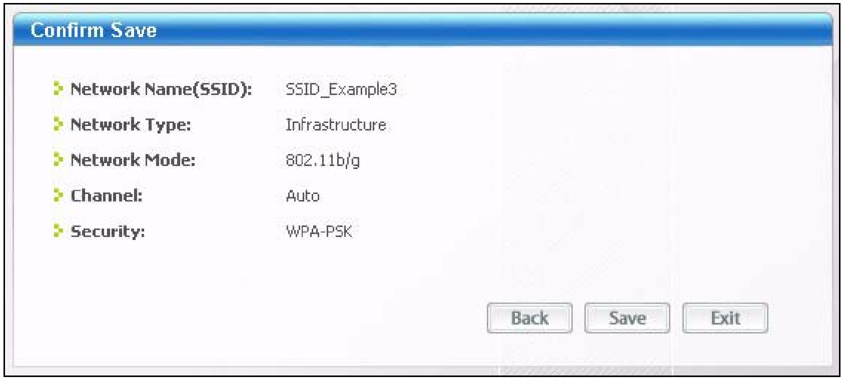
Wireless Protocol Settings

☑ 802.11b

☑ 802.11g

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

Figure 41 Profile: Confirm Save



Confirm Save

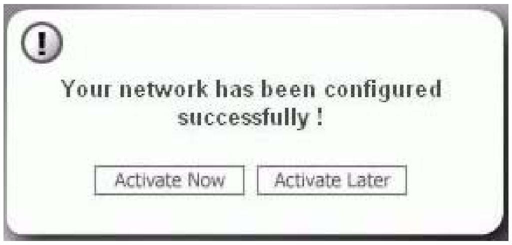
- Network Name(SSID): SSID_Example3
- Network Type: Infrastructure
- Network Mode: 802.11b/g
- Channel: Auto
- Security: WPA-PSK

8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

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

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

Figure 42 Profile: Activate



Your network has been configured successfully !

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

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

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

PART II
Network

7

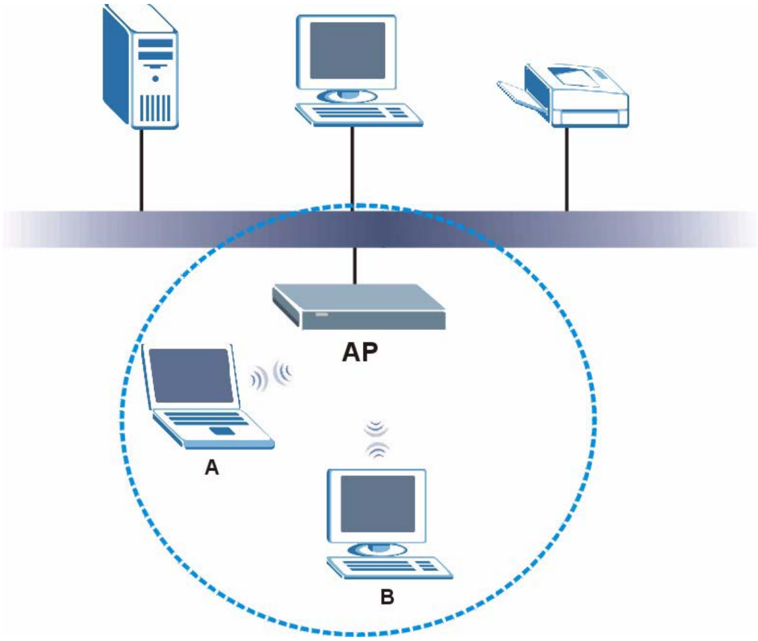
Wireless LAN

This chapter discusses how to configure the wireless network settings in your ZyXEL Device. See Appendix C on page 181 for more detailed information about wireless networks.

7.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 43 Example of a Wireless Network



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

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.
  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.
  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

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

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

7.2 Wireless Security Overview

The following table shows the relative strengths of common types of wireless security. Use the strongest security that every wireless client in the wireless network supports.

Table 6 Wireless Security Types

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

If you have a RADIUS server, you can use WPA or WPA2 so users have to log into the wireless network before using it. This is called user authentication. RADIUS servers are more common in businesses (WPA and WPA2 are also called the enterprise version of WPA).

If you do not have a RADIUS server, the strongest wireless security you can use is WPA2-PSK (WPA2-PSK and WPA-PSK are also known as the personal version of WPA).

It is recommended that wireless networks use WPA-PSK, WPA, or stronger security. WEP is better than no security, but it is still possible for unauthorized 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 wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA Compatible** option in the ZyXEL Device.

7.2.1 SSID

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

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

7.2.2 User Authentication

You can use WPA or WPA2 to have a RADIUS server authenticate users before they can use the wireless network. You store each user's user name and password on the RADIUS server. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

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

7.2.3 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.

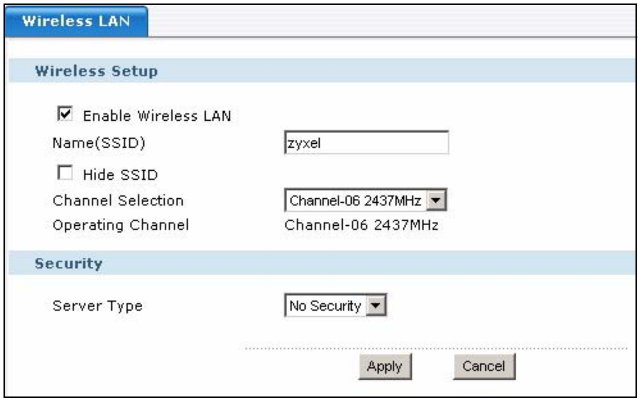
Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

7.3 Wireless LAN Screen

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

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

Figure 44 Network > Wireless LAN



☑ Enable Wireless LAN

Name(SSID) zyxel

□ Hide SSID

Channel Selection Channel-06 2437MHz

Operating Channel Channel-06 2437MHz

Server Type No Security

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

Table 7 Network > Wireless LAN

LABEL	DESCRIPTION
Enable a Wireless LAN	Click the check box to activate wireless LAN.
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	The range of radio frequencies used by IEEE 802.1 wireless devices is called a channel. Select a channel ID that is not already in use by a neighboring device. Select a channel from the drop-down list box. The options vary depending on whether you are using A or B/G frequency band and the country you are in. Select **Auto Channel** to have the ZyXEL Device automatically find a suitable channel to use.
Operating Channel	This displays the channel the ZyXEL Device is currently using.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

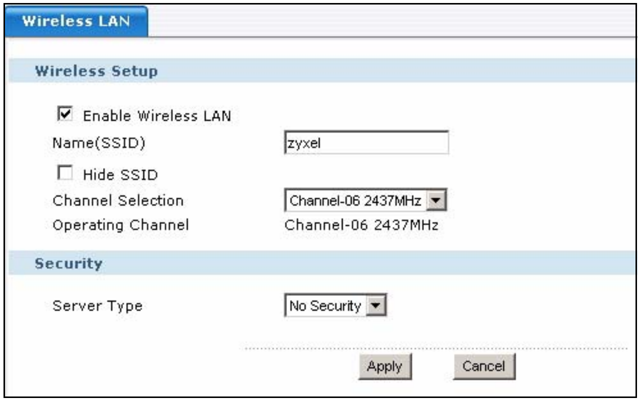
See the rest of this chapter for information on the other labels in this screen.

7.3.1 No Security

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

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

Figure 45 Network > Wireless LAN: No Security



☑ Enable Wireless LAN

Name(SSID): zyxel

□ Hide SSID

Channel Selection: Channel-06 2437MHz

Operating Channel: Channel-06 2437MHz

Server Type: No Security

The following table describes the labels in this screen.

Table 8 Network > Wireless LAN: No Security

LABEL	DESCRIPTION
Server Type	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

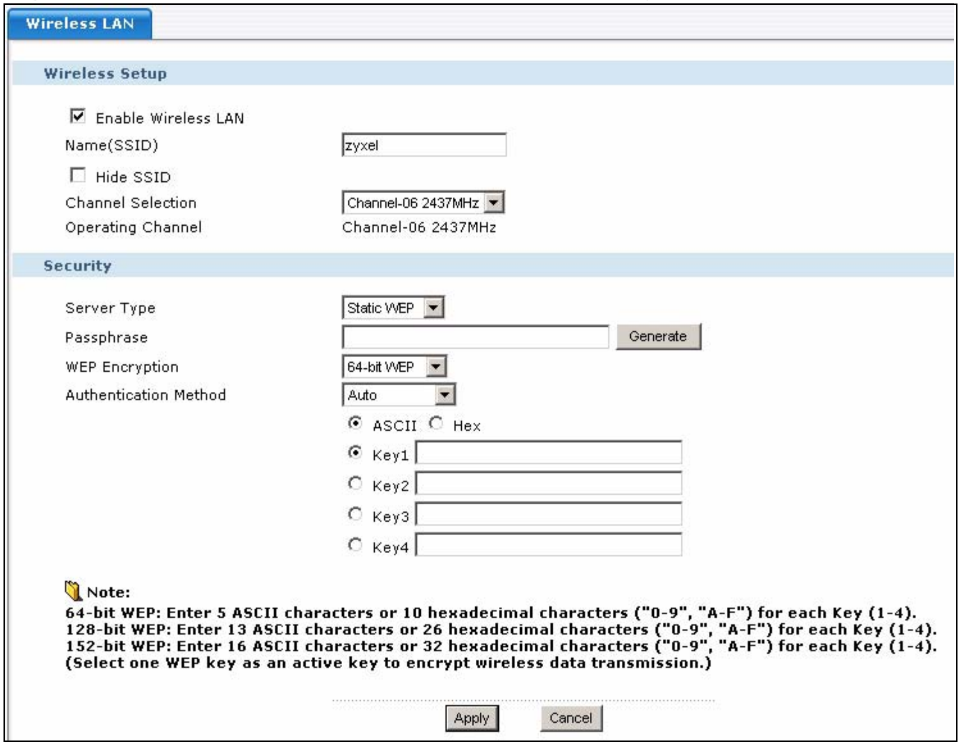
7.3.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key. Your ZyXEL Device allows you to configure up to four WEP keys but only one key can be enabled at any one time.

It is recommended that wireless networks use WPA-PSK, WPA, or stronger security. WEP is better than no security, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

In order to configure and enable WEP encryption; click **Network** > **Wireless LAN** to display the **General** screen. Select **Static WEP** as the **Server Type**.

Figure 46 Network > Wireless LAN: Static WEP Encryption



Wireless Setup

☑ Enable Wireless LAN

Name(SSID): zyxel

□ Hide SSID

Channel Selection: Channel-06 2437MHz

Operating Channel: Channel-06 2437MHz

Security

Server Type: Static WEP

Passphrase:

WEP Encryption: 64-bit WEP

Authentication Method: Auto

● ASCII ○ Hex

● Key1

○ Key2

○ Key3

○ Key4

Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

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

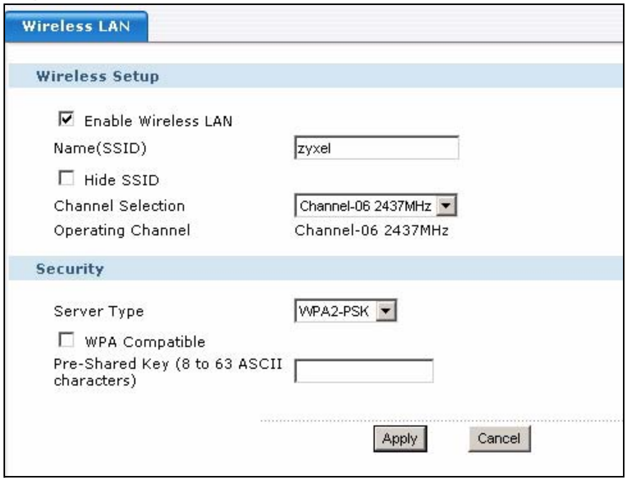
Table 9 Network > Wireless LAN: Static WEP Encryption

LABEL	DESCRIPTION
Passphrase	Enter a passphrase (password phrase) of up to 32 printable characters and click **Generate**. The ZyXEL Device automatically generates four different WEP keys and displays them in the **Key** fields below.
WEP Encryption	Select **64-bit WEP**, **128-bit WEP**, or **152-bit WEP** to enable data encryption.
Authentication Method	This field is activated when you select **64-bit WEP** or **128-bit WEP** in the **WEP Encryption** field. Select **Auto**, **Open System** or **Shared Key** from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you chose **152-bit WEP**, then enter 16 ASCII characters or 232 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7.3.3 WPA-PSK/WPA2-PSK

Click **Network** > **Wireless LAN** to display the following screen.

Figure 47 Network > Wireless LAN: WPA-PSK/WPA2-PSK



Wireless Setup

☑ Enable Wireless LAN

Name(SSID): zyxel

□ Hide SSID

Channel Selection: Channel-06 2437MHz

Operating Channel: Channel-06 2437MHz

Security

Server Type: WPA2-PSK

□ WPA Compatible

Pre-Shared Key (8 to 63 ASCII characters):

The following table describes the labels in this screen.

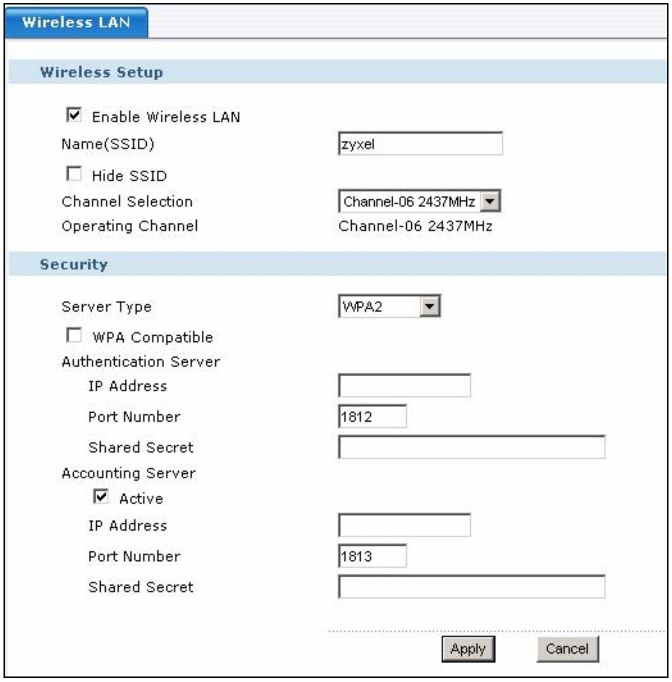
Table 10 Network > Wireless LAN: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Server Type** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for **WPA/WPA2** and **WPA-PSK/WPA2-PSK** are the same. The only difference between the two is that **WPA-PSK/WPA2-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). A minimum of 20 characters consisting of letters, upper and lower case, numbers and symbols is recommended.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7.3.4 WPA/WPA2

Click **Network** > **Wireless LAN** to display the following screen.

Figure 48 Network > Wireless LAN: WPA/WPA2



Wireless LAN

Wireless Setup

☑ Enable Wireless LAN

Name(SSID): zyxel

☐ Hide SSID

Channel Selection: Channel-06 2437MHz

Operating Channel: Channel-06 2437MHz

Security

Server Type: WPA2

☐ WPA Compatible

Authentication Server

IP Address:

Port Number: 1812

Shared Secret:

Accounting Server

☑ Active

IP Address:

Port Number: 1813

Shared Secret:

The following table describes the labels in this screen.

Table 11 Network > Wireless LAN: WPA/WPA2

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Server Type** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 64 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.
Accounting Server	
Active	Select this option to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8

WAN

This chapter shows you how to configure the WAN screens on the ZyXEL Device for Internet access.

8.1 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. The ZyXEL Device can get an IP address automatically if your ISP gives them out. If you have a static (fixed) IP address from the ISP, you can manually assign it to the ZyXEL Device’s WAN port.

8.2 DNS Server Addresses

A DNS (Domain Name System) server maps domain names (like www.zyxel.com) to their corresponding IP addresses (204.217.0.2 in the case of www.zyxel.com). This lets you use domain names to access web sites without having to know their IP addresses. The ZyXEL Device can receive the IP address of a DNS server automatically (along with the ZyXEL Device’s own IP address). You can also manually enter a DNS server IP address in the ZyXEL Device.

8.3 WAN MAC Address

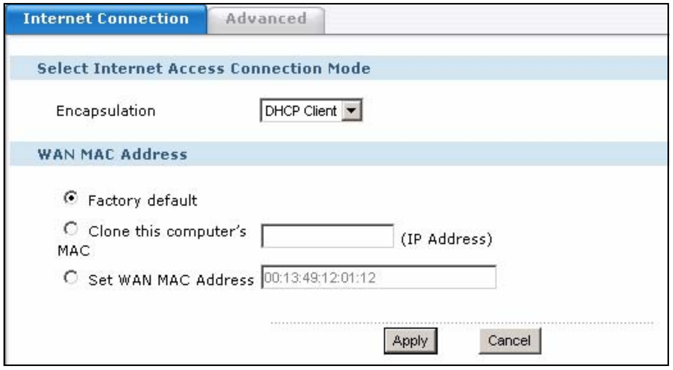
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

If the Internet Service Provider (ISP) uses your computer’s MAC address in authenticating your Internet access, have the ZyXEL Device use your computer’s MAC address. Once it is successfully configured, the address will be copied to the ZyXEL Device’s configuration file. It will not change unless you change the setting or upload a different configuration file. It is recommended that you change the MAC address prior to connecting the WAN port.

8.4 WAN DHCP Client Encapsulation

Select **DHCP Client** encapsulation in the **Network > WAN > Internet Connection** screen if your ISP did not assign you a fixed IP address.

Figure 49 Network > WAN > Internet Connection: DHCP Client Encapsulation



Select Internet Access Connection Mode

Encapsulation: DHCP Client

WAN MAC Address

● Factory default

○ Clone this computer's MAC (IP Address)

○ Set WAN MAC Address 00:13:49:12:01:12

The following table describes the labels in this screen.

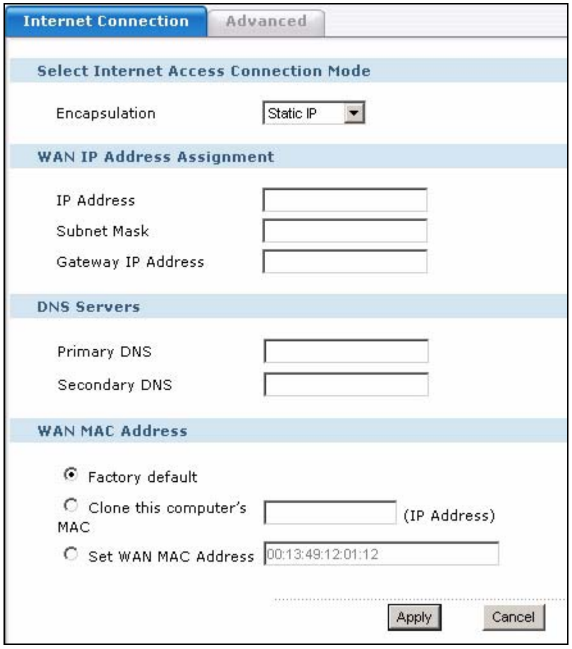
Table 12 Network > WAN > Internet Connection: DHCP Client Encapsulation

LABEL	DESCRIPTION
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the ZyXEL Device's MAC address, cloning a computer's IP address, or manually entering a MAC address.
Factory default	Select this option to use the factory assigned default MAC address.
Clone this computer's MAC	Select this option and enter the IP address of the computer on the LAN that is used for Internet access. Enter the IP address in dotted decimal notation, for example, 192.168.1.25. Once it is successfully configured, the address will be copied to the ZyXEL Device's configuration file. It will not change unless you change the setting or upload a different configuration file. This MAC address also displays in the **Status** screen.
Set WAN MAC Address	Select this option and enter the MAC address of the computer on the LAN that is used for Internet access. Enter the MAC address using colons, for example, 00:A0:C5:00:00:02. Once it is successfully configured, the address will be copied to the ZyXEL Device's configuration file. It will not change unless you change the setting or upload a different configuration file. This MAC address also displays in the **Status** screen.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.5 WAN Static IP Encapsulation

Select **Static IP** encapsulation in the **Network** > **WAN** > **Internet Connection** screen if your ISP did not assign you a fixed IP address.

Figure 50 Network > WAN > Internet Connection: Static IP Encapsulation



Encapsulation: Static IP

● Factory default

○ Set WAN MAC Address 00:13:49:12:01:12

The following table describes the labels in this screen.

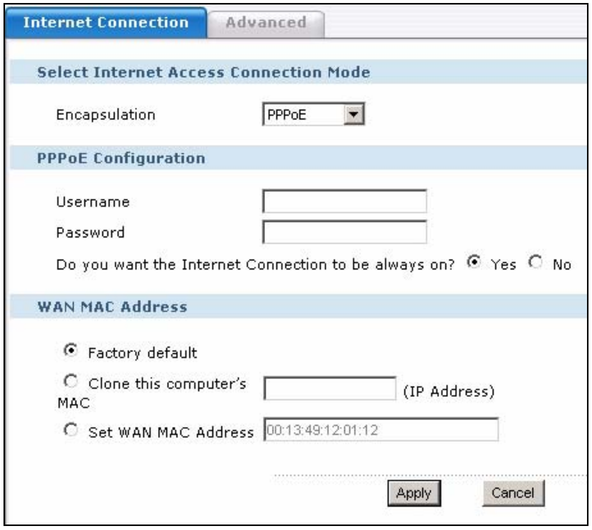
Table 13 Network > WAN > Internet Connection: Static IP Encapsulation

LABEL	DESCRIPTION
IP Address	Enter your WAN IP address in this field. Enter the IP address in dotted decimal notation, for example, 192.168.1.25.
Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	Enter a Gateway IP Address (if your ISP gave you one) in this field.
Primary DNS Server Secondary DNS Server	Enter the DNS server IP address (or addresses) provided by your ISP in these fields.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the ZyXEL Device's MAC address, cloning a computer's IP address, or manually entering a MAC address.
Factory default	Select this option to use the factory assigned default MAC address.
Clone this computer's MAC	Select this option and enter the IP address of the computer on the LAN that is used for Internet access. Enter the IP address in dotted decimal notation, for example, 192.168.1.25. Once it is successfully configured, the address will be copied to the ZyXEL Device's configuration file. It will not change unless you change the setting or upload a different configuration file. This MAC address also displays in the **Status** screen.
Set WAN MAC Address	Select this option and enter the MAC address of the computer on the LAN that is used for Internet access. Enter the MAC address using colons, for example, 00:A0:C5:00:00:02. Once it is successfully configured, the address will be copied to the ZyXEL Device's configuration file. It will not change unless you change the setting or upload a different configuration file. This MAC address also displays in the **Status** screen.
OK	Click **OK** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.6 WAN PPPoE Encapsulation

The ZyXEL Device supports PPPoE (Point-to-Point Protocol over Ethernet) for a dial-up connection. If your Internet connection type is PPPoE, select the **PPPoE** option in the **Network** > **WAN** > **Internet Connection** screen.

Figure 51 Network > WAN > Internet Connection: PPPoE Encapsulation



Select Internet Access Connection Mode

Encapsulation: PPPoE

PPPoE Configuration

Username:

Password:

Do you want the Internet Connection to be always on? ● Yes ○ No

WAN MAC Address

● Factory default

○ Clone this computer's MAC (IP Address)

○ Set WAN MAC Address 00:13:49:12:01:12

The following table describes the labels in this screen.

Table 14 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Do you want the Internet Connection to be always on?	Select **Yes** if you do not want the connection to time out. If you select **No**, you can configure a maximum idle time before the ZyXEL Device disconnects the Internet connection.
Maximum idle Time	Set how long the Internet connection can be idle before ZyXEL Device disconnects it. This only applies if you set the Internet connection to not be always on.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the ZyXEL Device's MAC address, cloning a computer's IP address, or manually entering a MAC address.
Factory default	Select this option to use the factory assigned default MAC address.
Clone this computer's MAC	Select this option and enter the IP address of the computer on the LAN that is used for Internet access. Enter the IP address in dotted decimal notation, for example, 192.168.1.25. Once it is successfully configured, the address will be copied to the ZyXEL Device's configuration file. It will not change unless you change the setting or upload a different configuration file. This MAC address also displays in the **Status** screen.
Set WAN MAC Address	Select this option and enter the MAC address of the computer on the LAN that is used for Internet access. Enter the MAC address using colons, for example, 00:A0:C5:00:00:02. Once it is successfully configured, the address will be copied to the ZyXEL Device's configuration file. It will not change unless you change the setting or upload a different configuration file. This MAC address also displays in the **Status** screen.

Table 14 Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
OK	Click **OK** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

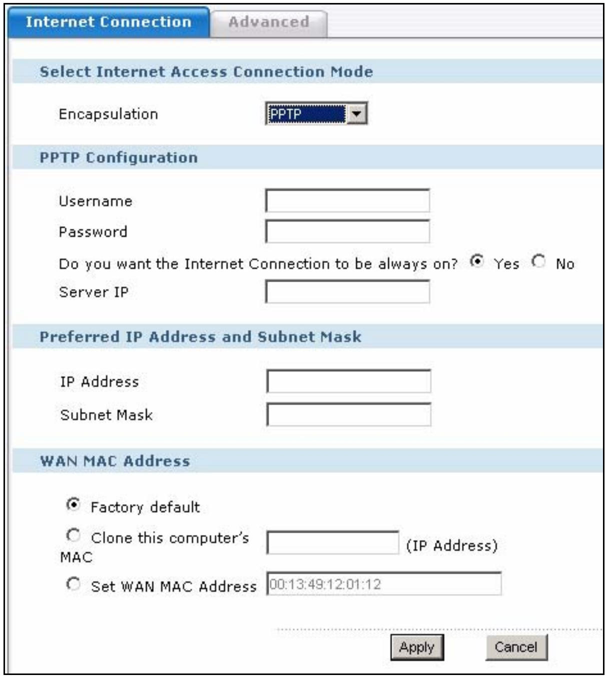
8.7 WAN PPTP Encapsulation

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

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The screen shown next is for **PPTP** encapsulation.

If your Internet connection type is PPTP, select the **PPTP** option in the **Network** > **WAN** > **Internet Connection** screen.

Figure 52 Network > WAN > Internet Connection: PPTP Encapsulation



Select Internet Access Connection Mode

Encapsulation: PPTP

PPTP Configuration

Username

Password

Do you want the Internet Connection to be always on? ● Yes ○ No

Server IP

Preferred IP Address and Subnet Mask

IP Address

Subnet Mask

WAN MAC Address

● Factory default

○ Clone this computer's MAC (IP Address)

○ Set WAN MAC Address 00:13:49:12:01:12

The following table describes the labels in this screen.

Table 15 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Do you want the Internet Connection to be always on?	Select **Yes** if you do not want the connection to time out. If you select **No**, you can configure a maximum idle time before the ZyXEL Device disconnects the Internet connection.

Table 15 Network > WAN > Internet Connection: PPTP Encapsulation (continued)

LABEL	DESCRIPTION
Maximum idle Time	Set how long the Internet connection can be idle before ZyXEL Device disconnects it. This only applies if you set the Internet connection to not be always on.
Server IP	Type the IP address of the PPTP server.
IP Address	Enter your WAN IP address in this field. You assign this IP address to the WAN interface temporarily to initiate the PPTP negotiation.
Subnet Mask	Enter the IP subnet mask in this field.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the ZyXEL Device’s MAC address, cloning a computer’s IP address, or manually entering a MAC address.
Factory default	Select this option to use the factory assigned default MAC address.
Clone this computer’s MAC	Select this option and enter the IP address of the computer on the LAN that is used for Internet access. Enter the IP address in dotted decimal notation, for example, 192.168.1.25. Once it is successfully configured, the address will be copied to the ZyXEL Device’s configuration file. It will not change unless you change the setting or upload a different configuration file. This MAC address also displays in the **Status** screen.
Set WAN MAC Address	Select this option and enter the MAC address of the computer on the LAN that is used for Internet access. Enter the MAC address using colons, for example, 00:A0:C5:00:00:02. Once it is successfully configured, the address will be copied to the ZyXEL Device’s configuration file. It will not change unless you change the setting or upload a different configuration file. This MAC address also displays in the **Status** screen.
OK	Click **OK** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.8 WAN Multicast

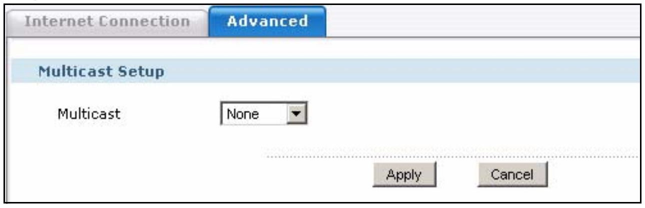
Multicast allows packets to be transmitted to multiple hosts. Multicast is an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer).

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.

When you have multicast enabled, the ZyXEL Device queries all directly connected networks when it starts up to gather group membership. After that, the ZyXEL Device periodically updates this information.

Click **Network** > **WAN** > **Advanced** to open the following screen.

Figure 53 Network > WAN > Advanced



Multicast Setup

Multicast: None

The following table describes the labels in this screen.

Table 16 Network > WAN > Advanced

LABEL	DESCRIPTION
Multicast	Select **None** to turn off multicasting on the ZyXEL Device. If any of the LAN computers are using applications that use multicasting, select **IGMP-v3** to have the ZyXEL Device proxy multicast traffic. This is especially useful for multimedia conferences over the Internet.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9

LAN

This chapter describes the LAN screen you use to configure the LAN IP address on the ZyXEL Device.

9.1 LAN Overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

9.1.1 Factory LAN Defaults

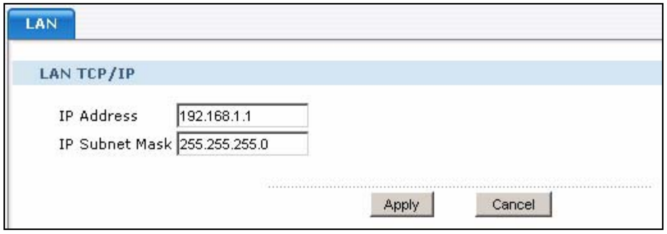
The LAN parameters of the ZyXEL Device are preset in the factory with an IP address of 192.168.1.1 and a subnet mask of 255.255.255.0 (24 bits)

These parameters should work for the majority of installations.

9.2 LAN Screen

Click **Network** > **LAN** to configure the LAN interface settings.

Figure 54 Network > LAN



IP Address 192.168.1.1
IP Subnet Mask 255.255.255.0

The following table describes the labels in this screen.

Table 17 Network > LAN

LABEL	DESCRIPTION
IP Address	Enter an IP address for the LAN interface in dotted decimal notation. For example, 192.168.1.1.
Subnet Mask	Enter the subnet mask for the IP address above. For example. 255.255.255.0.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10

DHCP

This chapter describes the DHCP screen you use to configure the DHCP server on the ZyXEL Device.

10.1 DHCP

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

10.1.1 Factory DHCP Defaults

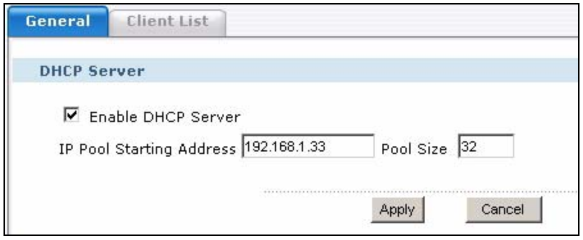
The LAN parameters of the ZyXEL Device are preset in the factory with the DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations.

10.2 DHCP Screen

Click **Network** > **DNCP** to configure the DHCP server settings.

Figure 55 Network > DHCP > General



☑ Enable DHCP Server

IP Pool Starting Address 192.168.1.33 Pool Size 32

The following table describes the labels in this screen.

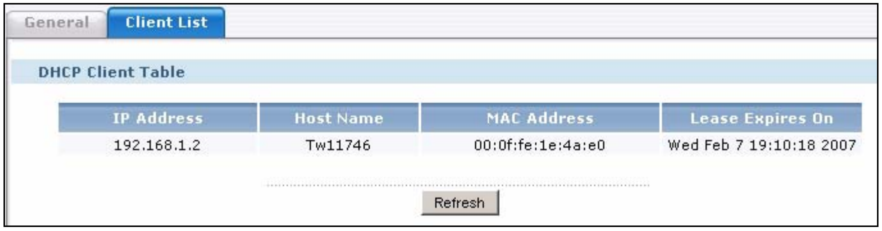
Table 18 Network > DHCP > General

LABEL	DESCRIPTION
Enable DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Select this option to enable this feature on the ZyXEL Device and configure the fields below. When configured as a server, the ZyXEL Device provides TCP/IP configuration for the clients. Clear this check box to disable DHCP server on the ZyXEL Device. You must have another DHCP server on your LAN, or else the computers must be manually configured.
IP Pool Starting Address	Enter the first of the contiguous addresses in the IP address pool.
Pool Size	Specify the maximum number of IP addresses you want the ZyXEL Device to assign to DHCP clients.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.2.1 DHCP Client List Screen

Click **Network** > **DHCP** > **Client List** to open the following screen. Use this screen to view current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the ZyXEL Device's DHCP server.

Figure 56 Network > DHCP > Client List



IP Address	Host Name	MAC Address	Lease Expires On
192.168.1.2	Tw11746	00:0f:fe:1e:4a:e0	Wed Feb 7 19:10:18 2007

The following table describes the labels in this screen.

Table 19 Network > DHCP > General

LABEL	DESCRIPTION
IP Address	This field displays the IP address assigned to a DHCP client.
Host Name	This field displays the DHCP client's host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique for each device (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.
Lease Expires On	This field displays how much longer the IP address is offered to that particular DHCP client.
Refresh	Click **Refresh** to reload the DHCP table.

NAT and Firewall (WAN to LAN)

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

11.1 NAT Overview

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

11.2 Port Forwarding and Firewall

Incoming sessions (sessions initiated from the WAN and going to the LAN) are blocked by default. Use port forwarding to allow access from the outside (the Internet) to server(s) on your LAN.

Configuring port forwarding also configures the firewall's WAN to LAN settings.

Port forwarding automatically has the firewall allow unencrypted access from the WAN (the Internet) to your LAN.

- For secure connections from the Internet to the LAN computers, use the secure remote user portal (see part VI on page 133).
- To set which services/protocols can access the ZyXEL Device from the WAN (the Internet), see Section 19.4 on page 129. This allows or disallows remote management of the ZyXEL Device.
- To control access going from the LAN to the WAN, use the security screens (see part III on page 91).

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

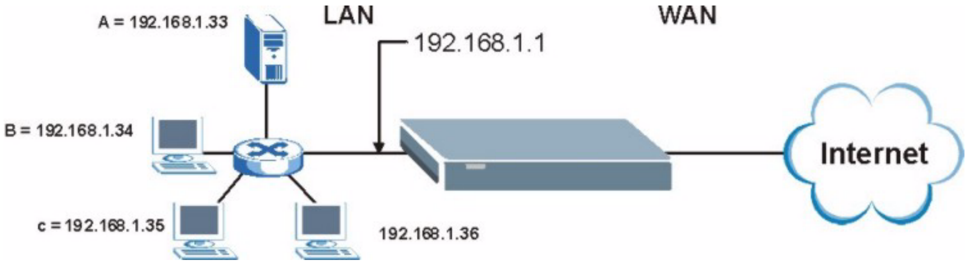
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Some 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.

11.2.1 Configuring Servers Behind Port Forwarding Example

The following example shows the IP addresses of computers on the LAN. You can use port forwarding to send web and FTP traffic to computer A at IP address 192.168.1.33 and Telnet traffic to computer B at 192.168.1.34. You could make computer C (at 192.168.1.35) the default. 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 57 Multiple Servers Behind NAT Example



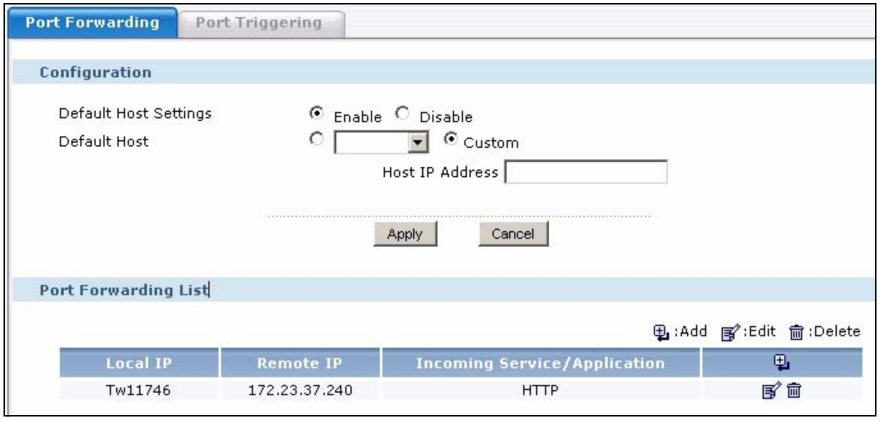
11.3 Port Forwarding Screen

Port forwarding allows traffic from the WAN to be forwarded through the ZyXEL Device. To change your ZyXEL Device’s port forwarding settings, click **Network** > **NAT** > **Port Forwarding**. The screen appears as shown. Use this screen to define the local servers to which to forward incoming services.

If you do not assign a default host, the ZyXEL Device discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix B on page 177 for port numbers commonly used for particular services.

Figure 58 Network > NAT > Port Forwarding



Configuration

Default Host Settings ● Enable ○ Disable

Default Host ○ [ ] ● Custom

Host IP Address [ ]

Port Forwarding List

Local IP	Remote IP	Incoming Service/Application	
Tw11746	172.23.37.240	HTTP	

The following table describes the labels in this screen.

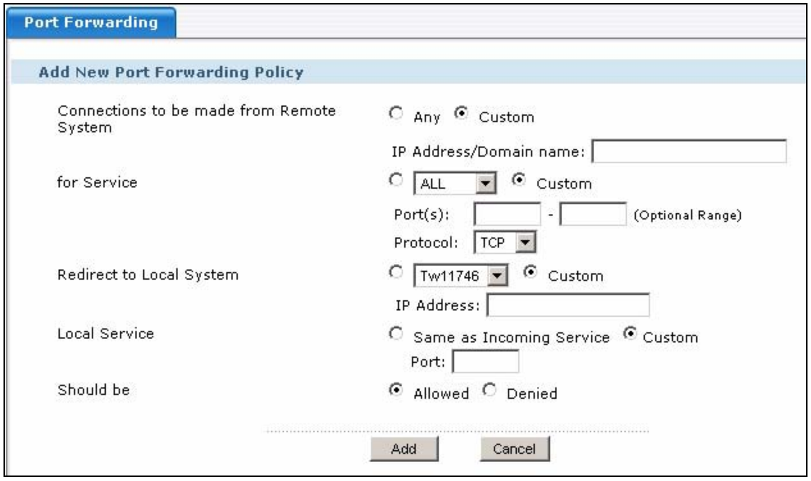
Table 20 NAT Application

LABEL	DESCRIPTION
Configuration	
Default Host Settings	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the port forwarding list. Enable this option to be able to assign a default host. If you do not assign a default host, the ZyXEL Device discards all packets received for ports that are not specified in the port forwarding list or remote management.
Default Host	Select a LAN computer from the drop-down list box or select **Custom** and specify a LAN IP address.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Port Forwarding List	
Local IP	This field displays the host name or IP address of the LAN computer server that receives the **Incoming Service/Application**.
Remote IP	This field displays the IP address or domain name of the WAN computer that can access the LAN computer. **All** displays if any WAN computer can access the LAN computer.
Incoming Service/ Application	This field displays the service that the ZyXEL Device sends to the computer configured in the **Local IP** field.
Add icon	This column provides icons to add, edit, and delete entries. Click the **Add** icon to go to the screen where you can configure a new entry. Click the **Edit** icon to go to the screen where you can edit the entry. Click the **Delete** icon to remove an entry.

11.4 Port Forwarding Add/Edit Screen

Click the **Add** or **Edit** icon in the **Network > NAT** > **Port Forwarding** screen to open this screen. Use this screen to configure a port forwarding rule.

Figure 59 Network > NAT > Port Forwarding > Add/Edit



Add New Port Forwarding Policy

Connections to be made from Remote System ○ Any ● Custom
IP Address/Domain name:

for Service ○ ALL ● Custom
Port(s): - (Optional Range)
Protocol: TCP

Redirect to Local System ○ Tw11746 ● Custom
IP Address:

Local Service ○ Same as Incoming Service ● Custom
Port:

Should be ● Allowed ○ Denied

The following table describes the labels in this screen.

Table 21 Network > NAT > Port Forwarding > Add/Edit

LABEL	DESCRIPTION
Connections to be made from Remote System	Select **Any** to allow connections from any IP address or domain name. To only allow specific users to access the inside server, select **Custom** and specify an IP address or domain name.
for Service	Select a service from the drop-down list box or select **Custom** and specify a port number (or numbers) and protocol. To enter a single port number, enter it in the first field. To enter a range of port numbers, enter the starting port number in the first field and the ending port number in the second field. For a custom service, select the protocol the service uses. Choices are: **TCP**, **UDP**, **AH**, **ESP**, and **GRE**.
Redirect to Local System	Select a LAN computer from the drop-down list box or select **Custom** and specify the IP address of a LAN computer.
Local Service	Select what port number the ZyXEL Device when forwarding the service's traffic to the LAN. If the LAN computer uses the same port for the service as the incoming packet's source port, select **Same as Incoming Service**. If the LAN computer uses a different port for the service, select **Custom** and specify the port.
Should be	Select whether the ZyXEL Device should forward (**Allowed**) or drop (**Denied**) incoming traffic that matches this port forwarding policy. For example, say you want to allow access for TCP ports 1000 to 2000, but block TCP port 1500. You could configure a policy that allows TCP ports 1000 to 2000 and then add another policy (higher in the list) that blocks TCP port 1500.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to return to the previous screen without saving your changes.

11.5 Trigger Port Forwarding

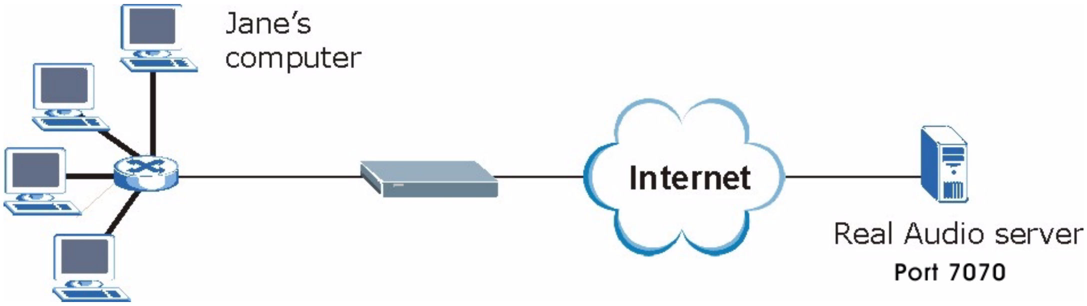
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem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

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The 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.

11.5.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 60 Trigger Port Forwarding Process: Example



1 Jane requests a file from the Real Audio server (port 7070).
2 Port 7070 is a “trigger” port and causes the 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).

11.5.2 Two Points To Remember About Trigger Ports

1 Trigger events only happen on data that is going coming from inside the ZyXEL Device and going to the outside.

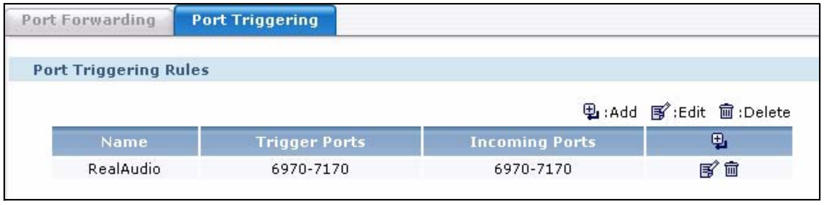
2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

11.6 Port Triggering Screen

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

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

Figure 61 Network > NAT > Port Triggering



Name	Trigger Ports	Incoming Ports	
RealAudio	6970-7170	6970-7170	

The following table describes the labels in this screen.

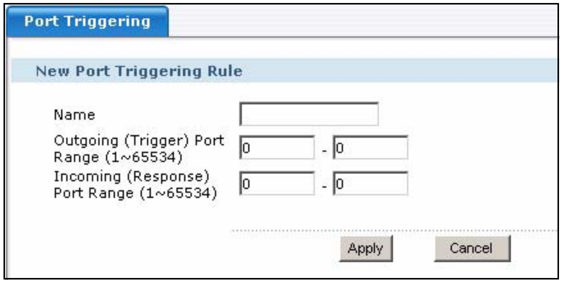
Table 22 Network > NAT > Port Triggering

LABEL	DESCRIPTION
Name	This name identifies the trigger port rule.
Trigger Ports	The trigger port range of ports causes (triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Incoming Ports	This is the range of ports that a server on the WAN uses when it sends out a service's traffic. The ZyXEL Device forwards incoming traffic with these ports to the LAN computer that requested the service.
Add icon	This column provides icons to add, edit, and delete entries. Click the **Add** icon to go to the screen where you can configure a new entry. Click the **Edit** icon to go to the screen where you can edit the entry. Click the **Delete** icon to remove an entry.

11.7 Port Triggering Add/Edit Screen

Click the **Add** or **Edit** icon in the **Network > NAT** > **Port Triggering** screen to open this screen. Use this screen to configure a port triggering rule.

Figure 62 Network > NAT > Port Triggering > Add/Edit



Port Triggering
New Port Triggering Rule
Name
Outgoing (Trigger) Port Range (1~65534)
0 - 0
Incoming (Response) Port Range (1~65534)
0 - 0
Apply
Cancel

The following table describes the labels in this screen.

Table 23 Network > NAT > Port Triggering > Add/Edit

LABEL	DESCRIPTION
Name	Type a unique name (up to 16 alpha-numeric characters) for identification purposes. Underscores (_) and hyphens (-) are also allowed but other special characters and spaces are not.
Outgoing (Trigger) Port Range	The trigger port range of ports causes (triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Enter the starting and ending port numbers for the range.
Incoming (Response) Port Range	This is the range of ports that a server on the WAN uses when it sends out a service's traffic. The ZyXEL Device forwards incoming traffic with these ports to the LAN computer that requested the service. Enter the starting and ending port numbers for the range.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

12

DDNS

12.1 Dynamic DNS

DDNS (Dynamic DNS) lets you use a fixed domain name with a dynamic WAN IP address that changes. This way people can find a website, FTP server, or any other service that you host on a LAN computer behind the ZyXEL Device.

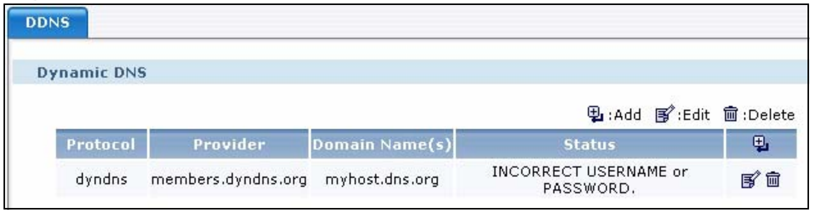
You must first register a DDNS account with www.dyndns.org and create your domain names (like myhost.dhs.org). You will also be provided with a password that you need to enter in the ZyXEL Device.

12.2 DDNS Screen

Click **Network** > **DDNS** to open the following screen. This screen displays the DDNS records configured on the ZyXEL Device for using DDNS domain names.

The ZyXEL Device must have a public WAN IP address to use DDNS.

Figure 63 Network > DDNS



Protocol	Provider	Domain Name(s)	Status	
dyndns	members.dyndns.org	myhost.dns.org	INCORRECT USERNAME or PASSWORD.	

The following table describes the labels in this screen.

Table 24 Network > DDNS

LABEL	DESCRIPTION
Protocol	This field displays the protocol that the DDNS service record uses (dyndns).
Provider	This is the name of your Dynamic DNS service provider.
Domain Name(s)	These are the domain names that you registered with the Dynamic DNS service provider.

Table 24 Network > DDNS

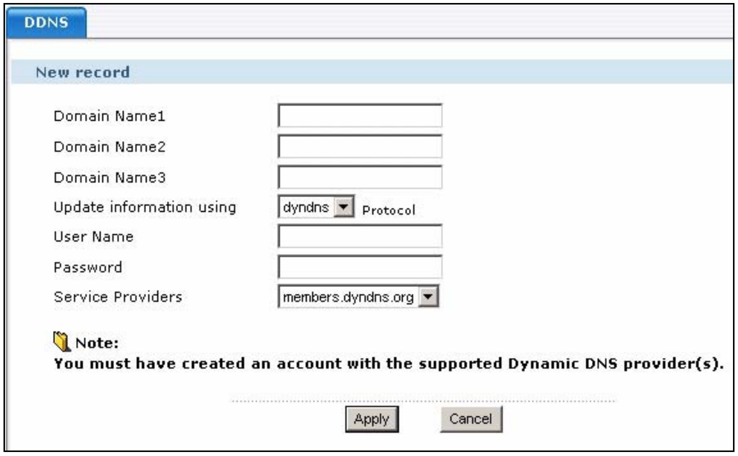
LABEL	DESCRIPTION
Status	This field displays the current usage status of the DDNS service record.
Add icon	This column provides icons to add, edit, and delete entries. Click the **Add** icon to go to the screen where you can configure a new entry. Click the **Edit** icon to go to the screen where you can edit the entry. Click the **Delete** icon to remove an entry.

12.3 DDNS Add/Edit Screen

Click the **Add** or **Edit** icon in the **Network > DDNS** screen to open this screen. Use this screen to configure the ZyXEL Device to use domain names with a dynamic WAN IP address.

The ZyXEL Device must have a public WAN IP address to use DDNS.

Figure 64 Network > DDNS > Add/Edit



Domain Name1

Domain Name2

Domain Name3

Update information using: dyndns Protocol

User Name

Password

Service Providers: members.dyndns.org

Note:
You must have created an account with the supported Dynamic DNS provider(s).

The following table describes the labels in this screen.

Table 25 Network > DDNS > Add/Edit

LABEL	DESCRIPTION
Domain Name1~3	Enter up to three of the domain names that you registered with the Dynamic DNS service provider.
Update information using	Select the protocol that the DDNS service record uses (dyndns).
User Name	Enter your user name. You can use up to 31. You can use alphanumeric characters and the underscore (_). Spaces are not allowed.
Password	Enter the password associated with the user name above. You can use up to 31 alphanumeric characters and the underscore (_). Spaces are not allowed.
Service Providers	Select your Dynamic DNS service provider.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

PART III
Security

13

Access Control

This chapter gives some background information on firewalls and explains how to get started with the ZyXEL Device's firewall.

13.1 Access Control Introduction

Access control controls access going from computers on the LAN to the WAN (the Internet). It also allows you to use QoS to give higher priority to traffic from specific applications (like voice).

✍ Configuring access control configures the firewall's LAN to WAN settings.

Port forwarding automatically has the firewall allow unencrypted access from the WAN (the Internet) to your LAN.

- For secure connections from the Internet to the LAN computers, use the secure remote user portal (see part VI on page 133).
- To set which services/protocols can access the ZyXEL Device from the WAN (the Internet), see Section 19.4 on page 129. This allows or disallows remote management of the ZyXEL Device.
- To allow unencrypted sessions in from the WAN to the LAN, use the NAT port forwarding screen (see Section 11.3 on page 82).

13.2 Quality of Service (QoS)

Quality of Service (QoS) prioritizes traffic by application. This helps guarantee the quality of high priority traffic like voice. QoS refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications. Here are some recommendations for assigning priorities to different types of traffic.

Figure 65 Priority Assignment Recommendations

PRIORITY	TYPE OF TRAFFIC TO USE FOR
Highest	Voice since it is especially sensitive to jitter (variations in delay).
High	Video since it consumes high bandwidth and is sensitive to jitter.

Figure 65 Priority Assignment Recommendations

PRIORITY	TYPE OF TRAFFIC TO USE FOR
Medium	Internet and chat since they are somewhat sensitive to delay.
Low	E-mail since it is important but can tolerate some delay.
Lowest	File transfers (like FTP) since they should not affect other applications and users.

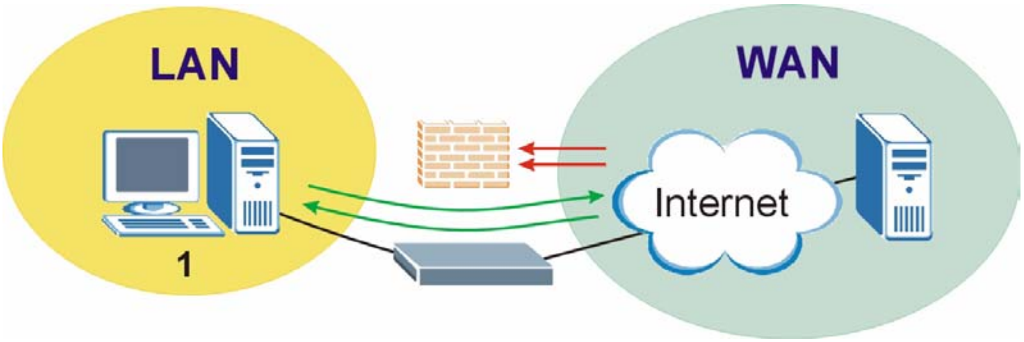
13.3 Firewall Overview

The ZyXEL Device acts as a secure gateway for all data passing between the Internet and the LAN. The ZyXEL Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The ZyXEL Device's firewall is a stateful inspection firewall. The ZyXEL Device restricts access by screening data packets against defined access rules. It can also inspect sessions. For example, traffic from the WAN is not allowed unless it is initiated by a computer in the LAN. You can configure firewall rules for data passing between interfaces.

The following figure shows the ZyXEL Device's default firewall rules in action as well as demonstrates how stateful inspection works. User **1** can initiate a Telnet session from within the LAN and responses to this request are allowed. However, other Telnet traffic initiated from the WAN and destined for the LAN is blocked. The firewall allows VPN traffic.

Figure 66 Default Firewall Action



Your customized rules take precedence and override the ZyXEL Device's default settings. The ZyXEL Device checks the schedule, source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyXEL Device takes the action specified in the rule.

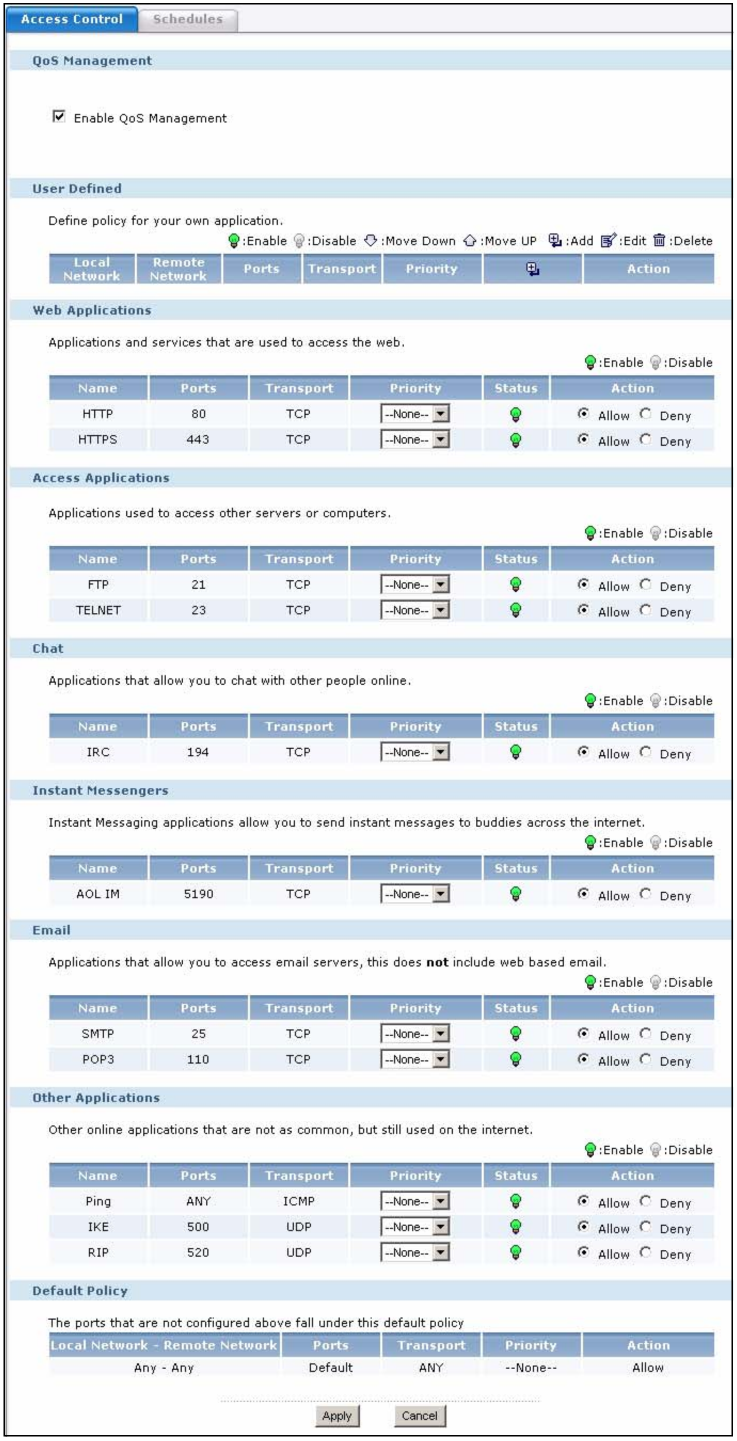
For example, if you want to allow a specific WAN user from any computer to access computers behind the ZyXEL Device, you can set up a rule based on the user's IP address only. If you also apply a schedule to the firewall rule, the user can only access the network at the scheduled time.

13.4 Access Control Screen

Click **Security** > **Access Control** to open the following screen. Use this screen to view the firewall settings and configure QoS settings.

Access control applies to outgoing access (sessions initiated from the LAN and going to the WAN). All outgoing sessions are allowed by default.

Figure 67   Security > Access Control



QoS Management

☑ Enable QoS Management

User Defined

Define policy for your own application.

● :Enable ○ :Disable ⇩ :Move Down ⇧ :Move UP :Add :Edit :Delete

Local Network	Remote Network	Ports	Transport	Priority		Action

Web Applications

Applications and services that are used to access the web.

● :Enable ○ :Disable

Name	Ports	Transport	Priority	Status	Action
HTTP	80	TCP	--None--	●	● Allow ○ Deny
HTTPS	443	TCP	--None--	●	● Allow ○ Deny

Access Applications

Applications used to access other servers or computers.

● :Enable ○ :Disable

Name	Ports	Transport	Priority	Status	Action
FTP	21	TCP	--None--	●	● Allow ○ Deny
TELNET	23	TCP	--None--	●	● Allow ○ Deny

Chat

Applications that allow you to chat with other people online.

● :Enable ○ :Disable

Name	Ports	Transport	Priority	Status	Action
IRC	194	TCP	--None--	●	● Allow ○ Deny

Instant Messengers

Instant Messaging applications allow you to send instant messages to buddies across the internet.

● :Enable ○ :Disable

Name	Ports	Transport	Priority	Status	Action
AOL IM	5190	TCP	--None--	●	● Allow ○ Deny

Email

Applications that allow you to access email servers, this does **not** include web based email.

● :Enable ○ :Disable

Name	Ports	Transport	Priority	Status	Action
SMTP	25	TCP	--None--	●	● Allow ○ Deny
POP3	110	TCP	--None--	●	● Allow ○ Deny

Other Applications

Other online applications that are not as common, but still used on the internet.

● :Enable ○ :Disable

Name	Ports	Transport	Priority	Status	Action
Ping	ANY	ICMP	--None--	●	● Allow ○ Deny
IKE	500	UDP	--None--	●	● Allow ○ Deny
RIP	520	UDP	--None--	●	● Allow ○ Deny

Default Policy

The ports that are not configured above fall under this default policy

Local Network - Remote Network	Ports	Transport	Priority	Action
Any - Any	Default	ANY	--None--	Allow

The following table describes the labels in this screen.

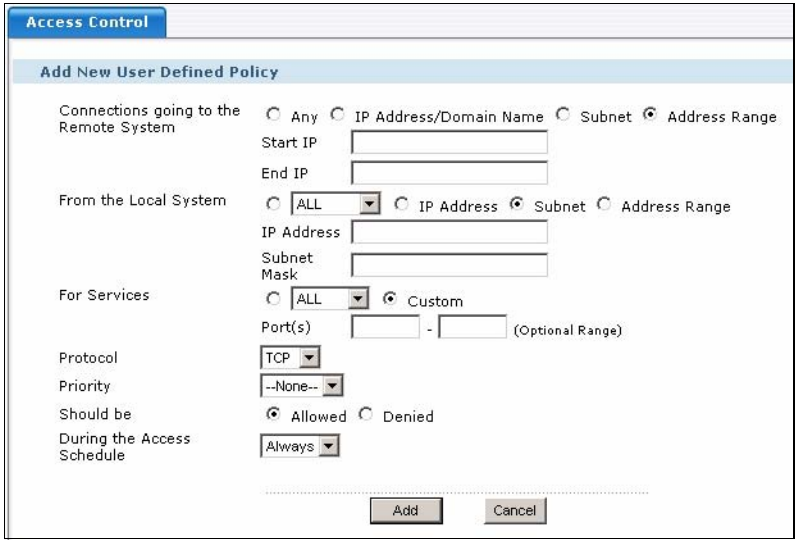
Table 26 Security > Access Control

LABEL	DESCRIPTION
Enable QoS Management	Use QoS to give different priorities to the traffic for different applications. To do so, enable the QoS option here and use the **Priority** fields to assign different priorities to different applications.
User Defined	This section lists your custom firewall rules.
Local Network	This firewall rule applies to traffic sent from this LAN computer(s). The LAN computers are identified by source host name, IP address, subnet, or range of IP addresses.
Remote Network	This firewall rule applies to traffic sent to this Internet destination(s). The Internet computers are identified by IP address, domain name, subnet, or range of IP addresses.
Ports	This is the service (or port numbers) to which the firewall rule applies.
Transport	This is the protocol that the service uses.
Priority	Select the priority you want to give to the traffic that matches this firewall rule.
Add icon	Click the **Add** icon in the heading row to add a new first entry. The **Enable** icon displays whether the rule is enabled or not. Click it to activate or deactivate the rule. The order of your rules is important as they are applied in sequence. Click the **Move Down** icon to move a firewall one row lower in the list. Click the **Move Up** icon to move a firewall one row higher in the list. Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule. A window displays asking you to confirm that you want to delete the rule. Note that subsequent firewall rules move up by one when you take this action.
Action	Select whether the ZyXEL Device should forward (**Allowed**) or drop (**Denied**) outgoing traffic that matches this rule.
	The rest of the screen lists pre-configured rules for common applications.
Name	This field displays the name of the application to which the firewall rule applies.
Default Policy	The firewall's default policy is to allow all outgoing traffic that does not match any of the firewall rules.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to start configuring this screen again.

13.5 Access Control Add/Edit Screen

Click the **Add** or **Edit** icon in the **Security > Access Control** screen to open this screen. Use this screen to configure a firewall rule.

Figure 68 Security > Access Control > Add/Edit



Add New User Defined Policy

Connections going to the Remote System ○ Any ○ IP Address/Domain Name ○ Subnet ● Address Range

Start IP

End IP

From the Local System ○ ALL ○ IP Address ● Subnet ○ Address Range

IP Address

Subnet Mask

For Services ○ ALL ● Custom

Port(s) - (Optional Range)

Protocol: TCP

Priority: --None--

Should be ● Allowed ○ Denied

During the Access Schedule: Always

The following table describes the labels in this screen.

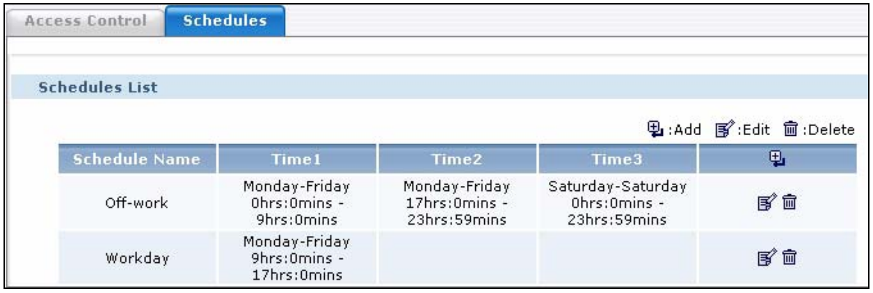
Table 27 Security > Access Control > Add/Edit

LABEL	DESCRIPTION
Connections going to the Remote System	This firewall rule applies to traffic sent to this Internet destination(s). You can select all destinations (**Any**), enter an IP address or domain name, enter an IP subnet, or enter a range of IP addresses.
From the Local System	This firewall rule applies to traffic sent from this LAN computer(s). You can select a host name, enter an IP address, enter an IP subnet, or enter a range of IP addresses. Select **ALL** in the drop-down list box to apply the rule to all of the LAN computers.
For Services	Select the service (or port numbers) to which the firewall rule applies. Select a service from the drop-down list box or select **Custom** and specify a port number (or numbers) and protocol. To enter a single port number, enter it in both fields. To enter a range of port numbers, enter the starting port number in the first field and the ending port number in the second field.
Protocol	Select the protocol that the service uses. Choices are: **TCP**, **UDP**, **AH**, **ESP**, and **GRE**.
Priority	Select the priority you want to give to the traffic that matches this firewall rule.
Should be	Select whether the ZyXEL Device should forward (**Allowed**) or drop (**Denied**) outgoing traffic that matches this rule.
During the Access Schedule	Select a time schedule to apply the rule only during the schedule's times. You must have already configured the schedule. See Section 13.6 on page 98 for how to configure schedules. **Always** applies the rule all the time. Schedules only apply to your custom firewall rules. The pre-defined (default) firewall rules apply all the time.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

13.6 Schedules Screen

Click **Security** > **Schedules** to open the following screen. Use this screen to view the configured firewall schedules.

Figure 69 Security > Schedules



Schedules List

:Add :Edit :Delete

Schedule Name	Time1	Time2	Time3	
Off-work	Monday-Friday 0hrs:0mins - 9hrs:0mins	Monday-Friday 17hrs:0mins - 23hrs:59mins	Saturday-Saturday 0hrs:0mins - 23hrs:59mins	
Workday	Monday-Friday 9hrs:0mins - 17hrs:0mins			

The following table describes the labels in this screen.

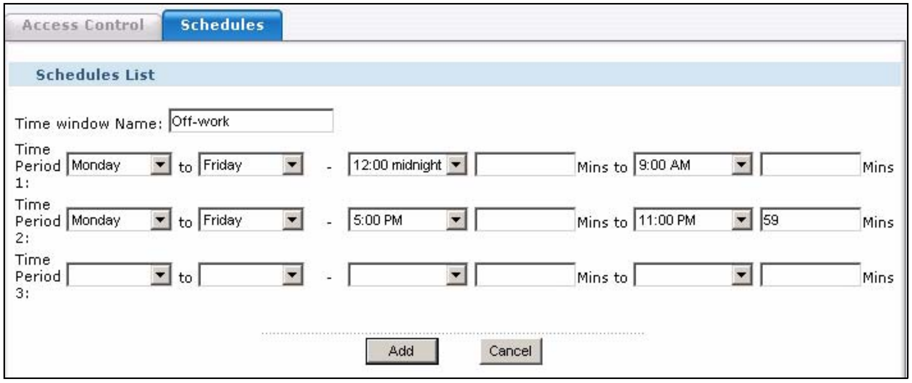
Table 28 Security > Schedules

LABEL	DESCRIPTION
Schedule Name	This is the name you used to identify the schedule.
Time 1~3	These sections list the days and times configured in the schedule.
Add icon	Click the **Add** icon in the heading row to add a new first entry. Click the **Edit** icon to go to the screen where you can edit the schedule. Click the **Delete** icon to delete an existing schedule. A window displays asking you to confirm that you want to delete it.

13.7 Schedules Add/Edit Screen

Click the **Add** or **Edit** icon in the **Security** > **Schedules** screen to open this screen. Use this screen to configure a firewall schedule.

Figure 70 Security > Schedules > Add/Edit



Schedules List

Time window Name: Off-work

Time Period 1: Monday to Friday - 12:00 midnight Mins to 9:00 AM Mins

Time Period 2: Monday to Friday - 5:00 PM Mins to 11:00 PM 59 Mins

Time Period 3: to - Mins to Mins

The following table describes the labels in this screen.

Table 29 Security > Schedules > Add/Edit

LABEL	DESCRIPTION
Time Window Name	Specify a unique name to identify this schedule. Use up to 15 alphanumeric characters. Underscores (_) and hyphens (-) are also allowed but other special characters and spaces are not.
Time Period 1~3	Use the drop-down list boxes to specify up to three time periods. Select upon which days of the week and during which times the schedule applies. The schedule repeats on those days every week. So if you select Monday to Tuesday, 9:00 AM to 5:00 PM, the schedule covers the hours from 9:00 AM to 5:00 PM on all Mondays and Tuesdays. It does not mean the time from Monday 9:00 AM to Tuesday 5:00 PM. See Section 13.7.1 on page 99 for more examples.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

13.7.1 Time Period Examples

Since a time period does not span across days, if you wanted a schedule for off-duty hours on weekdays, you would need two time periods. One time period covering weekday mornings (for example Monday to Friday, 12:00 Midnight to 9:00 AM). The other time period covering weekday evenings (for example Monday to Friday, 9:00 PM to 11:59 PM).

You may need to split into different time periods to have the schedule cover different times on specific days. For example, say you want to give Internet access to the LAN computers from 6:00 AM to 8:00 AM on all weekdays except Wednesdays. Since the days are not continuos, you use two different time periods. Add Monday to Tuesday, 6:00 AM to 8:00 AM in time period 1, and Thursday to Friday, 6:00 AM to 8:00 AM in time period 2.

If you would like to have an overnight schedule like 10:30 PM to 6:00 AM everyday, the time schedule needs to be broken into two pieces. You may add a Sunday to Saturday from 10:30 PM to 11:59 PM as time period 1, and Sunday to Saturday from 12:00 Midnight to 6:00 AM as time period 2.

14

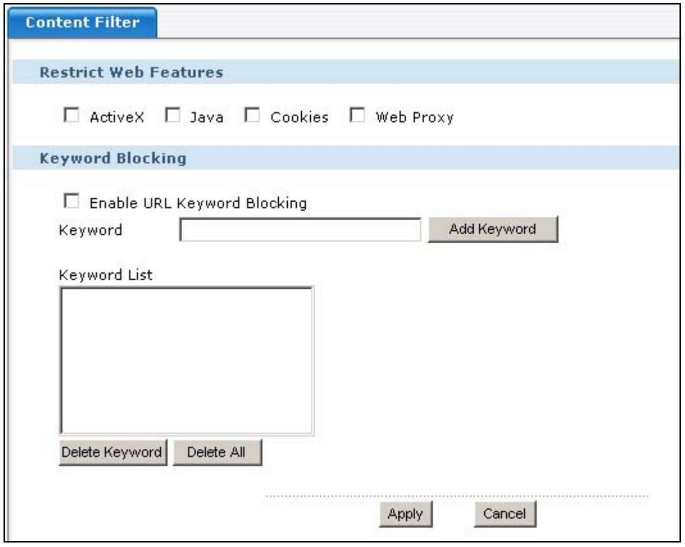
Content Filtering

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

14.1 Content Filter Screen

Use content filtering to block certain web features such as ActiveX controls, Java applets, cookies and disable web proxies. You can also block access to URLs with certain keywords. Click **Security** > **Content Filter** to open the **Content Filter** screen.

Figure 71 Content Filter: Filter



The following table describes the labels in this screen.

Table 30 Content Filter: Filter

LABEL	DESCRIPTION
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.

Table 30 Content Filter: Filter

LABEL	DESCRIPTION
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The ZyXEL Device can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, for example, URL http://www.website.com/notbad.html would be blocked. Select this check box to enable this feature. Keyword blocking has the ZyXEL Device check all of the characters in the URL.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the web filter is blocking this request.
Delete Keyword	Highlight a keyword in the lower box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Delete All	Click this button to remove all of the listed keywords.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to start configuring this screen again.

PART IV
Management

15

UPnP

This chapter introduces the Universal Plug and Play feature. This chapter is only applicable when the ZyXEL Device is in router mode.

15.1 Universal Plug and Play Overview

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

15.1.1 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.

15.1.2 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 Chapter 11 on page 81 for further information about NAT.

15.1.3 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 on the LAN only.

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

15.1.4 UPnP and ZyXEL

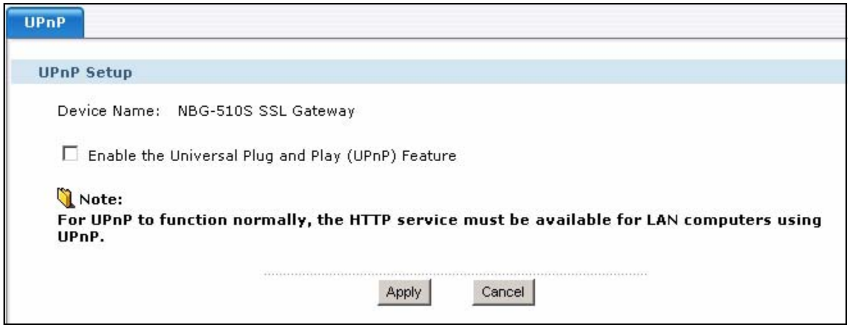
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device).

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

15.2 Configuring UPnP

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

Figure 72 Management > UPnP



Device Name: NBG-510S SSL Gateway

□ Enable the Universal Plug and Play (UPnP) Feature

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

The following table describes the fields in this screen.

Table 31 Management > UPnP

LABEL	DESCRIPTION
Device Name	This identifies the ZyXEL device in UPnP applications.
Enable the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.3 Installing UPnP in Windows Example

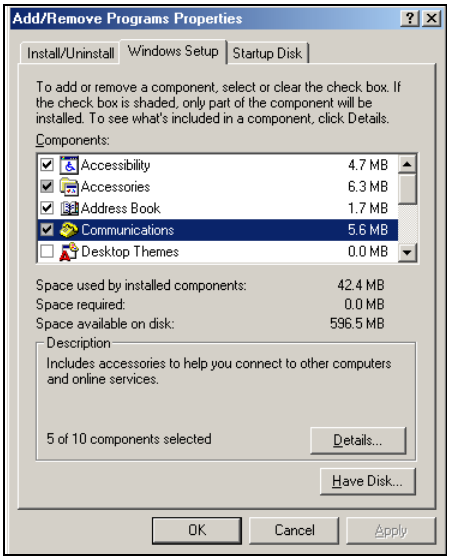
This section shows how to install UPnP in Windows Me and Windows XP.

15.3.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

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

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



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

Components:

☑	Accessibility	4.7 MB
☑	Accessories	6.3 MB
☑	Address Book	1.7 MB
☑	Communications	5.6 MB
□	Desktop Themes	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 596.5 MB

Description

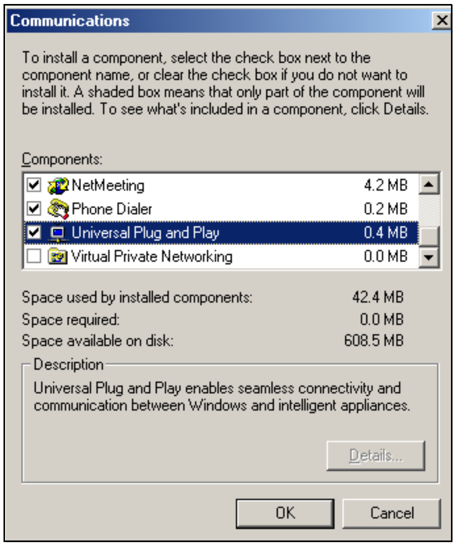
Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

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

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

5 Restart the computer when prompted.



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

Components:

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

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 608.5 MB

Description

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

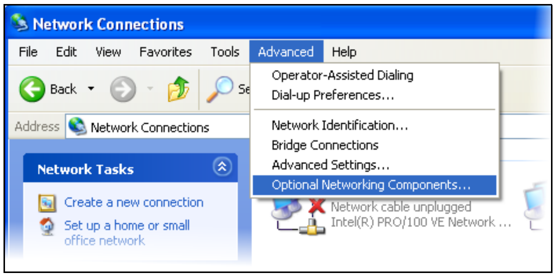
15.3.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

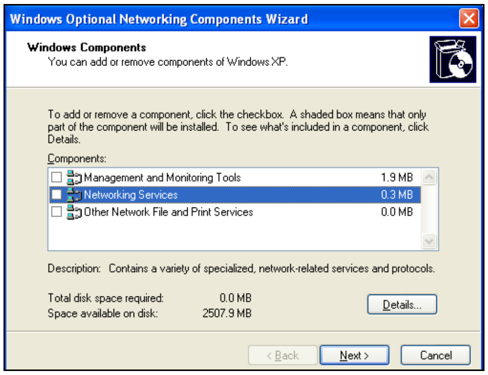
1 Click **Start**, **Settings** and **Control Panel**.

2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….** The **Windows Optional Networking Components Wizard** window displays.



4 Select **Networking Service** in the **Components** selection box and click **Details**.



You can add or remove components of Windows XP.

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

Components:

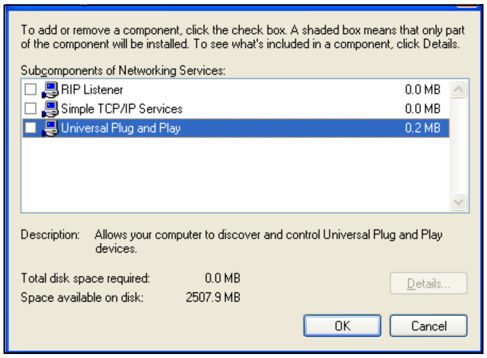
□ Management and Monitoring Tools	1.9 MB
□ Networking Services	0.3 MB
□ Other Network File and Print Services	0.0 MB

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

Total disk space required: 0.0 MB
Space available on disk: 2507.9 MB

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

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



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

Subcomponents of Networking Services:

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

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

Total disk space required: 0.0 MB
Space available on disk: 2507.9 MB

15.4 Using UPnP in Windows XP Example

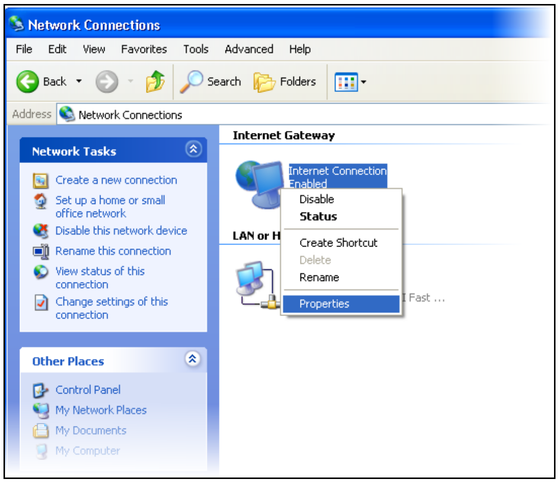
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

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

15.4.1 Auto-discover Your UPnP-enabled Network Device

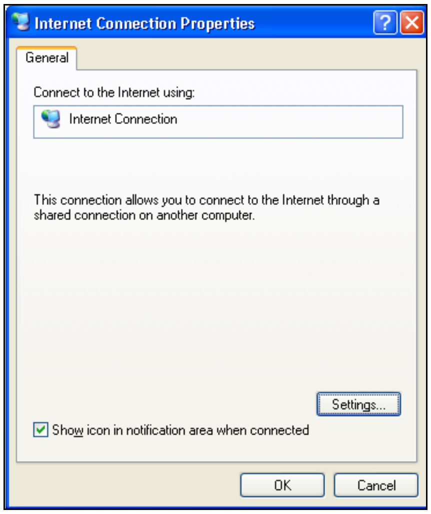
1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under **Internet Gateway**.

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



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

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

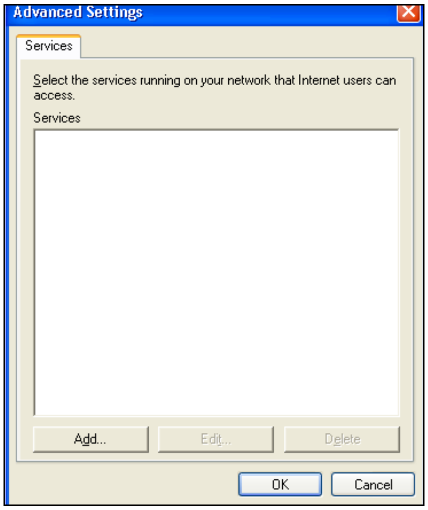


Connect to the Internet using:

Internet Connection

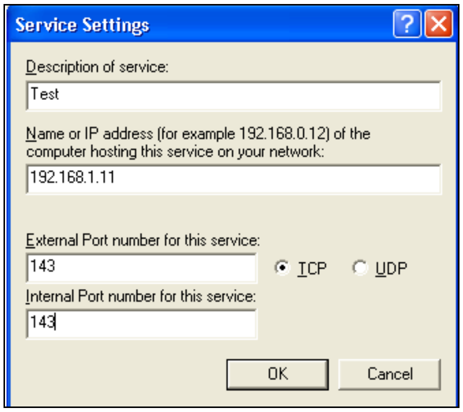
This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected



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

Services



Service Settings

Description of service:
Test

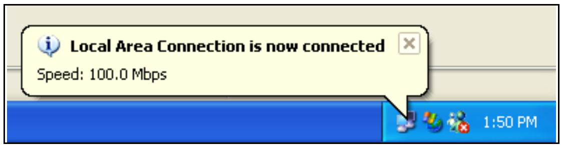
Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.11

External Port number for this service:
143 ● TCP ○ UDP

Internal Port number for this service:
143

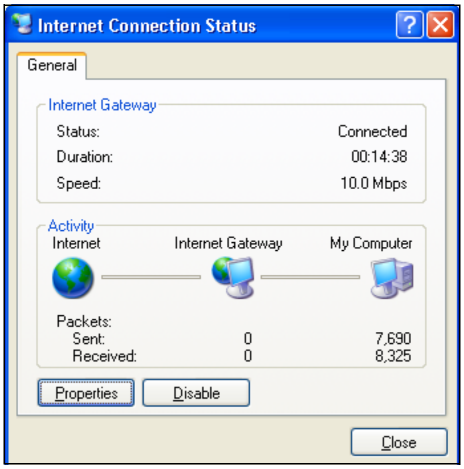
When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

4 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray.



Local Area Connection is now connected
Speed: 100.0 Mbps

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



Internet Connection Status

Internet Gateway

Status: Connected
Duration: 00:14:38
Speed: 10.0 Mbps

Activity

Internet	Internet Gateway	My Computer
Packets:		
Sent:	0	7,690
Received:	0	8,325

15.4.2 Web Configurator Easy Access

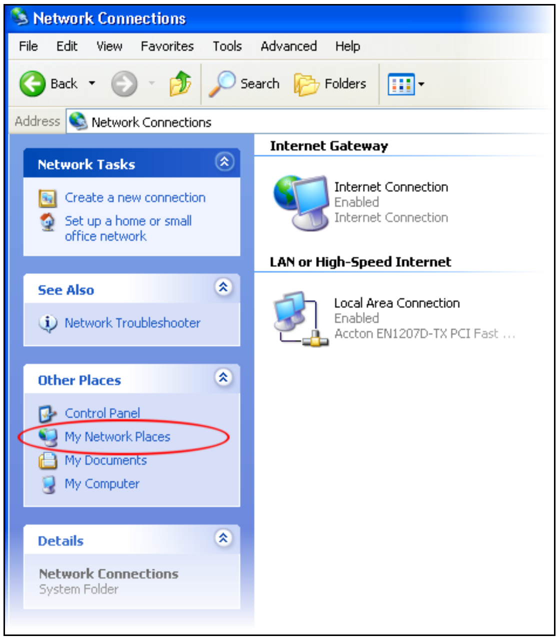
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

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

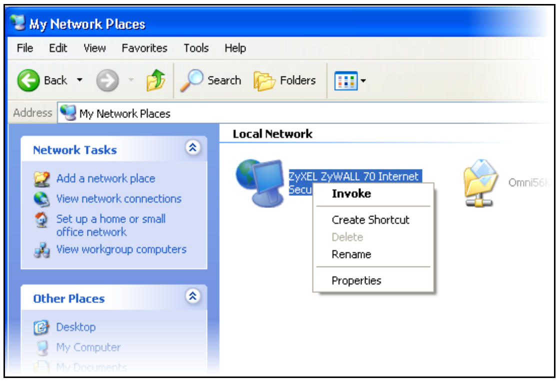
2 Double-click **Network Connections**.

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

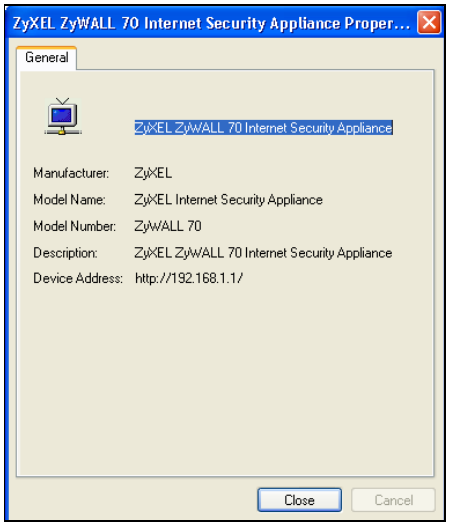


4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

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



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



ZyXEL ZyWALL 70 Internet Security Appliance

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Security Appliance

Model Number: ZyWALL 70

Description: ZyXEL ZyWALL 70 Internet Security Appliance

Device Address: http://192.168.1.1/

16

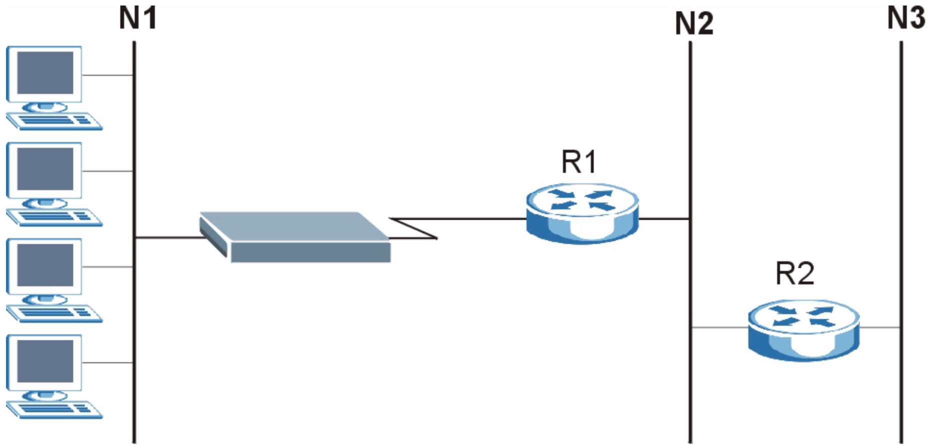
Static Route

This chapter shows you how to configure static routes for your ZyXEL Device.

16.1 IP Static Route

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network N2 in the following figure through remote node Router 1. However, the ZyXEL Device is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyXEL Device about the networks beyond the remote nodes.

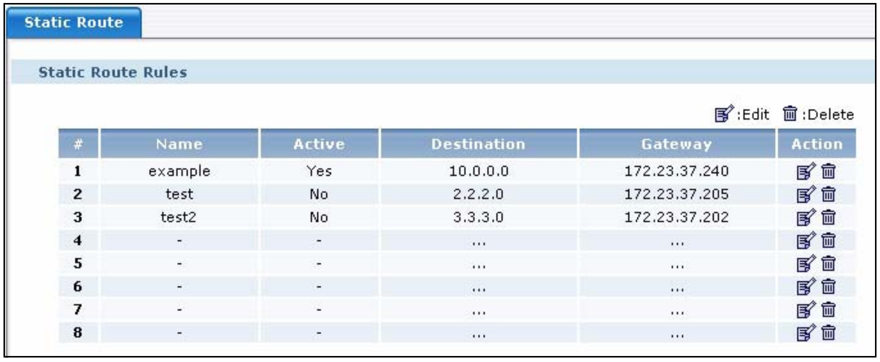
Figure 73 Example of Static Routing Topology



16.2 IP Static Route Screen

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

Figure 74 Management > Static Route



Static Route Rules

✎:Edit 🗑:Delete

#	Name	Active	Destination	Gateway	Action
1	example	Yes	10.0.0.0	172.23.37.240	✎ 🗑
2	test	No	2.2.2.0	172.23.37.205	✎ 🗑
3	test2	No	3.3.3.0	172.23.37.202	✎ 🗑
4	-	-	...	...	✎ 🗑
5	-	-	...	...	✎ 🗑
6	-	-	...	...	✎ 🗑
7	-	-	...	...	✎ 🗑
8	-	-	...	...	✎ 🗑

The following table describes the labels in this screen.

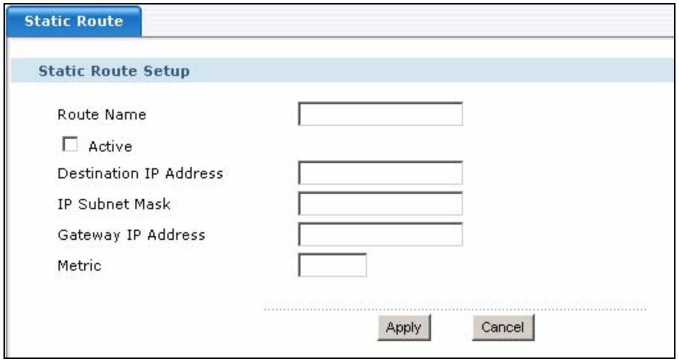
Table 32 Management > Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Name	This is the name that describes or identifies this route.
Active	This field shows whether this static route is active (**Yes**) or not (**No**).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the ZyXEL Device's interface. The gateway helps forward packets to their destinations.
Action	Click the **Edit** icon to go to the screen where you can set up a static route on the ZyXEL Device. No matter which edit icon you click, the entry is added in the first available row. Click the **Delete** icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.

16.2.1 IP Static Route Edit

Click a static route's **Edit** icon to display the following screen. Use this screen to configure the required information for a static route.

Figure 75 Management > Static Route > Edit



Static Route Setup

Route Name

□ Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

The following table describes the labels in this screen.

Table 33 Management > Static Route > Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

PART V
Maintenance

17

System

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

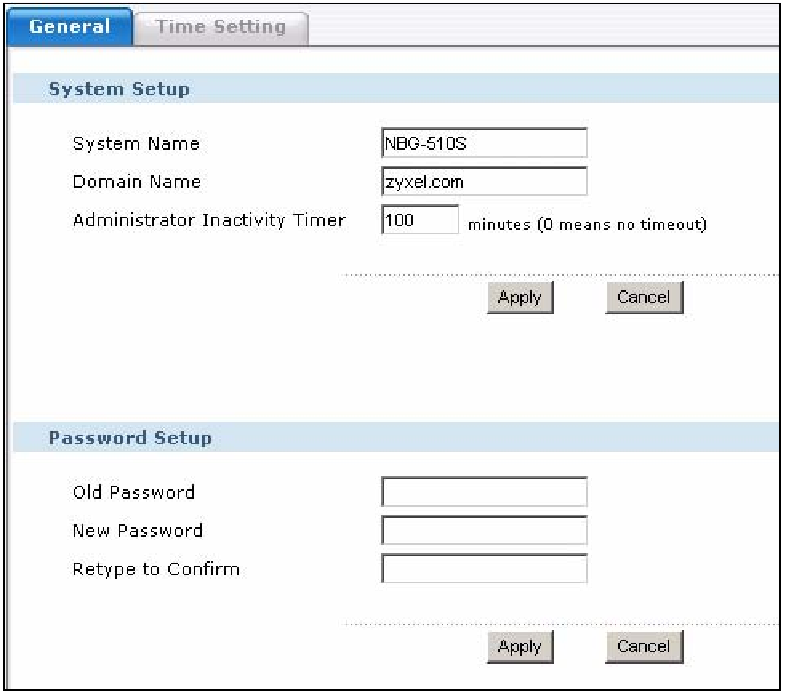
17.1 System Overview

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

17.2 System General Screen

Click **Maintenance** > **System** to display the following screen.

Figure 76 Maintenance > System > General



System Name: NBG-510S
Domain Name: zyxel.com
Administrator Inactivity Timer: 100 minutes (0 means no timeout)

The following table describes the labels in this screen.

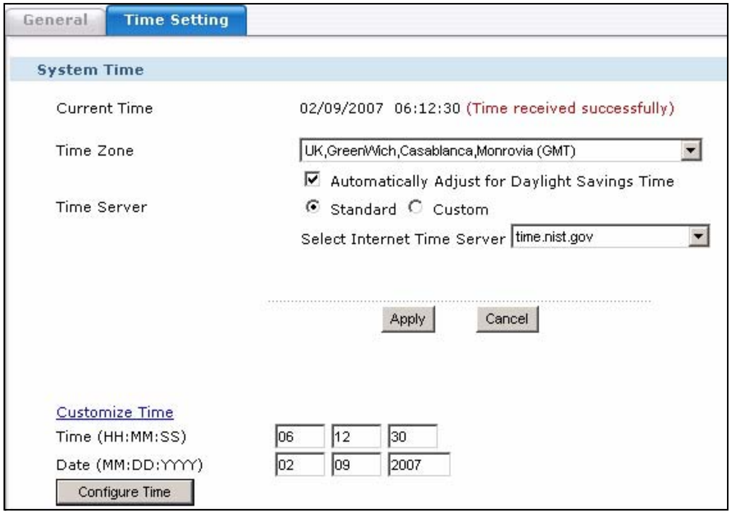
Table 34 Maintenance > System > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the ZyXEL Device in an Ethernet network. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Password Setup	Change your ZyXEL Device's password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 31 printable ASCII characters with no spaces allowed). As you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17.3 Time Setting Screen

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

Figure 77 Maintenance > System > Time Setting



Current Time 02/09/2007 06:12:30 (Time received successfully)

Time Zone UK,GreenWich,Casablanca,Monrovia (GMT)

☑ Automatically Adjust for Daylight Savings Time

Time Server ● Standard ○ Custom

Select Internet Time Server time.nist.gov

Time (HH:MM:SS) 06 12 30

Date (MM:DD:YYYY) 02 09 2007

The following table describes the labels in this screen.

Table 35 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time	This field displays the date and time of your ZyXEL Device in month/day/year hour:minute:second format. Unless you configure the time manually, the ZyXEL Device synchronizes the time with the time server each time you reload this page. The text to the right explains how the time was obtained. **manual time set** means the time is manually configured. **SNTP status enabled** means the time was synchronized with a SNTP (Simple Network Time Protocol) server.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Automatically Adjust for Daylight Savings Time	Select this option to have the ZyXEL Device automatically use Daylight Saving Time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Note: At the time of writing, only US and UK time zones are supported.
Time Server	Select **Standard** to be able to select a time server from the drop-down list of time servers. Select **Custom** to be able to specify another time server.
Select Internet Time Server	Select the time server the ZyXEL Device uses from the drop-down list. This is available when you select **Standard** for the **Time Server**.
Manual Entry of Time Server	Specify the IP address or domain name of the time server the ZyXEL Device uses. This is available when you select **Custom** for the **Time Server**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Customize Time	Click this link to enter the time and date manually.
Time (HH:MM:SS)	Enter the new time in these fields.

Table 35 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Date (MM:DD:YYYY)	Enter the new date in these fields.
Configure Time	Click **Configure Time** to have the ZyXEL Device start using the time you manually configured.

18

Logs

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

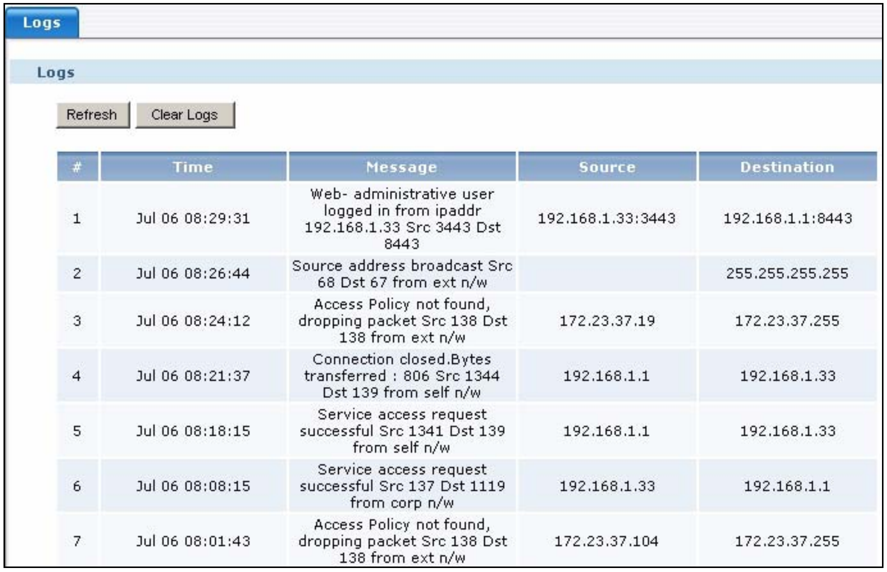
18.1 Logs Screen

The web configurator allows you to look at all of the ZyXEL Device's logs in one location.

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

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries.

Figure 78 Maintenance > Logs



#	Time	Message	Source	Destination
1	Jul 06 08:29:31	Web- administrative user logged in from ipaddr 192.168.1.33 Src 3443 Dst 8443	192.168.1.33:3443	192.168.1.1:8443
2	Jul 06 08:26:44	Source address broadcast Src 68 Dst 67 from ext n/w		255.255.255.255
3	Jul 06 08:24:12	Access Policy not found, dropping packet Src 138 Dst 138 from ext n/w	172.23.37.19	172.23.37.255
4	Jul 06 08:21:37	Connection closed.Bytes transferred : 806 Src 1344 Dst 139 from self n/w	192.168.1.1	192.168.1.33
5	Jul 06 08:18:15	Service access request successful Src 1341 Dst 139 from self n/w	192.168.1.1	192.168.1.33
6	Jul 06 08:08:15	Service access request successful Src 137 Dst 1119 from corp n/w	192.168.1.33	192.168.1.1
7	Jul 06 08:01:43	Access Policy not found, dropping packet Src 138 Dst 138 from ext n/w	172.23.37.104	172.23.37.255

The following table describes the labels in this screen.

Table 36 Maintenance > Logs

LABEL	DESCRIPTION
Refresh	Click **Refresh** to renew the log screen.
Clear Log s	Click **Clear Logs** to delete all the logs.
#	This is the number of an individual log entry.
Time	This field displays the time the log was recorded in month day hour:minute:second format. See Chapter 17 on page 119 to configure the ZyXEL Device's time and date.

Table 36 Maintenance > Logs

LABEL	DESCRIPTION
Message	This field states the reason for the log.
Source	If the log was caused by an incoming packet, this field lists the packet's source IP address and port number.
Destination	If the log was caused by an incoming packet, this field lists the packet's destination IP address and port number.

19

Tools

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the ZyXEL Device.

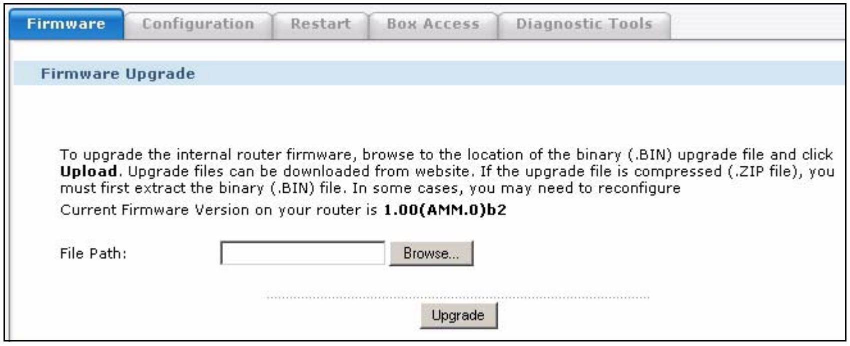
19.1 Firmware Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "ZyXEL Device.bin". The upload process uses HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) and may take up to two minutes. After a successful upload, the system will reboot.

Only upload firmware for your specific model!

Click **Maintenance** > **Tools**. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

Figure 79 Maintenance > Tools > Firmware



Firmware Upgrade

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

Current Firmware Version on your router is **1.00(AMM.0)b2**

File Path:

The following table describes the labels in this screen.

Table 37 Maintenance > Tools > Firmware

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

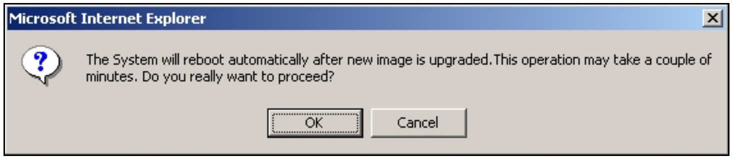
Do not turn off the ZyXEL Device while firmware upload is in progress!

19.1.1 Upgrading Firmware

The following steps describes the firmware upgrade process.

1. Specify the firmware file in the **Firmware Upgrade** screen and click **Upload** to start the file transfer process.
2. A warning screen displays as shown. Click **OK** to continue.

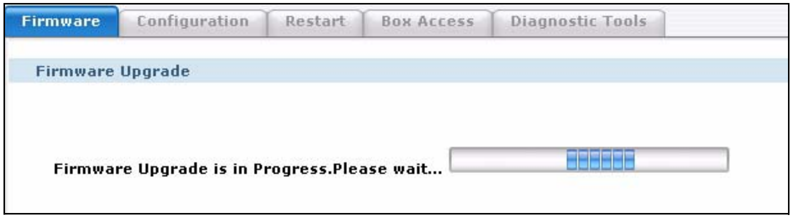
Figure 80 Firmware Upload: Warning



The System will reboot automatically after new image is upgraded.This operation may take a couple of minutes. Do you really want to proceed?

3. A status bar displays to indicate that the file transfer process is in progress.

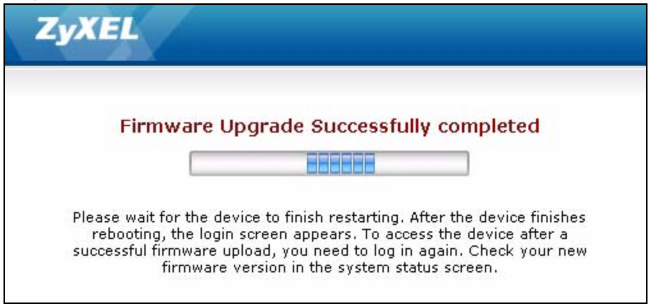
Figure 81 Firmware Upload: Progress Status



Firmware Upgrade is in Progress.Please wait...

4. After the file transfer is complete, the ZyXEL Device automatically reboots, in this time causing a temporary network disconnect. A warning screen displays as shown. Do NOT restart the ZyXEL Device at this point.

Figure 82 Firmware Upload: Reboot



Firmware Upgrade Successfully completed

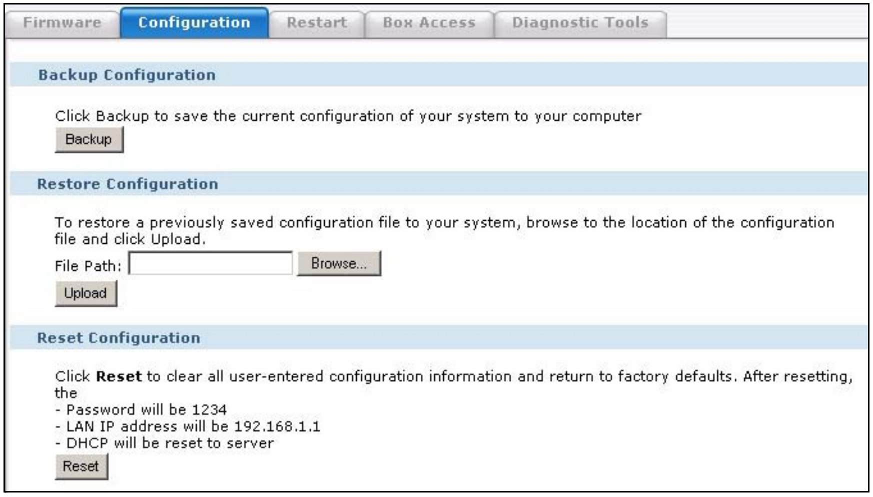
Please wait for the device to finish restarting. After the device finishes rebooting, the login screen appears. To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status screen.

5. After the ZyXEL Device finishes rebooting, the login screen displays. Otherwise, access the login screen again. Log in and check your new firmware version in the **Status** screen.

19.2 Configuration Screen

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

Figure 83 Maintenance > Tools > Configuration



Backup Configuration

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

Restore Configuration

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

File Path:

Reset Configuration

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

19.2.1 Backup Configuration

You can 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.

Click **Backup** and follow the on-screen instruction to save the ZyXEL Device's current configuration to your computer.

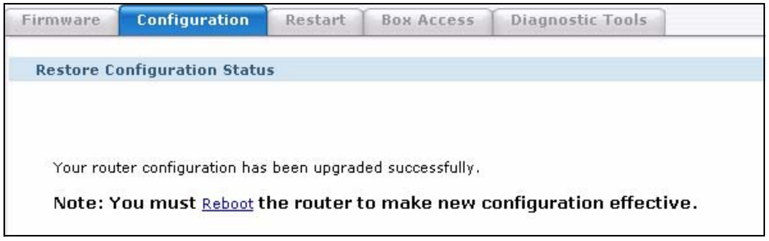
19.2.2 Restore Configuration

Follow the steps below to upload a previously saved configuration file from your computer to your ZyXEL Device.

1 Click **Maintenance** > **Tools** > **Configuration** and specify the configuration file in the **File Path** field. Or click **Browse** to locate it.

2 Click **Upload** to start the file transfer process. The following screen displays after the file transfer is complete. Click **Reboot** to have the ZyXEL Device restart to make the configuration file take effect.

Figure 84 Maintenance > Tools > Configuration: Upload



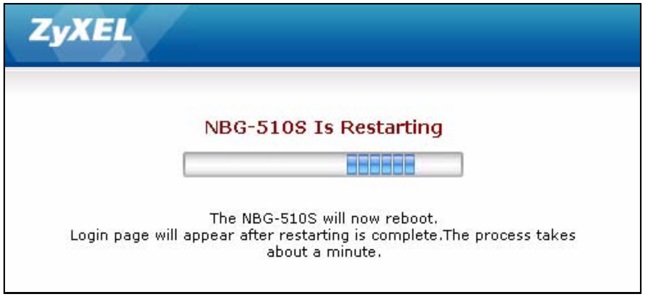
Restore Configuration Status

Your router configuration has been upgraded successfully.

Note: You must Reboot the router to make new configuration effective.

3 The following screen displays while the ZyXEL Device is restarting.

Figure 85 Maintenance > Tools > Configuration: Upload Restart



NBG-510S Is Restarting

The NBG-510S will now reboot.
Login page will appear after restarting is complete.The process takes about a minute.

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

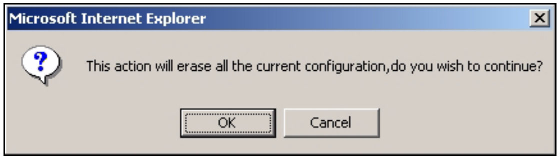
4 After the ZyXEL Device finishes rebooting, the login screen displays (you may need to refresh your browser to get it to appear). You may need to change the IP address of your computer to be in the same subnet as that of the ZyXEL Device LAN IP address (192.168.1.1).

19.2.3 Device Reset

You can use the **Configuration** screen to clear all your custom settings and return the ZyXEL Device to its factory defaults.

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

Figure 86 Reset Warning Message

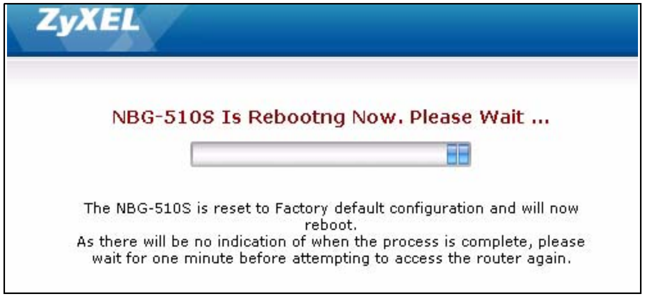


Microsoft Internet Explorer

This action will erase all the current configuration,do you wish to continue?

2 The following screen displays while the ZyXEL Device restarts.

Figure 87 Maintenance > Tools > Configuration: Reset Restart



NBG-510S Is Rebootng Now, Please Wait ...

The NBG-510S is reset to Factory default configuration and will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

Do NOT turn off the ZyXEL Device while it is restarting.

3 After the ZyXEL Device finishes rebooting, the login screen displays (you may need to refresh your browser to get it to appear). You may need to change the IP address of your computer to be in the same subnet as that of the default ZyXEL Device LAN IP address (192.168.1.1).

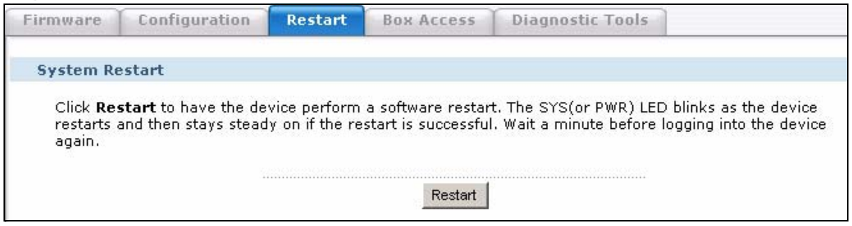
You can also press the ZyXEL Device’s physical **RESET** button to reset the factory defaults of your ZyXEL Device. Refer to Section 3.6 on page 38 for more information on the **RESET** button.

19.3 Restart Screen

System restart allows you to reboot the ZyXEL Device without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

Figure 88 Maintenance > Tools > Restart



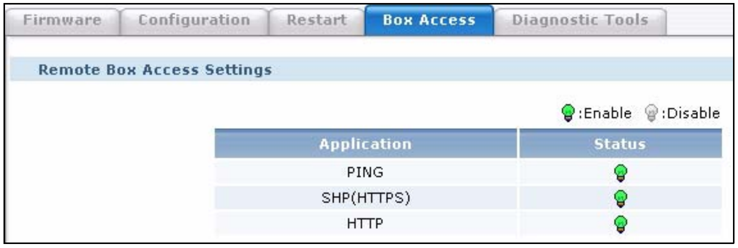
System Restart

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

19.4 Box Access Screen

Use this screen to set which services/protocols can access the ZyXEL Device from the WAN (the Internet). Click **Maintenance** > **Tools** > **Box Access** to open the screen as shown.

Figure 89 Maintenance > Tools > Box Access



Remote Box Access Settings

● :Enable ○ :Disable

Application	Status
PING	●
SHP(HTTPS)	●
HTTP	●

The following table describes the labels in this screen.

Table 38 Maintenance > Tools > Box Access

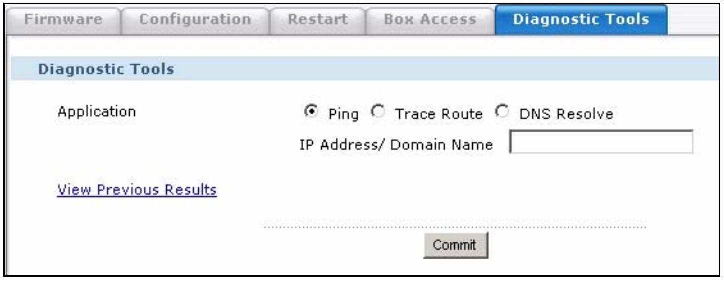
LABEL	DESCRIPTION
Application	This column lists services and protocols that can be used to access the ZyXEL Device from the Internet. **PING** is used to test whether or not a host can be reached. Enable this to have the ZyXEL Device respond to pings from the WAN. **SHP (HTTPS)** Enable this to allow web configurator and secure remote access from the WAN. Disable this option to block web configurator and secure remote access from the WAN. **HTTP** Enable this to allow web configurator management sessions from the WAN (you must also have **SHP (HTTPS)** enabled). If you have **SHP (HTTPS)** enabled, disable **HTTP** to block web configurator access from the WAN (secure remote access is still allowed.
Status	The **Status** icon displays whether or not the service is allowed to access the ZyXEL Device from the Internet. Click it to activate or deactivate the service.

19.5 Diagnostic Tools Screen

Use this screen to check connectivity to a website or computer on the Internet, check the Internet connection's behavior, and resolve a domain name's IP address.

Click **Maintenance** > **Tools** > **Diagnostic Tools** to open the screen as shown.

Figure 90 Maintenance > Tools > Diagnostic Tools



The following table describes the labels in this screen.

Table 39 Maintenance > Tools > Diagnostic Tools

LABEL	DESCRIPTION
Application	Select the diagnostic application that you want to use. **Ping** checks whether or not the ZyXEL Device can reach a device or website on the Internet. If you select this, enter the IP address of the device or domain name of the website. **Trace Route** checks the Internet connection's behavior. It shows the number of hops your data goes through to reach a specific IP address or website. If you select this, enter the IP address or domain name. **DNS Resolve** finds the IP address of a valid domain name. If you select this, enter the domain name.
View Previous Results	Click this link to see the existing test results (for earlier diagnostic tests). Note that you cannot see the earlier diagnostic results if you clicked **Clear** in the **Results** screen. Click **Back** in the **Results** screen to return to the **Diagnostic Tools** screen and still be able to see the results again later.

Table 39 Maintenance > Tools > Diagnostic Tools

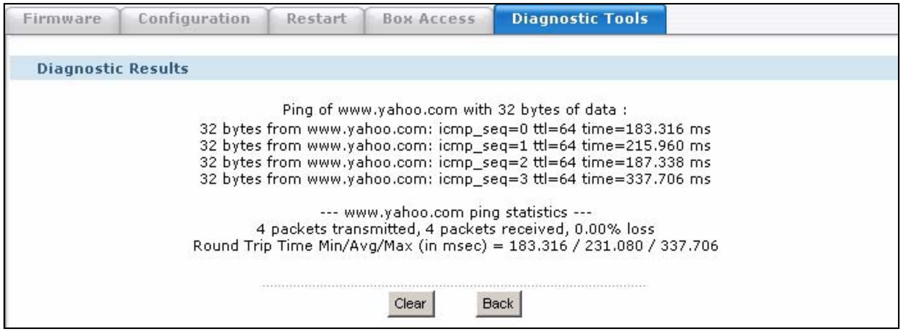
LABEL	DESCRIPTION
Commit	Click **Commit** to start the selected diagnostic test. Note: Previous results display along with the current results. You may need to wait a few seconds for the ZyXEL Device to perform the diagnostic test and display the current test's results.
Status	The **Status** icon displays whether or not the service is allowed to access the ZyXEL Device from the Internet. Click it to activate or deactivate the service.

19.5.1 Diagnostic Tools Ping Results

When the packets transmitted and packets received fields are greater than zero, there is a connection to the target IP address or domain name.

The data in the figure also shows the packet loss percentage in addition to minimum, maximum and average round trip times.

Figure 91 Maintenance > Tools > Diagnostic Tools > Ping Results



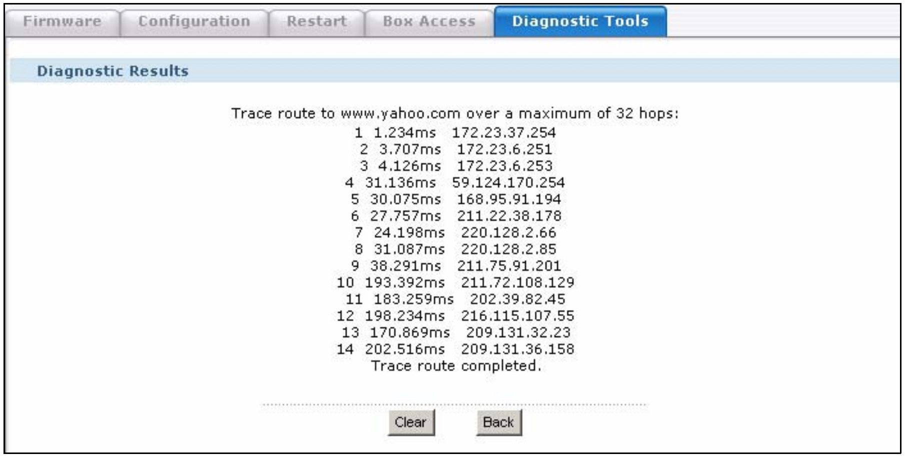
```
Ping of www.yahoo.com with 32 bytes of data :
32 bytes from www.yahoo.com: icmp_seq=0 ttl=64 time=183.316 ms
32 bytes from www.yahoo.com: icmp_seq=1 ttl=64 time=215.960 ms
32 bytes from www.yahoo.com: icmp_seq=2 ttl=64 time=187.338 ms
32 bytes from www.yahoo.com: icmp_seq=3 ttl=64 time=337.706 ms

--- www.yahoo.com ping statistics ---
4 packets transmitted, 4 packets received, 0.00% loss
Round Trip Time Min/Avg/Max (in msec) = 183.316 / 231.080 / 337.706
```

19.5.2 Diagnostic Tools Trace Route Results

The trace route results show each hop (device) the packet went through on the way to the target IP address or domain name and how long each hop took.

Figure 92 Maintenance > Tools > Diagnostic Tools > Trace Route Results

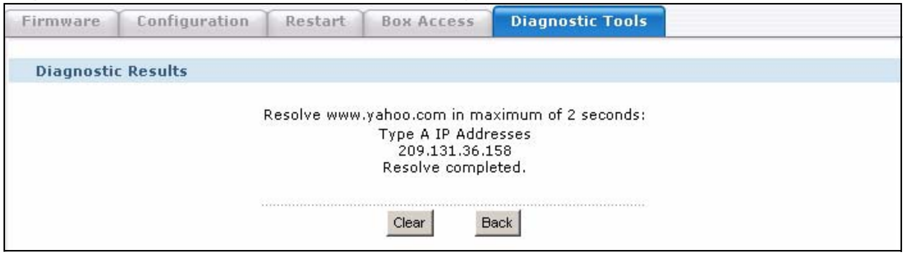


```
Trace route to www.yahoo.com over a maximum of 32 hops:
 1  1.234ms   172.23.37.254
 2  3.707ms   172.23.6.251
 3  4.126ms   172.23.6.253
 4  31.136ms  59.124.170.254
 5  30.075ms  168.95.91.194
 6  27.757ms  211.22.38.178
 7  24.198ms  220.128.2.66
 8  31.087ms  220.128.2.85
 9  38.291ms  211.75.91.201
10  193.392ms  211.72.108.129
11  183.259ms  202.39.82.45
12  198.234ms  216.115.107.55
13  170.869ms  209.131.32.23
14  202.516ms  209.131.36.158
Trace route completed.
```

19.5.3 Diagnostic Tools DNS Resolve Results

The DNS resolve results show which IP address the target domain name is using.

Figure 93 Maintenance > Tools > Diagnostic Tools > DNS Resolve Results



```
Resolve www.yahoo.com in maximum of 2 seconds:
Type A IP Addresses
209.131.36.158
Resolve completed.
```

PART VI
Secure Remote Access (User Portal)

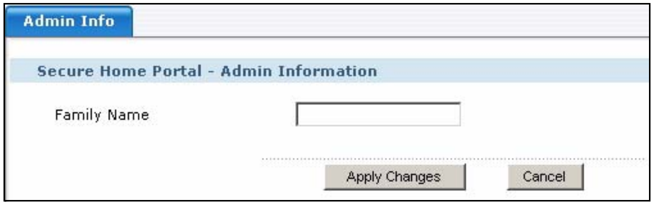
Secure Remote Access Title

This chapter describes how to configure the name the remote user sees in the secure remote access screens. See Section 6.1 on page 45 and Section 6.2 on page 45 for an overview of the secure remote access screens.

20.1 Configuring the Secure Remote Access Title

The user portal is the secure remote access screens that the remote user uses to access shared files or secure remote desktop connections. Click **User Portal > Admin Info** to open the following screen. Use this screen to configure the name that displays in the secure remote access screens.

Figure 94   User Portal > Admin Info



Admin Info

Secure Home Portal - Admin Information

Family Name

The following table describes the labels in this screen.

Table 40   User Portal > Admin Info

LABEL	DESCRIPTION
Family Name	Enter the name to be displayed on the top left corner of the user portal.
Apply Changes	Click **Apply Changes** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21

Secure Remote Access User Info

This chapter describes how to set up user accounts.

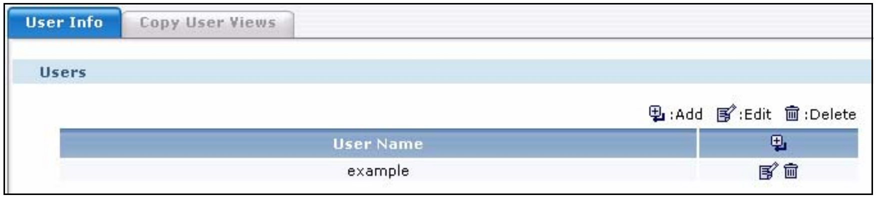
21.1 Overview

A user account allows a remote user to use the secure remote access (user portal) screens to access resources on the LAN. See Chapter 23 on page 143 to configure the collection of resources that the user can access (called the remote user's view).

21.2 User Info Screen

Click **Portal User > User Info** to open the following screen. This screen lists the remote user accounts.

Figure 95 User Portal > User Info



User Name	
example	

The following table describes the labels in this screen.

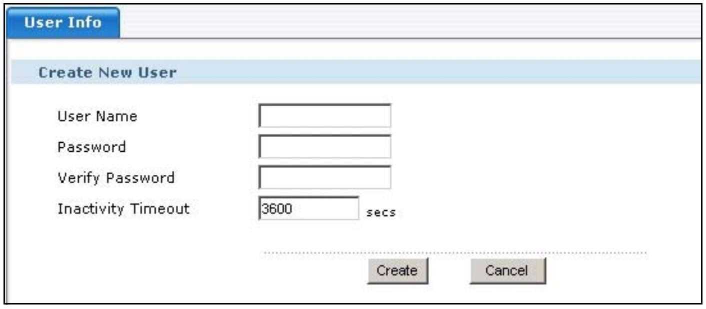
Table 41 User Portal > User Info

LABEL	DESCRIPTION
User Name	This field displays the user name of a user account.
Add icon	This column provides icons to add, edit, and remove users. Click the **Add** icon to go to the screen where you can add a user. Click the **Edit** icon to go to the screen where you can edit the user account. Click the **Delete** icon to remove a user account.

21.2.1 Add/Edit User Info Screen

Click the **Add** or **Edit** icon in the **Portal User > User Info** screen to open this screen. Use this screen to create a new or edit an existing user account.

Figure 96 User Portal > User Info > Add



User Name	
Password	
Verify Password	
Inactivity Timeout	3600 secs

The following table describes the labels in this screen.

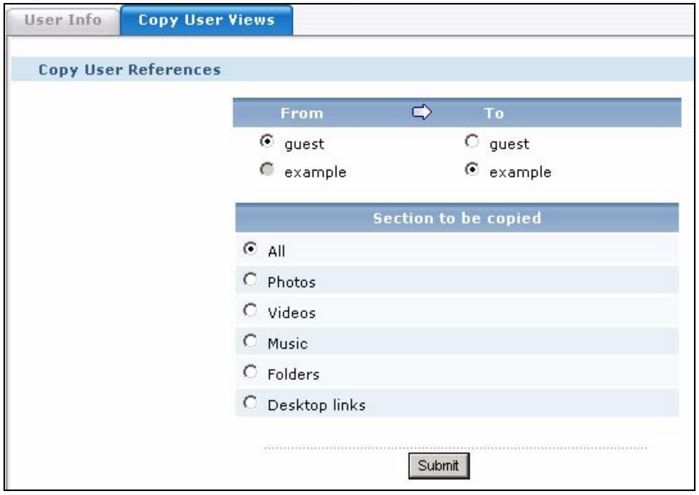
Table 42 User Portal > User Info > Add

LABEL	DESCRIPTION
User Name	Type the user name for this user account. Enter up to 16 alphanumeric characters, underscores (_), the at sign (@), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User account and user group names must be unique. Spaces are not allowed.
Password	Enter the password in the field. You can enter between 4 to 31 characters. Alphanumeric characters (0-9a-zA-Z) and `~!@#$%^&*()_-+={}|\;:'<,>./ characters are allowed. Spaces are not allowed.
Verify Password	Enter the password again.
Inactivity Timeout	Type how many minutes a secure remote access session can be left idle before timing out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Create/Modify	Click **Create** or **Modify** to create or edit the user account and return to the previous screen.
Cancel	Click **Cancel** to return to the previous screen without saving your changes.

21.3 Copy User Views Screen

Click **Portal User** > **Copy User Views** to open the following screen. Use this screen to copy a user's view (or sections of the view) to another user.

Figure 97 User Portal > Copy User Views



From	To
● guest	○ guest
○ example	● example

Section to be copied

● All
○ Photos
○ Videos
○ Music
○ Folders
○ Desktop links

The following table describes the labels in this screen.

Table 43 User Portal > User Info

LABEL	DESCRIPTION
From To	Select the port user with the view that you want to copy and to which portal user you want to copy it.
Sections to be copied	Select which parts of the portal user's view you want to copy to the other portal user.
Submit	Click **Submit** to modify the portal user's view.

22

Manage Accessible LAN Resources

This chapter describes how to manage the list of servers that remote users can access.

22.1 Manage Servers Overview

A user account allows a remote user to access resources on the LAN. Use the **Manage Servers** screens to list the servers that remote users can use after logging into the ZyXEL Device.

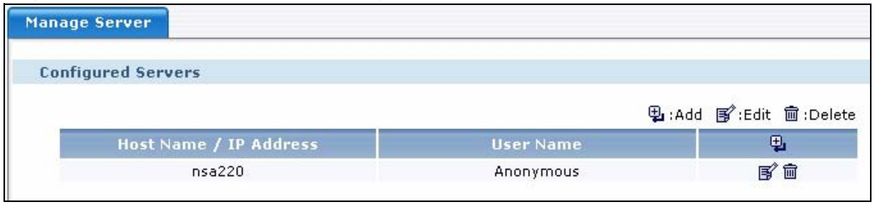
A server can be a LAN computer or network access storage device. For example:

- A Windows computer with some shared folders
- A Linux computer running samba server
- A network storage appliance (NSA) with shared folders (like the NSA-220)

22.2 Manage Servers Screen

Click **Portal User** > **Manage Servers** to open the following screen. This screen lists the servers that remote users can access.

Figure 98 User Portal > Manage Servers



Host Name / IP Address	User Name	
nsa220	Anonymous	

The following table describes the labels in this screen.

Table 44 User Portal > Manage Servers

LABEL	DESCRIPTION
Host Name / IP Address	This field displays the host name or IP address of a computer that you want to allow portal users to access.

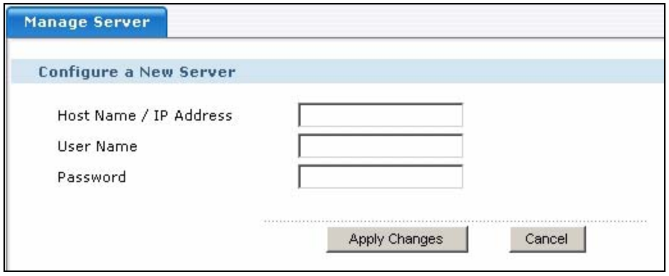
Table 44 User Portal > Manage Servers (continued)

LABEL	DESCRIPTION
User Name	This field displays the user name used to access the computer. **Anonymous** displays if a user name and password are not required to access the server.
Add icon	This column provides icons to add, edit, and remove server entries. Click the **Add** icon to go to the screen where you can add an entry. Click the **Edit** icon to go to the screen where you can edit the server entry. Click the **Delete** icon to remove a server entry.

22.2.1 Add/Edit Server Screen

Click the **Add** or **Edit** icon in the **Portal User** > **Manage Servers** screen to open this screen. Use this screen to create a new or edit an existing server entry.

Figure 99 User Portal > Manage Servers > Add



The following table describes the labels in this screen.

Table 45 User Portal > Manage Server > Add

LABEL	DESCRIPTION
Host Name / IP Address	Type the name of the computer or the computer's (static) IP address. Enter between 1 and 31 alphanumeric characters, underscores (_), the at sign (@), or dashes (-). This value is case-sensitive.
User Name	Enter the user name that you need to use to access the server. Enter between 1 and 31 alphanumeric characters, underscores (_), the at sign (@), or dashes (-), but the first character cannot be a number. This value is case-sensitive. Spaces are not allowed.
Password	Enter the password in the field. You can enter between 4 to 31 characters. Alphanumeric characters (0-9a-zA-Z) and `~!@#$%^&*()_-+={}|\;:'<,>./ characters are allowed.
Apply Changes	Click **Apply Changes** to create or edit the server entry and return to the previous screen.
Cancel	Click **Cancel** to return to the previous screen without saving your changes.

23

Manage User Access Permissions

This chapter describes how to manage the list of resources that each remote user can access.

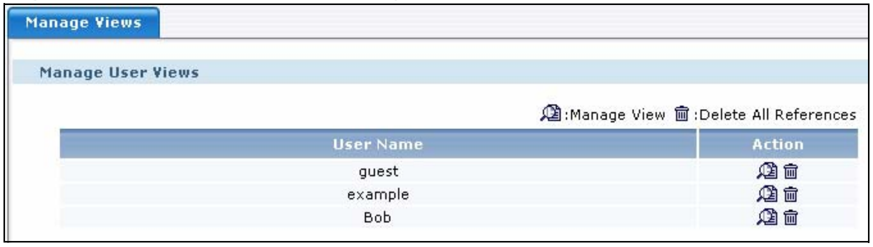
23.1 Manage Views Overview

A user account allows a remote user to access files on the LAN. Use the **Manage Views** screens to configure each user's view (the collection of resources that the user can access).

23.2 Manage Views Screen

Click **Portal User** > **Manage Views** to open the following screen. This screen lists the user accounts.

Figure 100 User Portal > Manage Views



User Name	Action
guest	
example	
Bob	

The following table describes the labels in this screen.

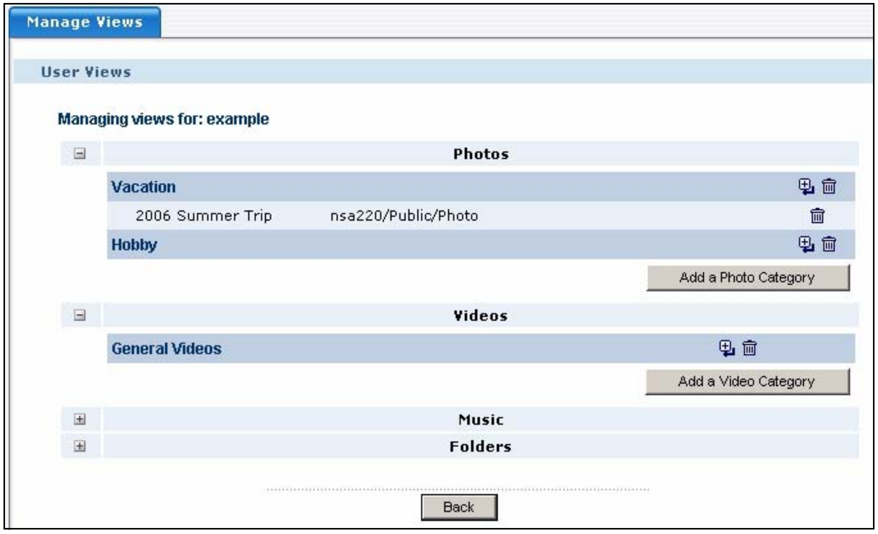
Table 46 User Portal > Manage Views

LABEL	DESCRIPTION
User Name	This field displays the user name of a secure remote access account. The guest account is a special default account that makes it easy to give a guest access to files (without having to configure a new account). The guest user name is "**guest**" and the password is "**guest123**". You cannot change them. Guest users can view, download, and upload files. For security reasons, desktop links not available to guest users.
Action	This column provides icons to edit or remove a user's view. Click the **Manage View** icon to go to the screen where you can edit the user's view. Click the **Delete All References** icon to remove a user's view (stop the user from using any of the portal's resources).

23.3 Manage a User’s View

Click the **Manage View** icon in the **Portal User > Manage Views** screen to open this screen. Use this screen to manage the user’s view (what the user can access).

Figure 101 User Portal > Manage Views > Manage View



Manage Views

User Views

Managing views for: example

Photos

Vacation

2006 Summer Trip nsa220/Public/Photo

Hobby

Videos

General Videos

Music

Folders

The following table describes the labels in this screen.

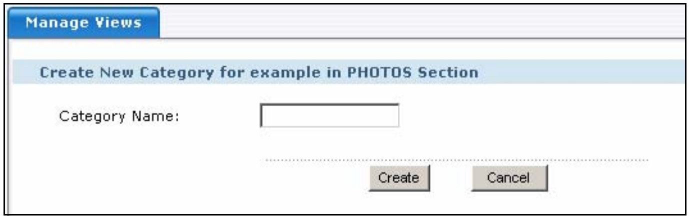
Table 47 User Portal > Manage Views > Manage View

LABEL	DESCRIPTION
User Views	This screen is divided into photos, videos, music and folders sections. For any section, you first have to create a category and then references within the category. The categories are like albums and the references within the category are like individual photos in an album. You can create more than one category in each section and more than one reference in each category.
+/-	Click the **+** icon to show display a section’s categories and button for adding categories. Click the **-** icon to collapse the view.
Add a .... Category	Click **Add a .... Category** to create a category within that section.
Add icon	This column provides icons to add and remove server entries. Click the **Add new reference** icon to go to the screen where you can add a reference. Click the **Remove this category** icon to delete a category. Click the **Delete** icon to remove a reference.
Back	Click **Back** to return to the previous screen.

23.4 Add a Category

From the screen for managing a user’s view, click **Add a .... Category** to open the following screen. Use this screen to create a new category.

Figure 102 User Portal > Manage Views > Manage View > Add a .... Category



The following table describes the labels in this screen.

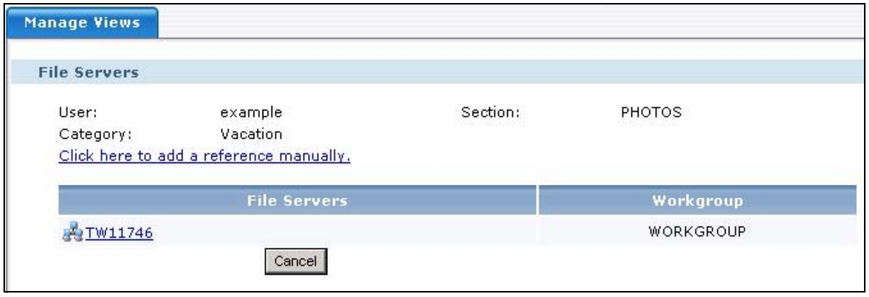
Table 48 User Portal > Manage Views > Manage View > Add a .... Category

LABEL	DESCRIPTION
Category Name	Enter a unique name to identify the category. Enter between 1 and 31 alphanumeric characters, underscores (_), the at sign (@), or dashes (-), but the first character cannot be a number.
Create	Click **Create** to create the category account and return to the previous screen.
Cancel	Click **Cancel** to return to the top-level **Manage Views** screen without saving your changes.

23.5 Adding a Reference

From the screen for managing a user's view, click a category's **Add new reference** icon to open the following screen. Use this screen to specify the files that the category is to contain. You must create a separate reference (link) for each individual file.

Figure 103 User Portal > Manage Views > Manage View > Add Reference



User: example Section: PHOTOS
Category: Vacation
Click here to add a reference manually.

File Servers	Workgroup
TW11746	WORKGROUP

The following table describes the labels in this screen.

Table 49 User Portal > Manage Views > Manage View > Add Reference

LABEL	DESCRIPTION
User	This field displays the secure remote access account's user name.
Section	This field displays the name of the section that you are working in.
Category	This field displays the name of the category to which you are adding a reference.
Click here to a add a reference manually.	Click this link to select the server to use and manually specify a server and the file path of the file. You must have already manually added the server in the **Manage Server** screen (see Section 22.2 on page 141 for details).
File Servers	This field displays the host names of computers that the ZyXEL Device detects on the network.

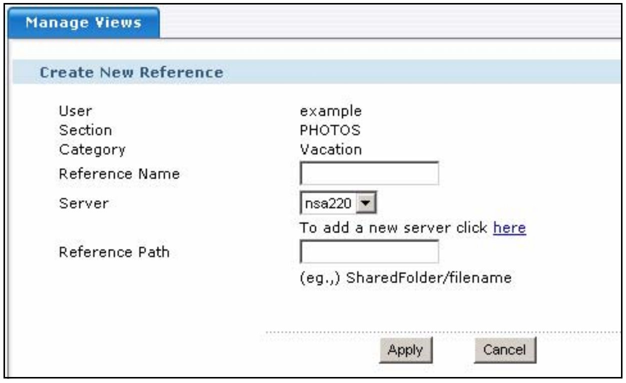
Table 49 User Portal > Manage Views > Manage View > Add Reference (continued)

LABEL	DESCRIPTION
Workgroup	This field displays the name of the workgroup to which the computer belongs. A workgroup is a group of computers on a network that can share files.
Cancel	Click **Cancel** to return to the top-level **Manage Views** screen without saving your changes.

23.5.1 Adding a Reference: Manually

When adding a reference, click **Click here to a add a reference manually.** to open the following screen. Use this screen to specify the file path of the file.

Figure 104 User Portal > Manage Views > Manage View > Add Reference > Manually



Create New Reference

User example
Section PHOTOS
Category Vacation
Reference Name
Server nsa220
To add a new server click here
Reference Path
(eg.,) SharedFolder/filename

The following table describes the labels in this screen.

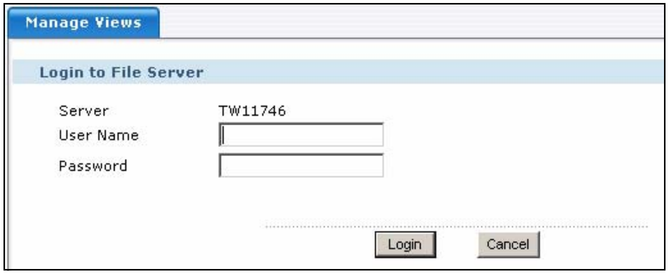
Table 50 User Portal > Manage Views > Manage View > Add Reference > Manually

LABEL	DESCRIPTION
User	This field displays the secure remote access account's user name.
Section	This field displays the name of the section that you are working in.
Category	This field displays the name of the category to which you are adding a reference.
Reference Name	Specify the name for the reference. This appears as a link that the portal user can click to open the associated file. It works like a title for the referenced file.
Server	Select the server where the file is located. Click the **here** link if you need to go to the screen where you add servers (see Section 22.2 on page 141 for details).
Reference Path	Type the full file path for the file that you want to add. Make sure you include the full path from the shared folder to the file extension.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to return to the top-level **Manage Views** screen without saving your changes.

23.5.2 Adding a Reference: File Server Login

When adding a reference, you can click a file server's link to browse the computer's shared folders. Use this screen to configure the user name and password for logging into the server's shared folder.

Figure 105 User Portal > Manage Views > Manage View > Add Reference > Configure Login



Server TW11746
User Name
Password

The following table describes the labels in this screen.

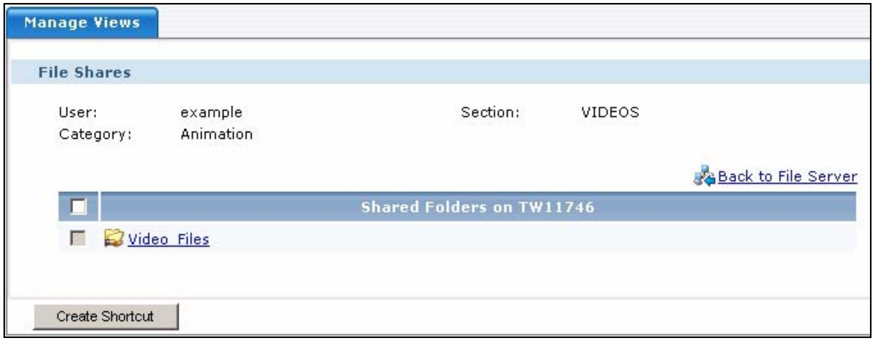
Table 51 User Portal > Manage Views > Manage View > Add Reference > Configure Login

LABEL	DESCRIPTION
Server	This is the server where the file is located.
User Name	Enter the user name that you need to use to access the shared folder on the server. Enter between 1 and 31 alphanumeric characters, underscores (_), the at sign (@), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Password	Enter the password in the field. You can enter between 4 to 64 characters. Alphanumeric characters (0-9a-zA-Z) and `~!@#$%^&*()_-+={}|\;:'<,>./ characters are allowed.
File Servers	This field displays the host names of computers on the network that you have configured as servers for the ZyXEL Device. Click a computer's link to browse the computer's shared contents.
Login	Click **Login** to have the ZyXEL Device try to log into the server.
Cancel	Click **Cancel** to return to the top-level **Manage Views** screen without saving your changes.

23.5.3 Adding a Reference: Browsing the Shared Folders

When adding a reference, click a file server's link to browse the computer's shared folders. After you have configured the user name and password for accessing the server's shared folder, use this screen to select the shared folder containing the files for which you want to add references.

Figure 106 Adding a Reference: Browsing the Shared Folders



User: example
Category: Animation
Section: VIDEOS

The following table describes the labels in this screen.

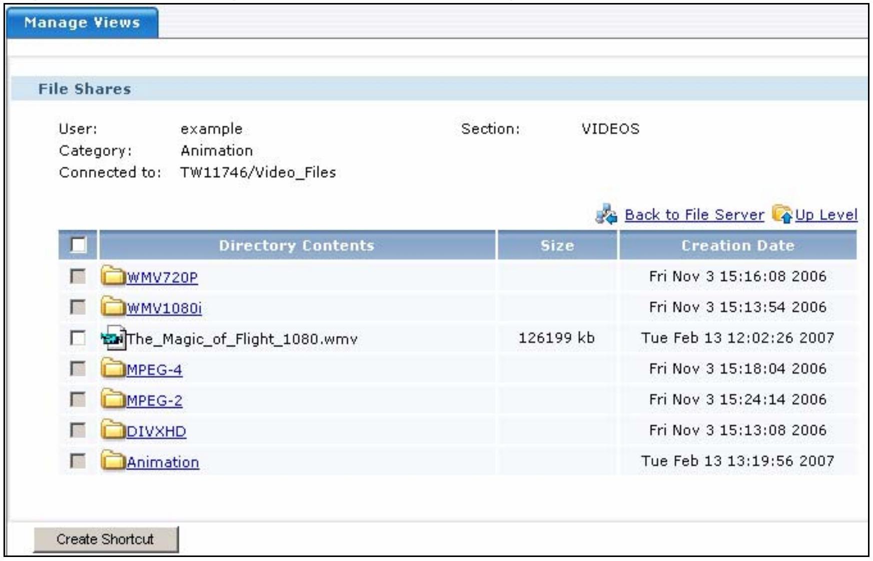
Table 52 Adding a Reference: Browsing the Shared Folders

LABEL	DESCRIPTION
User	This field displays the secure remote access account’s user name.
Section	This field displays the name of the section that you are working in.
Category	This field displays the name of the category to which you are adding a reference.
Back to File Server	Click this to return to the screen where you select which computer the files are on.
Shared Folders On	This lists the shared folders on the selected computer. Click a folder’s link to see its contents.
Create Shortcut	When you are in a screen with files that you can share, select the check boxes next to the files that you want to share and click **Create Shortcut** to make them accessible to the portal user.

23.5.4 Adding a Reference: Browsing the Shared Folder Contents

After you have selected a shared folder on the server, use these screens to select the files for which to add references.

Figure 107 Adding a Reference: Browsing the Shared Folder Contents



File Shares

User: example

Section: VIDEOS

Category: Animation

Connected to: TW11746/Video_Files

□	Directory Contents	Size	Creation Date
□	WMV720P		Fri Nov 3 15:16:08 2006
□	WMV1080i		Fri Nov 3 15:13:54 2006
□	The_Magic_of_Flight_1080.wmv	126199 kb	Tue Feb 13 12:02:26 2007
□	MPEG-4		Fri Nov 3 15:18:04 2006
□	MPEG-2		Fri Nov 3 15:24:14 2006
□	DIVXHD		Fri Nov 3 15:13:08 2006
□	Animation		Tue Feb 13 13:19:56 2007

The following table describes the labels in this screen.

Table 53 Adding a Reference: Browsing the Shared Folder Contents

LABEL	DESCRIPTION
User	This field displays the secure remote access account’s user name.
Section	This field displays the name of the section that you are working in.
Category	This field displays the name of the category to which you are adding a reference.
Back to File Server	Click this to return to the screen where you select which computer the files are on.
Up Level	Click this to go to the next higher layer in the shared folder’s tree.
Directory Contents	This lists the folders and files in the shared folder. Click a sub-folder’s link to see its contents. Select the files that you want to add for the user.

Table 53 Adding a Reference: Browsing the Shared Folder Contents (continued)

LABEL	DESCRIPTION
Size	This lists the size of the file.
Creation Date	This lists the date and time that a folder was created or a file was last modified.
Create Shortcut	Select the check boxes next to the files that you want to add and click **Create Shortcut** to make them accessible to the portal user.

24

Secure Remote Desktop Control

This chapter describes how to configure the ZyXEL Device to allow remote users to manage LAN computers.

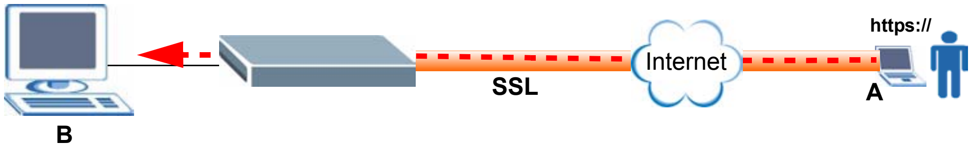
24.1 Desktop Links Overview

The ZyXEL Device's desktop link policies allow remote users to use remote desktop connections to securely manage LAN computers. The remote user can control and work on the LAN computer as if he was actually there. He can install (or remove) software, run programs, change settings, open, copy, create, and delete files.[1] This remote management can be used for troubleshooting, support, and administration, and also for remote access to files and programs. Since several users can simultaneously connect to the same computer, it is also perfect for education and team-based work.

The LAN computer to be managed and the remote user's computer must both have VNC (Virtual Network Computing) or RDP (Remote Desktop Protocol) software installed. The server software must be on the LAN computer to be managed and the client software must be on the remote user's computer.

In the following figure, user A uses his user account to log into the ZyXEL Device. Then he uses the Real VNC client on his computer to manage LAN computer B. The connection between the remote user and the ZyXEL Device is secured by an SSL tunnel.

Figure 108 SSL-protected Remote Management

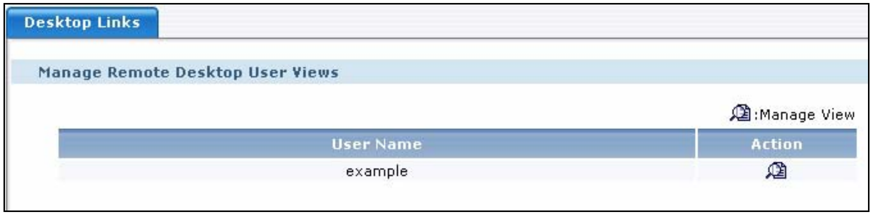


24.2 Desktop Links Screen

Click **Portal User > Desktop Links** to open the following screen. This screen lists the user accounts. See Section 6.2 on page 45 for an example of using the secure remote desktop management connection.

[1] The actual functions available depends on your remote desktop software. Not all remote desktop software versions support all of the functions listed.

Figure 109 User Portal > Desktop Links



User Name	Action
example	

The following table describes the labels in this screen.

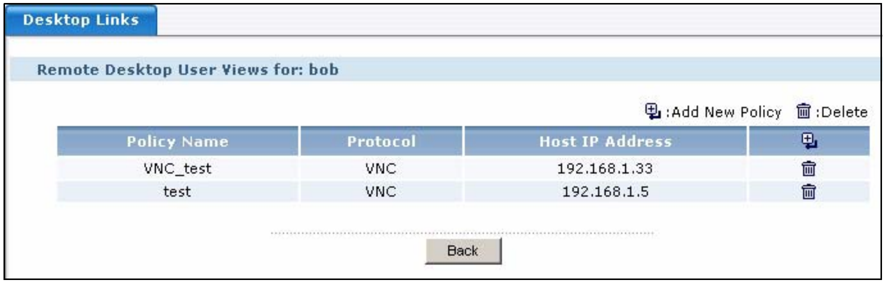
Table 54 User Portal > Desktop Links

LABEL	DESCRIPTION
User Name	This field displays the user name of a (remote) user account.
Action	Click the **Manage View** icon to go to the screen where you can edit the list of LAN computers that the user can manage.

24.3 Manage a User's Desktop Links View

Click the **Manage View** icon in the **Portal User > Desktop Links** screen to open this screen. Use this screen to manage the list of policies for LAN computers the remote user can manage.

Figure 110 User Portal > Desktop Links > Manage View



Policy Name	Protocol	Host IP Address	
VNC_test	VNC	192.168.1.33	
test	VNC	192.168.1.5	

The following table describes the labels in this screen.

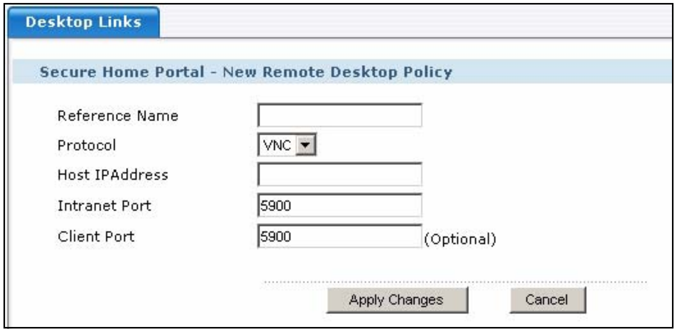
Table 55 User Portal > Desktop Links > Manage View

LABEL	DESCRIPTION
Policy Name	This displays the name you entered to identify which computer this policy allows the portal user to manage.
Protocol	This is the protocol of the remote desktop software the LAN computer is using.
Host IP Address	This field displays the IP address of the computer that you want to allow the portal user to manage.
Add icon	This column provides icons to add and remove server entries. Click the **Add new policy** icon to go to the screen where you can add a desktop link. Click the **Delete** icon to remove a desktop link entry.
Back	Click **Back** to return to the previous screen.

24.4 Add Desktop Link Screen

Click the **Add** or **Edit** icon in the **User Portal > Desktop Links > Manage View** screen to open this screen. Use this screen to create a new or edit an existing server entry.

Figure 111 User Portal > Desktop Links > Manage View > Add



Secure Home Portal - New Remote Desktop Policy

Reference Name	
Protocol	VNC
Host IPAddress	
Intranet Port	5900
Client Port	5900 (Optional)

The following table describes the labels in this screen.

Table 56 User Portal > Desktop Links > Manage View > Add

LABEL	DESCRIPTION
Reference Name	Specify the name for the link that the portal user can click to connect to the associated computer.
Protocol	Select the protocol of the remote desktop server software on the LAN computer to be managed. **VNC** stands for Virtual Network Computing. **RDP** stands for Remote Desktop Protocol. Note: The remote desktop client software on the remote user's computer must use the same protocol as the remote desktop server software on the LAN computer.
Host IP Address	Type the computer's (static) IP address.
Intranet Port	This is the listening port of the LAN computer running the server version of the remote desktop software. The ZyXEL Device uses this port number to send traffic to the LAN computer that is being remotely managed.
Client Port	This is the sending port of the authorized remote computer with the client version of the remote desktop software installed. The remote computer uses this port number to communicate with the ZyXEL Device. If the remote computer is also running server remote desktop software, ensure that it uses a different port number.
Apply Changes	Click **Apply Changes** to create the entry and return to the previous screen.
Cancel	Click **Cancel** to return to the previous screen without saving your changes.

25

Secure Remote Access Screens

This chapter describes how to access and use the ZyXEL Device secure remote access screens (also called the secure remote access portal or user portal).

25.1 Secure Remote Access Screens

Remote users use the secure remote access portal screens to access shared files, upload files, or manage LAN computers.

25.1.1 System Requirements

The following lists the browser and computer system requirements for remote user access.

- Internet Explorer 5 (administrator login only), 6.0, or 7.0
- Netscape Navigator 7.2
- Mozilla 1.7.13,
- FireFox 1.5.0.9 or 2.0.
- Java Runtime Environment (JRE) 1.5.0 or later must be installed to access Desktop links. It also must be enabled in your browser. Java does not need to be installed for accessing other links like photos, videos, music and files.
- Web browser pop-up windows allowed. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript allowed (these are usually enabled by default).
- Java permissions allowed (these are usually enabled by default).

25.2 Logging into the Secure Remote Access Screens

Accessing the secure remote access screens works in the same way as accessing the web configurator screens except that you use a user account's user name and password (instead of the administrator user name and password). If you are connecting through the Internet, connect to the ZyXEL Device's WAN IP address or domain name (DDNS lets the ZyXEL Device use a domain name even with a dynamic WAN IP address). The recommended screen resolution is 1024 by 768 pixels.

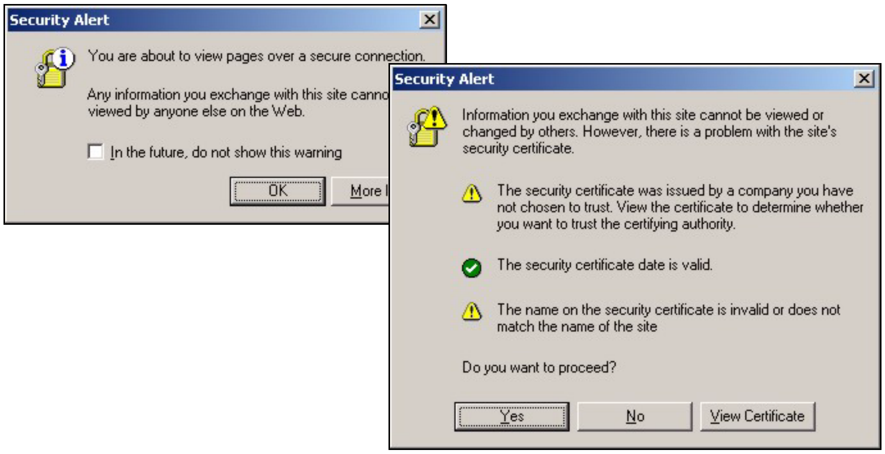
25.2.1 Logging into the Secure Remote Access Screens Example

1 Open Internet Explorer (or another supported web browser).

- If you are on the ZyXEL Device's LAN, enter the ZyXEL Device's LAN IP address (http://192.168.1.1 default).
- If you are connecting through the Internet, enter the ZyXEL Device's WAN IP address or domain name (DDNS lets the ZyXEL Device use a domain name even with a dynamic WAN IP address).

2 A security alert and/or certificate screen displays. Click **OK** and/or **Yes** to continue.

Figure 112 Login: Security Message



Security Alert

You are about to view pages over a secure connection.

Any information you exchange with this site canno viewed by anyone else on the Web.

□ In the future, do not show this warning

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

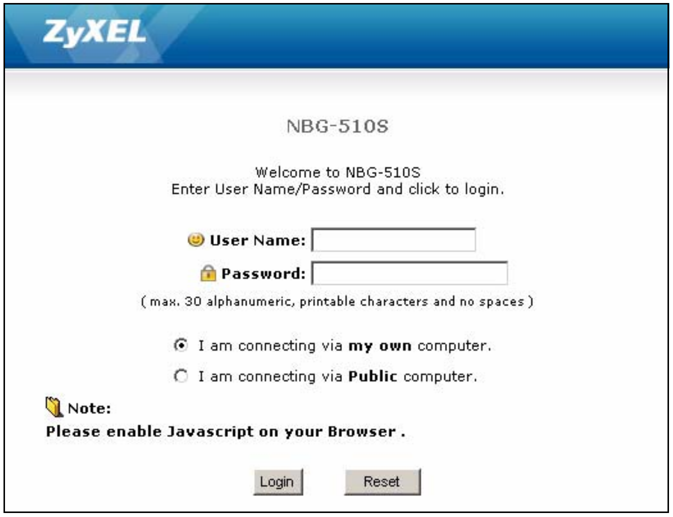
3 The **Login** screen appears. Enter your user account's user name and password (remember to use the correct case).

- Guests can use "**guest**" as the user name and "**guest123**" as the password. See Table 46 on page 143 for more about the guest account.
- If you are using a computer that is also used by others, select **I am connecting via public computer**. Your web browser cache will be automatically cleaned once you terminate the connection. This prevents anyone from obtaining information from the browser cache.

It is best to make secure remote connections to your ZyXEL Device from your own computer or a "trusted" computer since public computers may contain key loggers, trojans, sniffers, or phishing activity.

- If you are using your computer to access the ZyXEL Device, select **I am connecting via my own computer**. Your web browser cache will not be cleaned after you log out.

Figure 113 Login: Enter Account Information



NBG-510S

Welcome to NBG-510S
Enter User Name/Password and click to login.

User Name:

Password:

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

● I am connecting via **my own** computer.

○ I am connecting via **Public** computer.

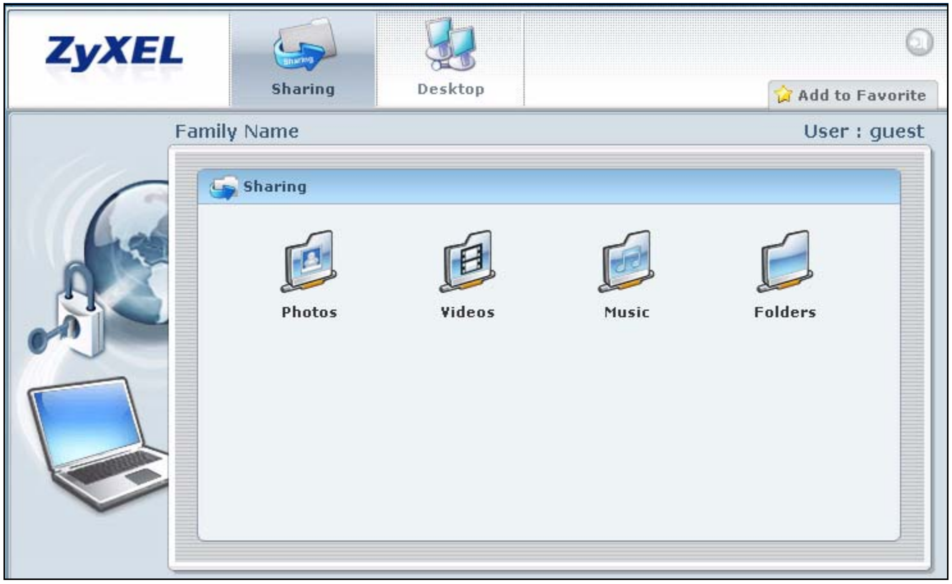
Note:
Please enable Javascript on your Browser .

The ZyXEL Device logs you out if your secure remote access session is idle for longer than the idle timeout set for your account (see Section 21.2.1 on page 137). Just log back in if this happens.

25.3 Secure Remote Access Screens Overview

This is the first secure remote access portal screen you see after login.

Figure 114 Main Secure Remote Access Screen



The icons and language label at the top-right of the screen (1) are visible from most screens. Use the tabs at the top of the screen to navigate the secure remote access screens. The following table describes the ‘global’ icons and tabs in the secure remote access portal screens.

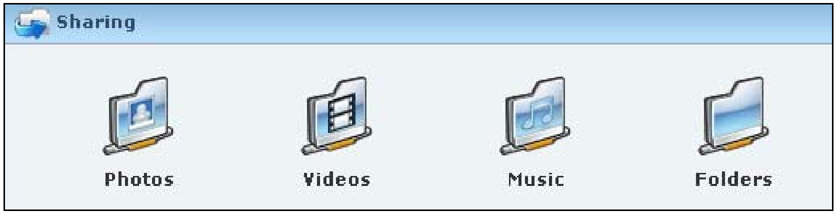
Table 57 Secure Remote Access Global Labels and Icons

LABEL/ICON	DESCRIPTION
⏻	Click the **Logout** icon at any time to exit the web configurator. This is the same as clicking the **Logout** link at the bottom of the Navigation panel. Note: Always use the **Logout** icon to exit the web configurator.
Add to Favorite	Click this to add the secure remote access portal screen to your browser’s favorites list.
Sharing	Click this tab to go to screens where you can access and upload files.
Desktop	Click this tab to go to screens that list computers that you can manage using VNC or RDP software. Note: For security reasons, desktop links are only available to users with an account (not guest users).

25.4 Secure Remote Access Sharing Screen

Click **Sharing** to open the main **Sharing** screen. This screen displays the categories of files that you can access. Click a folder icon to access files in that category. You can also upload files in the **Folders** screens.

Figure 115 Sharing

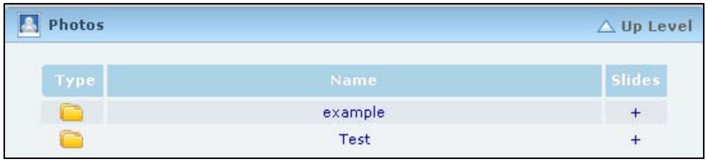


25.5 Secure Remote Access File Browsing

This example shows how the remote user can navigate through the files to which he has access.

Click **Sharing** > **Photos** to open the following screen.

Figure 116 Secure Remote User File Browsing



Type	Name	Slides
📁	example	+
📁	Test	+

The following table describes the labels in this screen.

Table 58 Secure Remote User File Browsing

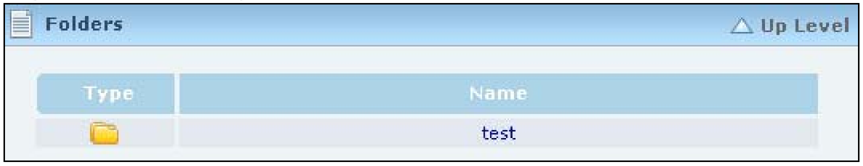
LABEL	DESCRIPTION
Up Level	Click this to go up one level in the folder tree.
Type	The icon in this column identifies the entry as a folder or a file.
Name / File Name	This column identifies the names of folders or files in the category. Click a folder's name to display the folder's contents. Click a file's file name to open the file.
Slides	Click the icon to display a slideshow of the photos.

25.6 File Uploading

This example shows how the remote user can upload files to a folder which he has access.

1 Click **Sharing** > **Folders** to open the following screen. This screen is the equivalent of the **Folder Category** in the user's view (see Chapter 23 on page 143 for how to manage the user's view). Click the link for the folder containing the folder into which you want to upload files (**test** in this example).

Figure 117 Sharing > Folders

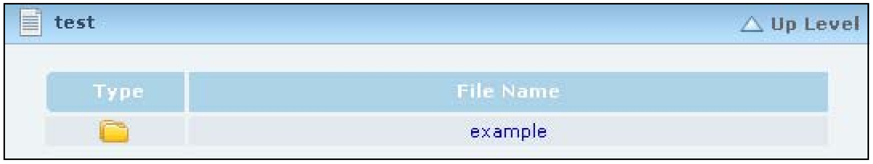


Folders

Type	Name
📁	test

2 This screen shows the individual references in the user's view (see Chapter 23 on page 143 for how to manage the user's view). Click the name of the individual folder to which you want to upload files (**example** here).

Figure 118 Sharing > Folders > Folder

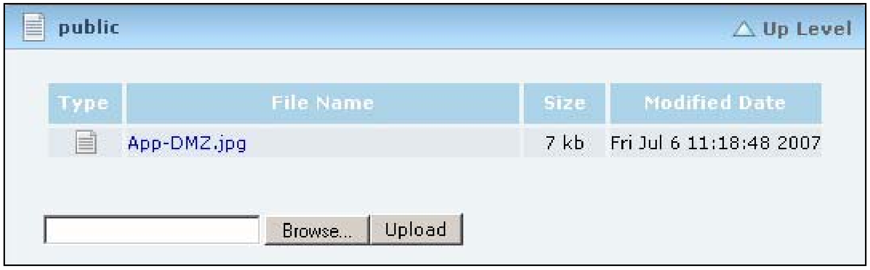


test

Type	File Name
📁	example

3 This screen shows the files already available to the user in this reference. The file sizes and when they were last modified also display. Click **Browse**. and select the file you want to upload. Then click **Upload** to upload the file.

Figure 119 Sharing > Folders > Folder > Folder

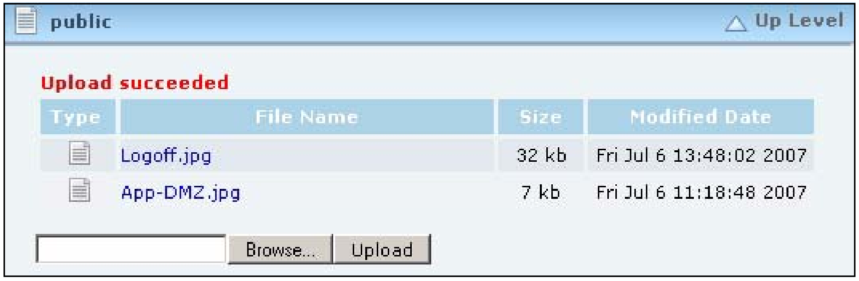


public

Type	File Name	Size	Modified Date
📄	App-DMZ.jpg	7 kb	Fri Jul 6 11:18:48 2007

4 The file displays in the screen after the upload finishes. The file is now available to the other secure remote access users with user views configured to access this reference.

Figure 120 File Uploaded



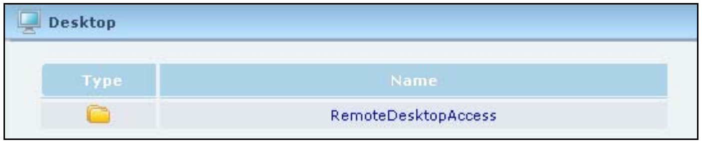
Upload succeeded

Type	File Name	Size	Modified Date
	Logoff.jpg	32 kb	Fri Jul 6 13:48:02 2007
	App-DMZ.jpg	7 kb	Fri Jul 6 11:18:48 2007

25.7 Desktop Screen

Click the **Desktop** link at the top of the screen to open the main **Desktop** screen. The remote user uses this screen to find information on the LAN computers behind the ZyXEL Device that he can manage.

Figure 121 Desktop Main Screen



Type	Name
	RemoteDesktopAccess

The following table describes the labels in this screen.

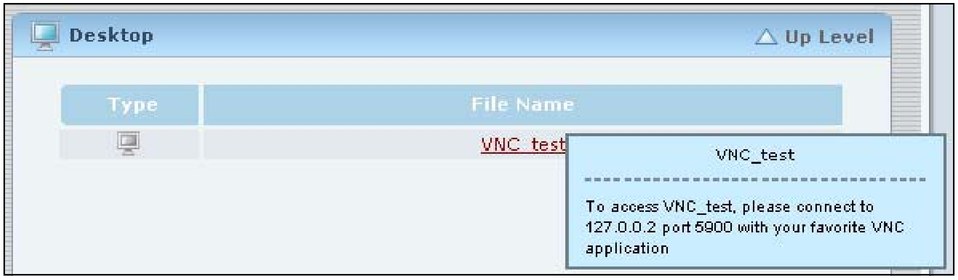
Table 59 Desktop Main Screen

LABEL	DESCRIPTION
Type	The icon in this column identifies the entry as a folder.
Name	Click **RemoteDesktopAccess** to display the references to use to manage LAN computers using VNC/ RDP software.

25.8 Desktop Links

Click **Desktop > RemoteDesktopAccess** to open the following screen. A remote user gets information from this screen to manage the LAN computer represented by a link in the screen. See Section 6.2 on page 45 for an example of using the secure remote desktop management connection.

Figure 122 Desktop Links



VNC_test

To access VNC_test, please connect to 127.0.0.2 port 5900 with your favorite VNC application

The following table describes the labels in this screen.

Table 60 Desktop Links

LABEL	DESCRIPTION
Up Level	Click this to go up one level in the folder tree.
Type	The icon in this column identifies the entry as a computer that you can manage.
File Name	Roll your mouse over a link to open a tool tip with the loopback IP address and port number to use in your VNC or RDP client program to connect to the LAN computer. Refer to your VNC or RDP program's documentation for details. The remote user must: • Enter the loopback IP address and port number in his VNC or RDP client program. • Stay logged into the ZyXEL Device's secure remote access portal. • Make sure his computer is not running a remote desktop server on the same port number.

PART VII

Troubleshooting and Appendices

26

Troubleshooting

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

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access

26.1 Power, Hardware Connections, and LEDs

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

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

2 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.

3 Disconnect and re-connect the power adaptor or cord to the ZyXEL Device.

4 If the problem continues, contact the vendor.

? One of the LEDs does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Section 2.2 on page 31.

2 Check the hardware connections. See the Quick Start Guide or Section 2.1 on page 31.

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

4 Disconnect and re-connect the power adaptor to the ZyXEL Device.

5 If the problem continues, contact the vendor.

26.2 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. Use the console port to log in to the ZyXEL Device.
3. 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.
4. If this does not work, you have to reset the device to its factory defaults. See Section 3.6 on page 41.

I forgot the password.

1. The default administrator login password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 3.6 on page 41.

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, 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 the Quick Start Guide or Section 2.1 on page 31.
3. Make sure you are using a supported web browser and that the web browser does not block pop-up windows and has JavaScripts and Java enabled.
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. 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.
5. Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 3.6 on page 41.

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

Advanced Suggestions

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

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

1. Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
2. The **Maintenance > Tools** > **Box Access** screen must have HTTP enabled for you to be able to log into the web configurator's management session from the WAN.
3. If the ZyXEL Device is behind a firewall or NAT router, make sure you configure port forwarding or a firewall rule to allow traffic to the ZyXEL Device on TCP port 8443 for administration connections and TCP port 443 for secure remote access connections.
4. You cannot log in to the web configurator while someone is already logged in using the same account. Ask the person who is logged in to log out.
5. Disconnect and re-connect the power adaptor or cord to the ZyXEL Device.
6. If this does not work, you have to reset the device to its factory defaults. See Section 3.6 on page 41.

Login fails. The **Login** screen says I am already logged in from this computer.

1. If you still have the logged in browser session open, log out.
2. If you already closed the browser session (without logging out), wait for your session to timeout or restart the ZyXEL Device.

26.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide or Section 29.1 on page 175.

2 If you deploy the ZyXEL Device as a new gateway, make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you connect the ZyXEL Device behind another gateway, make sure the WAN connection is up.

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

5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the 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 the Quick Start Guide or Section 29.1 on page 175.

2 Disconnect and re-connect the power adaptor to the ZyXEL Device to restart the device.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 29.1 on page 175. 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 Check the signal strength. If the signal strength is low, try moving the ZyXEL Device closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 Disconnect and re-connect the power adaptor to the ZyXEL Device to restart the device.

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

26.4 Reset the ZyXEL Device to Its Factory Defaults

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

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

To reset the ZyXEL Device,

1. Make sure the **PWR** LED is on and not blinking.
2. Use a pointed object to press the **RESET** button in for five seconds and release it.

If the ZyXEL Device restarts automatically, wait for the ZyXEL Device to finish restarting, and log in to the web configurator. The LAN IP address is 192.168.1.1. The user name is “**admin**”. The password is “**1234**”.

If the ZyXEL Device does not restart automatically, disconnect and reconnect the ZyXEL Device’s power. Then, follow the directions above again.

A

Product Specifications

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

Table 61 Hardware Specifications

Dimensions	190(W) x 150 (D) x 33 (H) mm
Ethernet Ports	5 auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
Operation Environment	Temperature: 0º C ~ 50º C Humidity: 20% ~ 95% RH non-condensing
Storage Environment	Temperature: -20º C ~ 60º C Humidity: 20% ~ 95% RH non-condensing
External Antenna	One detachable 2 dBi (maximum) antenna
Wireless LAN Output Power	IEEE 802.11b = 15 dBm IEEE 802.11g = 18 dBm
Screw size for wall mounting	M 3*10
Approvals	Safety CSA 60950-1, IEC 60950-1, EN 60950-1, ANSI/UL 60950-1 EMI EN 61000-3-2, EN 61000-3-3, FCC Part 15B EMS FCC Part15C, CE EN 300328, CE EN 301 489-1, CE 301 489-17

Table 62 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Login User Name	admin
Default Password	1234
DHCP Pool	32 addresses, starting at 192.168.1.33
Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!

Table 62 Firmware Specifications

FEATURE	DESCRIPTION
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.
SSL	Your ZyXEL Device provides an end-to-end Secure Socket Layer based connection that allows remote users to securely and easily access files on the intranet or manage intranet computers.
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.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logging and Tracing	Use trace route and logs for troubleshooting.
PPPoE	PPPoE mimics a dial-up Internet access connection.
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.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyXEL Device.

The following list, which is not exhaustive, illustrates the standards supported in the ZyXEL Device.

Table 63 Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band

Table 63 Standards Supported (continued)

STANDARD	DESCRIPTION
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)

Wall-mounting Instructions

Complete the following steps to hang your ZyXEL Device on a wall.

See Table 61 on page 171 for the size of screws to use and how far apart to place them.

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

2 Drill two holes for the screws. The distance between the centers of the holes is listed in the product specifications appendix.

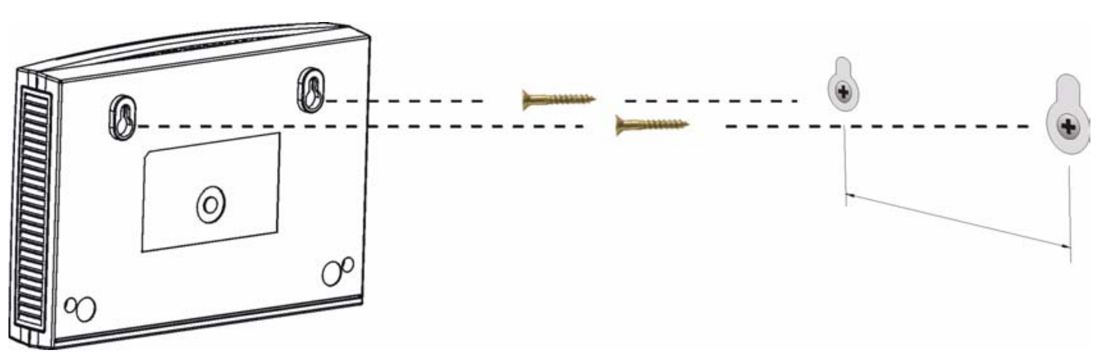
Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

3 Do not insert the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.

4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the ZyXEL Device with the connection cables.

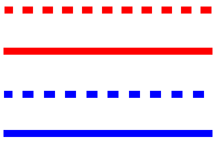
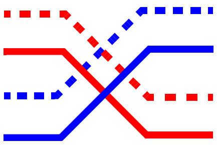
5 Align the holes on the back of the ZyXEL Device with the screws on the wall. Hang the ZyXEL Device on the screws.

Figure 123 Wall-mounting Example



Cable Pin Assignments

Table 64 Ethernet Cable Pin Assignments

WAN / LAN ETHERNET CABLE PIN LAYOUT					
Straight-through			**Crossover**		
(Switch)		(Adapter)	(Switch)		(Switch)
1 IRD +		1 OTD +	1 IRD +		1 IRD +
2 IRD -		2 OTD -	2 IRD -		2 IRD -
3 OTD +		3 IRD +	3 OTD +		3 OTD +
6 OTD -		6 IRD -	6 OTD -		6 OTD -

Power Adaptor Specifications

Table 65 US Power Adaptor Specifications

AC Power Adaptor Model	30-112-122204B
Input Power	AC 120 Volts
Output Power	AC 12 Volts/ 1 A
Power Consumption	12 W
Safety Standards	UL and CSA

Table 66 EU Power Adaptor Specifications

AC Power Adaptor Model	30-123-122001B
Input Power	AC 230 Volts
Output Power	AC 12 Volts/ 1 A

Table 66 EU Power Adaptor Specifications

Power Consumption	12 W
Safety Standards	ITS, GS, and CE

B

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 67 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.
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.

Table 67 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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).
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.

Table 67 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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.

C

Wireless LANs

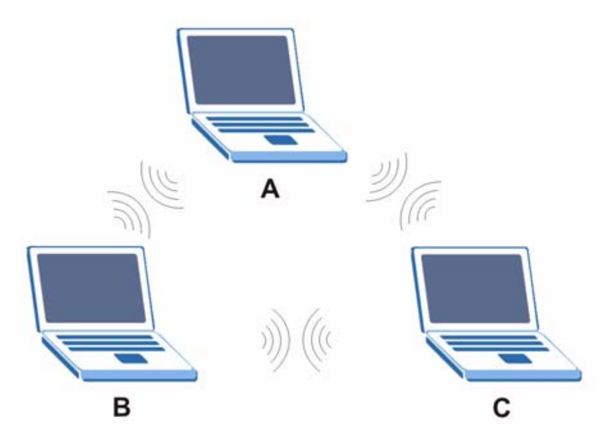
Wireless LAN Topologies

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 124 Peer-to-Peer Communication in an Ad-hoc Network

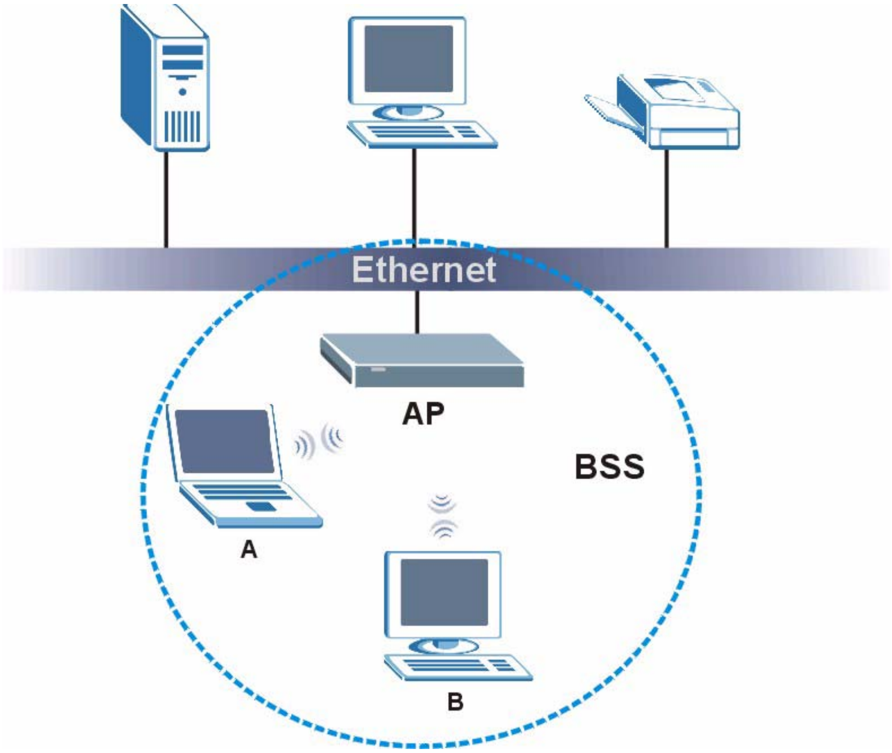


BSS

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 125 Basic Service Set



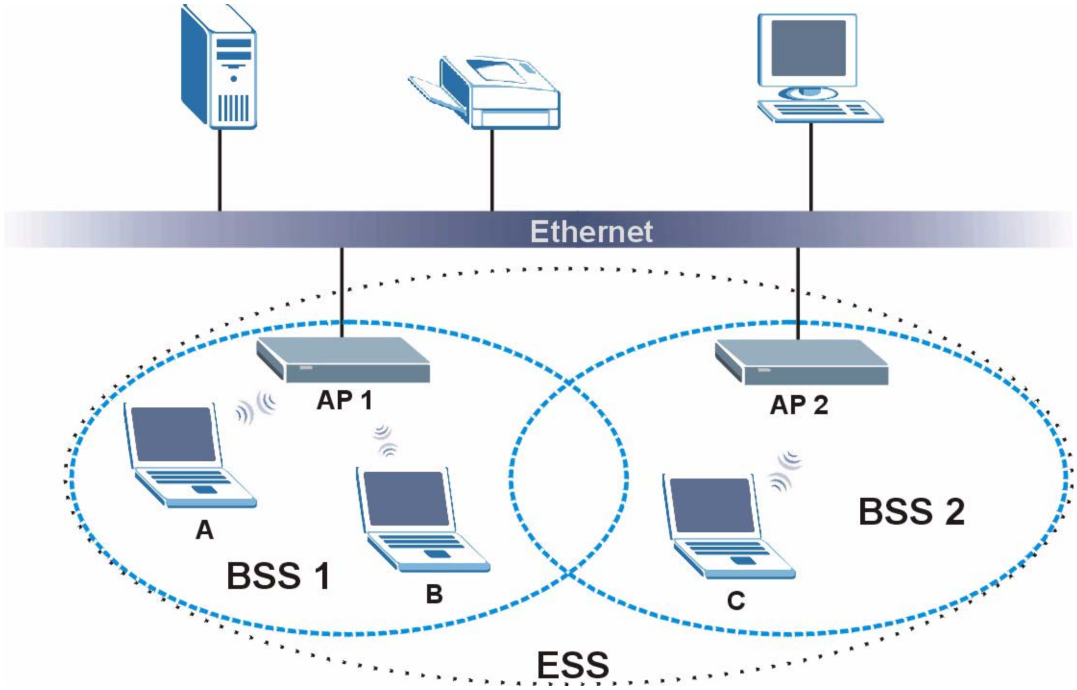
ESS

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 126 Infrastructure WLAN



Channel

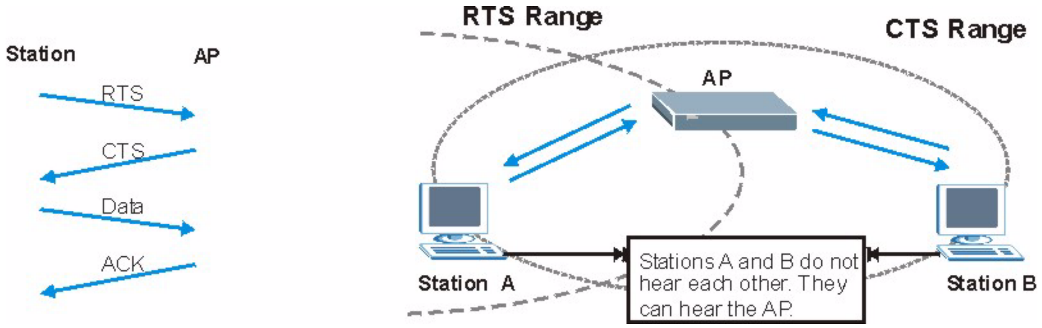
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference 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 127 RTS/CTS


Station
AP
RTS
CTS
Data
ACK
RTS Range
CTS Range
AP
Station A
Station B
Stations A and B do not hear each other. They can hear the AP.

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

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

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

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

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

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

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.

✍ 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 68 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 69 Wireless Security Levels

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

✍ 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.

✍ 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 70 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

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

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.

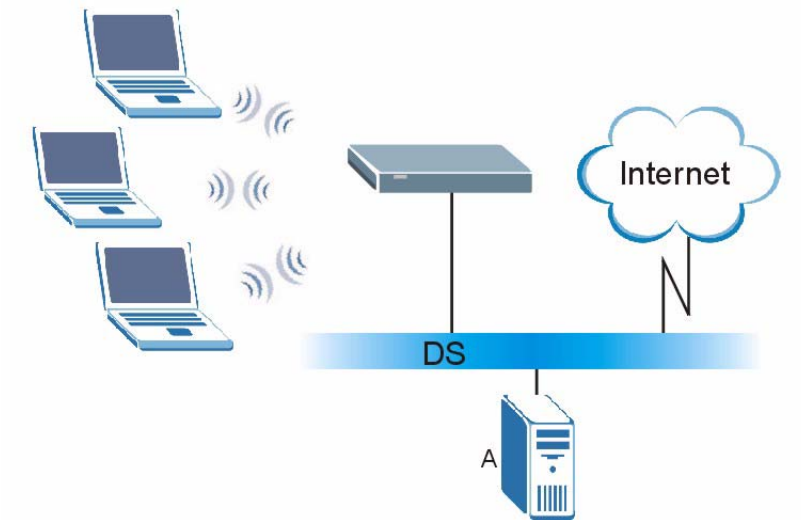
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

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 128 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

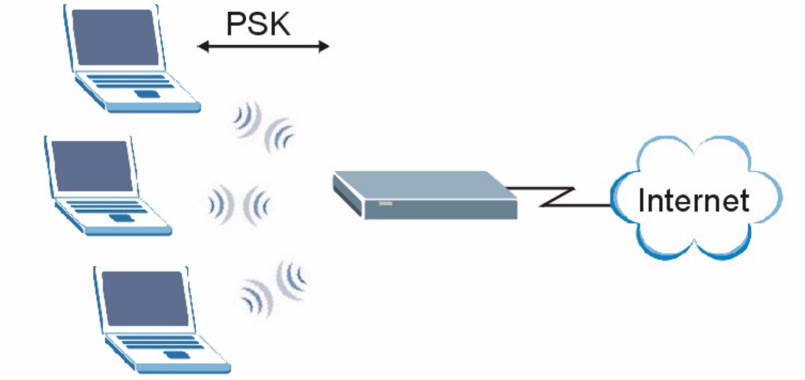
A WPA(2)-PSK application looks as follows.

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 129 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 71 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTIO N 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.

D

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

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。

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.

E

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- 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.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.us.zyxel.com
- FTP: ftp.us.zyxel.com

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5^{a} planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index